T.C.

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI

YÜKSEK LİSANS PROGRAMI

SİBER GÜVENLİK ÖLÇEĞİ GELİŞTİRME: GEÇERLİK VE GÜVENİRLİK ÇALIŞMASI

YÜKSEK LİSANS TEZİ

Kadir SEVİNÇ

Danışman: Doç. Dr. İbrahim ARPACI

TOKAT

Mayıs, 2021

ETİK SÖZLEŞME

Bu belge ile bu tezdeki bütün bilgi toplama ve raporlaştırma sürecinin Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği'ne, Lisansüstü Eğitim Enstitüsü Tez Yazım Kılavuzuna, genel akademik kurallara ve etik ilkelere uygun olarak gerçekleştirildiğini; bu tez çalışmasının "intihal engelleme" programı ile tarandığını, bana ait olmayan tüm bilgi, düşünce ve bulgulara atıf yaptığımı ve kaynağını gösterdiğimi beyan eder, sorumluğun tarafıma ait olduğunu kabul ederim.

Tarih: 20/05/2021

Tezi hazırlayan öğrencinin

Kadir SEVİNÇ

İmza

Jüri Onay Sayfası

Lisansüstü Eğitim Enstitüsü Müdürlüğü'ne,

Bilgisayar ve Öğretim Teknolojileri Eğitimi tezli yüksek lisans öğrencisi Kadir SEVİNÇ'in Siber Güvenlik Ölçeği Geliştirme Geçerlik ve Güvenirlik Çalışması adlı çalışması 20/05/2021 tarihinde jürimiz tarafından Bilgisayar ve Öğretim Teknolojileri Anabilim Dalı'nda yüksek lisans tezi olarak kabul edilmiştir.

Adı Soyadı	İmza
Başkan: Prof. Dr. Gülşah BAŞOL	.....
Üye (Tez Danışmanı): Doç. Dr. İbrahim ARPACI	.....
Üye : Dr. Öğretim Üyesi Kasım KARATAŞ	.....

Onay

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

…/…/2021

……

Enstitü Müdürü

TEŞEKKÜR

Yüksek lisans eğitim sürecinde bana yol gösteren, tezimin yazım sürecinde tecrübesi ve bilgi birikimiyle benimle sürekli fikirlerini paylaşan ve ölçek geliştirilmesi, ölçeğin uygulanması ve analiz aşamasında bana yardımcı olan, yol gösteren tez danışmanım Doç. Dr. İbrahim ARPACI'ya teşekkürlerimi sunarım.

Tokat Gaziosmanpaşa Üniversitesi BÖTE bölümündeki hocalarıma da mesleki gelişimimde ve akademik anlamda bilgi birikimleriyle bana katkıda bulundukları için hepsine ayrı ayrı teşekkürlerimi sunarım. Ayrıca hazırlamış olduğum bu tezimde ölçek geliştirme ve veri toplama sürecinde bana yardımlarını hiç esirgemeyen değerli arkadaşım Ersin ATEŞ'e de ayrıca teşekkürlerimi sunarım. Sevgili eşim Esra SEVİNÇ ve kızım Elif Bilge'ye de bana tez yazım sürecinde benden ayrı kaldıkları, benimle vakit geçiremedikleri için tez çalışmamın yazım aşamasında bana göstermiş oldukları hoşgörü ve anlayıştan dolayı kendilerine sonsuz teşekkürlerimi sunarım.

Tezimi yazmam konusunda bana sürekli telkinlerde bulunan bana yol gösteren, benim bugünlere gelmemde en büyük paya sahip, hayatımın her anında yanımda olan, bana hayat tecrübeleriyle rehberlik eden, yol gösteren eğitimci, emekli öğretmen babam Yusuf SEVİNÇ'e de sonsuz sevgi ve saygılarımı sunarım. Ayrıca sevgisini, desteğini bana karşı hiç eksik etmeyen, her zaman manevi olarak bana destek veren benim yanımda olan annem Melek SEVİNÇ'e de sevgi ve saygılarımı sunar, teşekkür ederim.

Kadir SEVİNÇ

ÖZET

SİBER GÜVENLİK ÖLÇEĞİ GELİŞTİRME:

GEÇERLİK VE GÜVENİRLİK ÇALIŞMASI

Sevinç, Kadir

Yüksek Lisans, Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

Tez Danışmanı: Doç. Dr. İbrahim Arpacı

Mayıs 2021, vii + 56 sayfa

Siber güvenlik, nesnelerin interneti veya siber fiziksel sistemler çağının en büyük güçlüklerinden birisi olacaktır. Siber saldırılar sadece kurumlar değil bireyler için de artan bir risk haline gelmiştir. Dolayısıyla, herkes siber güvenlik risklerinin farkında olmalı ve proaktif eylemlerle siber saldırılara karşı hazır olmalıdır. Bu çalışmanın amacı, günümüz siber fiziksel sistemler çağında ülkemizdeki ve dünyadaki bireylerin siber güvenlik pratiklerini ve algılarını belirlemeye yönelik geçerli ve güvenilir bir ölçek geliştirmektir. Bu çalışmada, Parker Altılısı (Parkerian Hexad) modeli temel alınarak bir siber güvenlik ölçeği (SGÖ) geliştirilmiş ve bu ölçeğin psikometrik özellikleri test edilmiştir. Bu çalışmanın örneklemini Tokat Gaziosmanpaşa Üniversitesinde öğrenim gören toplam 993 üniversite öğrencisi oluşturmaktadır. Birinci çalışma toplam 380(239 kadın, 141 erkek) katılımcıdan oluşmaktadır. Birinci çalışmada geliştirilen ölçek açımlayıcı faktör analizi (AFA) ile test edilmiştir. AFA sonuçları altı faktörlü bir yapı ortaya koymuştur ve ölçeğin tamamı için Cronbach alfa iç güvenirlik kat sayısı .88 olarak bulunmuştur. İkinci çalışma ise toplam 613 (325 kadın ve 288 erkek) katılımcıdan oluşmaktadır. İkinci çalışmada doğrulayıcı faktör analizi ile altı faktörlü yapının (gizlilik, kontrol/sahiplik, bütünlük, gerçeklik, erişilebilirlik ve fayda) verilerle iyi uyum gösterip göstermediği incelenmiştir. Sonuçlar SGÖ'nün yakınsak ve ayrım geçerliliği ile yapı geçerliliğine sahip olduğunu göstermektedir. Bu tez çalışması sonucunda bireylerin siber güvenlik pratiklerini ve algılarını ölçmek için kullanılabilecek geçerli ve güvenilir bir ölçek geliştirilmiştir.

Anahtar Kelimeler: Siber Güvenlik, Siber Güvenlik Ölçeği, SGÖ, Ölçek Geliştirme

ABSTRACT

DEVELOPMENT OF THE CYBERSECURITY SCALE (CS-S):

EVIDENCE OF VALIDITY AND RELIABILITY

Sevinç, Kadir
Master's Thesis, Department of Computer Education and Instructional Technology
Advisor: Assoc. Prof. Dr. İbrahim Arpacı
May 2021, xii + 56 pages

Cybersecurity will be one of the main challenges in the age of Internet of Things (IoT) or cyber-physical systems. Cyber-attacks are a growing risk not only organizations but also individuals. Anyone should be aware of cybersecurity risks, and thereby, ready for cyberattacks by proactive actions. This study aimed to develop Cyber Security Scale (CS-S) based on the Parkerian Hexad model and test its psychometric properties. Sample of the study consisted of 993 undergraduate students studying at Tokat Gaziosmanpaşa University. The first study (239 women, 141 men) consisted of 380 participants. The first study tested the scale by conducting an explanatory factor analysis (EFA). The EFA results a six-factor structure and Cronbach alpha internal consistency of the total scales was found as .88. The second study (325 women, 288 men) consists of 613 participants in total. The second study conducted a confirmatory factor analysis (CFA) to investigate whether the six-factor model (i.e., availability, authenticity, confidentiality, control/possession, integrity, and utility) has a good fit with the data or not. The CFA results indicated that the CS-S has convergent and, discriminant validity along with construct validity. As a result of this thesis study, a valid and reliable scale was developed to measure individuals' cybersecurity practices and perceptions.

Keywords: Cyber Security, Cyber Security Scale, CS-S, Scale Development

İÇİNDEKİLER

Sayfa

TABLO LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

KISALTMALAR

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

AFAD: Afet ve Acil Durum Yönetimi Başkanlığı

AFA: Açımlayıcı Faktör Analizi

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CIA: Bilgi Güvenliği Üçlüsü

DFA: Doğrulayıcı Faktör Analizi

CMK: Ceza Muhakemeleri Kanunu

EGM: Emniyet Genel Müdürlüğü

ITU: Uluslararası Telekomünikasyon Birliği

IEC: Uluslararası Elektroteknik Komisyonu

MEB: Millî Eğitim Bakanlığı

SGÖ: Siber Güvenlik Ölçeği

SOME: Siber Olaylara Müdahale Ekibi

TCK: Türk Ceza Kanunu

TBMM: Türkiye Büyük Millet Meclisi

TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

USOM: Ulusal Siber Olaylara Müdahale Merkezi

BÖLÜM I

GİRİŞ

Problem

Siber güvenlik "siber ortamı ve kurum ve kullanıcının varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kılavuzlar, risk yönetim yaklaşımları, eylemler, eğitimler, en iyi uygulamalar, güvenceler ve teknolojiler" olarak tanımlanabilir (ITU, 2008). Kullanıcıların ve örgütlerin varlıkları arasında bağlı servisler, uygulamalar, cihazlar, sistemler ve siber alanda saklanan veya iletilen veriler yer alır (Reid ve Van Niekerk, 2014; ITU, 2008). Yukarıda verilen tanımdan yola çıkarak siber güvenliğin siber alanın kendisinin, bilginin ve siber alan kullanıcılarını destekleyen teknolojileri korumayı içerdiği ve "fiziksel formda var olmayan şekillerde teknoloji cihazları ve ağlarıyla bağlı olan insanlar, yazılımlar ve hizmetlerin etkileşiminden meydana gelen karmaşık ortam" olarak tanımlandığı açıkça görülmektedir (ISO/IEC, 2012). Böylelikle, siber güvenlik siber alanın kendisinin ve siber alanda bulunan bilginin ve teknolojilerin bütünlüğünün ve gizliliğinin korunmasını içerir (ISO/IE, 2012).

Siber suç bir bilişim sisteminin güvenliğini ve buna bağlı kullanıcı verilerini hedef alan, bilişim sistemi kullanılarak işlenen suçlardır (EGM, 2019). Siber suçu diğer suçlardan ayıran en temel özellik bir bilişim sistemi olmadan işlenememesidir. Dolayısıyla, bu suç türü bilgisayar ve internetle işlenen suçlar olarak da adlandırılmaktadır (EGM, 2019). 21. yüzyılda dünyada milyarlarca bilgisayar ve internet kullanıcısı olduğu bilinmektedir. Ülkemizde ve birçok dünya ülkesinde haberleşme, telekomünikasyon, eğitim, sağlık, ulaşım gibi birçok kritik altyapıların güvenliği de bilgisayar ve internetten oluşan bilişim sistemleri sayesinde sağlanmaktadır. Dünya üzerindeki ülkeler arasında gerçekleştirilen siber saldırıların sosyal ve ekonomik hayatı olumsuz yönde etkilediği bilinmektedir. Bu nedenle, küresel ölçekte risk oluşturulan siber saldırılar dünya ekonomisini ve ülkelerin kritik altyapılarının güvenliğinin sağlanmaları için ülkeleri yeni önlemler almaya bu konuda ortaya çıkacak problemlerin ve sorunların çözümü noktasında ulusal ve uluslararası boyutta bir dizi eylemler gerçekleştirmelerine yol açmıştır. Bu nedenle, siber güvenlik sorunu ülkemizde ve dünyada gelecekte en büyük sorunlardan biri olacağı düşünülmektedir. Siber güvenlik

üzerine literatürde yapılmış çalışmalar incelendiğinde siber güvenlikle ilgili literatürde birçok yapılmış çalışma bulunmasına rağmen bireylerin siber güvenlik pratiklerini ve algılarını ölçmeye yarayan bir ölçek geliştirme çalışmasına rastlanılmamıştır. Bu nedenle bu çalışmada bireylerin siber güvenlik pratiklerini ve algılarını ölçmeye yönelik bir ölçme aracı geliştirme çalışması yapılması planlanmıştır. Bu ölçek gizlilik, bütünlük ve erişilebilirlik (CIA) bilgi güvenliği modelinin güncellenmesi ile ortaya çıkan Parker Altılısı modeli temel alınarak geliştirilmiştir (Parker, 1992). Bu tez çalışması sonunda geliştirilen siber güvenlik ölçeği bireylerin siber güvenlik ihtiyaçlarını ortaya koyarak siber güvenliği artıracak politikalar geliştirmek için karar vericilere yol gösterici olabilir.

Amaç

Siber suçlar günümüzde hızla yaygınlaşırken bireylerin siber güvenlik pratiklerini ve algısını ölçen bir ölçme aracına rastlanmamıştır. Bu konu ile ilgili literatürde yapılmış mevcut herhangi bir ölçek geliştirme çalışmasına rastlanılmadığından literatürdeki bu alandaki boşluğu doldurulup literatüre katkı sağlayacağı düşünülmektedir. Dolayısıyla, bu araştırmanın amacı bireylerin siber güvenlik pratiklerini ve algısını ölçen bir ölçek geliştirilmesi, geliştirilen aracın geçerlik ve güvenirlik çalışmasının gerçekleştirilmesidir. Bu ölçek gizlilik, bütünlük ve erişilebilirlik (CIA) bilgi güvenliği modelinin güncellenmesi ile ortaya çıkan Parker Altılısı modeli temel alınarak geliştirilecektir (Solomon ve Chapple, 2005).

Önem

Bireysel ve genel olarak tüm özel ve kamusal alanda her türlü hassas bilgi içeren sistemlerin dışarıdan gelebilecek güvenlik sorununa karşı gerekli önlemlerin alınması gerekmektedir. Bu nedenle güvenlik sorunlarının asgari düzeyde olması, ülkelerin siber güvenlik ve bilgi güvenliğine gereken önemi vermesi ve bu konuda gerekli hassasiyetin gösterilmesi azami derecede önemlidir. Dijital ortamda siber güvenlik sadece siber saldırı şeklinde gerçekleşmeyip, doğal afetler sonucu veya terör olayları sonucu da ülkelerin bilişim sistemleri zarar görmektedir. Günümüzde en büyük güvenlik sorunu bilişim dünyasında yaşayan siber saldırılar olarak ifade edilmektedir.

“Web of Science” veri tabanında 1999 yılından günümüze kadar toplam 3088 siber güvenlik yayını (1151 makale) bulunmaktadır. Tüm bu yayınların anahtar kelimesinde “cybersecurity” (siber güvenlik) veya bağlığında “cyber security” ifadesi geçmektedir. Bu çalışmalarda en çok kullanılan anahtar kelimelerin “cybersecurity” (f=633), “cyber security” (f=510) ve “security” (f=97) olduğunu göstermektedir. Sonuçlar siber güvenlik çalışmalarının sayısındaki ciddi artışı göstermektedir. Ancak bu çalışmaların hiçbiri bireylerin siber güvenlik pratiklerini ve algılarını ölçmeye odaklanmamıştır. Siber güvenlik, siber fiziksel sistemler olarak da adlandırılan nesnelerin interneti (IoT) çağında önemli bir kavramdır (Ashibani & Mahmoud, 2017). Birbiriyle ilişkili cihazların dağıtılmış doğası, siber saldırı zafiyeti oluşturarak bilginin bütünlük, gizlilik ve erişilebilirlik özelliklerini hedef alarak güvenlik ve gizliliği ihlal etmektedir (Cherdantseva vd., 2016). Bu nedenle, herkes siber güvenlik risklerinin farkında olmalı ve proaktif eylemlerle siber saldırılara karşı hazır olmalıdır. Buna göre mevcut araştırma bireylerin siber güvenlik durumunu veya seviyesini ölçmeyi amaçlayan siber güvenlik ölçeği (SGÖ) geliştirme ve doğrulama sürecine odaklanmaktadır. Alanyazın incelendiğinde bireylerin bilgi güvenliği farkındalıklarını ölçen ölçeklere rastlansa da siber güvenlik pratiklerini ve algısını ölçen bir ölçme aracına rastlanmamıştır. Bu nedenle, bu ölçek geliştirme çalışması özgün bir çalışmadır.

Günümüzde teknolojisinin gelişmesine ve bireylerin aktif olarak bilişim sistemlerini kullanması sonucu bilgisayar ve internet aracılığıyla işlenen bilişim suçları, yani siber suçlar hızla artmaktadır. Hacking, Bot-Net / D-Dos Saldırıları, Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, Haberleşmenin Gizliliğini İhlal, Özel Hayatın Gizliliğine Müdahale Etme, İletişimi Engelleme, İletişimi İzinsiz İzleme ve Kayıt Etme, Kişisel Verilen Kaydedilmesi, Nitelikli Hırsızlık, Nitelikli İnteraktif Dolandırıcılık, Banka ve Kredi Kartı Suçları, Online Örgütlü Kumar gibi faaliyetler siber suç olarak adlandırılmaktadır (EGM, 2019). Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığına yansıyan olaylar incelendiğinde bilişim sistemleri vasıtasıyla işlenen birçok suç olduğu görülmektedir. Bilişim sistemleri dünya üzerinde gelişmiş ve gelişmekte olan birçok ülkede farklı sektörlerde aktif olarak kullanılmasına rağmen bilişim suçları konusunda bireylerin yeterince aydınlatılmadığı veya bilişim suçları konusunda yeterince bilgi sahibi olmadıkları Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüklerine ve adliyelere yansıyan bilişim suçlarından da anlaşılmaktadır. Günümüzde

toplumda bilişim sistemlerinin yaygın olarak kullanılmasına bağlı olarak artan siber saldırılar ve bunun sonucu yaşanabilecek sosyal ve ekonomik zararlar dikkate alındığında bu durumun ülkelerin mali, sosyal ve ekonomik alt yapısına, ülkelerin dünyadaki saygınlığına, kritik altyapılarına ve siber güvenlik sistemlerine verdiği zararların boyutunun çok büyük olduğu anlaşılmaktadır. Bu nedenle, bilişim sistemleri kullanılarak işlenen suçları ve yaşanabilecek siber saldırıları bertaraf etmek, kamu kurumu ve özel kuruluşlardaki bilgisayarların ve ağ sistemlerinin güvenliğini sağlamak amacıyla birçok kurum ve kuruluş siber güvenlik uzmanı, bilişim uzmanı, yazılım mühendisi, bilgisayar mühendisi, bilgisayar programcısı, network uzmanı gibi birçok meslek grubundan bünyesinde çalıştırmak üzere eleman almaktadır. Bilgi güvenliğini konusunda dikkat çeken en büyük sorunlardan biri de bilişim sistemlerini kullanan bireylerin siber güvenlik konusundaki farkındalık düzeylerinin düşük seviyelerde olmasıdır. Bu konuda en çok problem yaşayan bilişim sektörleri incelendiğinde temel problemin bilişim sistemlerinde çalışanların bilgi güvenliği ve siber güvenlik konularındaki bilgi eksikliğinden kaynaklandığı görülmektedir (Bilişim Teknolojileri ve Siber Güvenlik Derneği, 2018).

Bilişim sistemlerinin, bilgisayar ve internetin hayatımızın her alanına girdiği 21. yüzyılda siber güvenlik sorunu, siber saldırılar gelecekte bütün dünya ülkelerinin en temel sorunlarından birisi olacağı düşünülmektedir. Bilim insanlarınca gelecekte olası yaşanabilecek savaşların da teknolojik savaş ya da siber savaş olarak gerçekleşeceği öngörülmektedir. Günümüz bilgi çağında insan gücünün yerini bilgisayar ve bilişim sistemlerinin aldığını, eğitimden sağlığa, emniyetten adalete, güvenlikten ekonomiye kadar bütün sektörlerde bilişim sistemlerinin yaygın olarak kullanıldığı düşünüldüğünde milyarlarca kullanıcının bulunduğu internet olarak adlandırılan küresel alemde birçok siber saldırının yaşanabileceği, bunun akabinde birçok insanın siber güvenlik sorunu yaşayabileceği düşünülmektedir. Bilişim dünyasında yaşanan gelişmelere bağlı olarak bütün bu olaylar geniş bir çerçevede ele alınıp incelendiğinde siber güvenlik ölçeğinin geliştirilip bilgisayar ve internet kullanıcılarının hizmetine sunulmasının literatürdeki bu alana katkı sağlayacağı düşünülmektedir.

Sınırlılıklar

- Bu çalışmanın örneklemi Tokat Gaziosmanpaşa Üniversitesinde 2019-2020 yıllarında öğrenim gören bilgisayar ve internet kullanan üniversite öğrencileri ile sınırlıdır (n=993).
- Bu çalışma nicel ve nitel araştırma yöntemlerinin birlikte kullanıldığı karma yöntemdir.

Tanımlar

Bilişim sistemleri: Siber ortamda bilgi ve iletişimin sağlandığı, bilgisayar ve internet ağı yardımıyla bilgi ve iletişim teknolojileri kullanılarak gerçekleştirilen bütün işlemlerdir (Ulusal Siber Olaylara Müdahale Merkezi, 2014).

Siber: Bilgisayar ve internet gibi bilişim sistemlerinde kullanılan her türlü aygıtın bir bütün olarak birleşiminden oluşan sistemlerin ağ (network) yardımıyla iletişimini sağlayan elektronik ortamdır (Sağıroğlu, 2018). Siber, sibernetik kelimesinin kökeninden gelen bir kavramdır. Literatürde ilk defa 1958 yılında insanlar ve teknolojik cihazlar ve makineler arasındaki iletişimi sağlayan ve insanlarla bu cihazlar arasındaki ilişkiyi inceleyen Sibernetik biliminin öncülerinden Louis Couffignal tarafından kullanılmıştır (https://istanbulism.saglik.gov.tr).

Siber suç: Siber suç bir bilişim sisteminin güvenliğini ve buna bağlı verileri ve kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber suçu diğer suçlardan ayıran özelliği bir bilişim sistemi olmadan işlenememesidir. Bu suç türü bilgisayar ve internetle işlenen suçlar olarak da adlandırılmaktadır (EGM, 2019).

Siber ortam: Dünyada ve uzaydaki bilişim sistemleri olarak adlandırılan bilgisayar ve internetin kullanıldığı, bilişim sistemlerinde sanal ortam olarak tabir edilen, internet ağı veya diğer network sistemleri ile birbirine bağlı ortamlar siber ortam olarak ifade edilmektedir (AFAD Sözlüğü, 2020).

Bilgi güvenliği: Bilginin başkalarının rızası olmadan kullanılmasını, tahrip edilmesini, izinsiz değiştirilmesini, yok edilmesini veya bilgisayar kullanıcılarının bilgisayarlarında sakladıkları bilginine izinsiz erişmek isteyen kişilerin erişimini engellemek için gerçekleştirilen işlemdir (https://tr.wikipedia.org).

Siber güvenlik: Bilişim sisteminin güvenliği, bilgisayar ve internetin güvenliği, bireylerin kullanmış oldukları bilgisayar ve internetteki kişisel verilerinin korunması, ayrıca bireylerin sanal ortamda kendilerini rahat ve güvende hissetmeleri için bilişim sistemlerindeki verilerin korunması olarak adlandırılmaktadır (https://sibertehdit.com).

Siber varlık: Siber ortamlarda bulunan, araçlar, işlemler, dokümanlar, planlar, veriler veya bilgilerdir. Bu bir bilgisayar, sunucu veya bir ağ cihazı olabileceği gibi kişisel, kurumsal veya ulusal veriler de olabilir. İnternete bağlı televizyon, cihaz, sistem veya araç olabileceği gibi veri tabanı, veri merkezi, veri kayıt sistemi veya kullanılan yazılımlar, donanımlar ve süreçler siber ortamdaki varlıklardır (USOM-TRCERT, 2014).

Siber Saldırı: Bilişim sistemlerinin güvenlik alt yapısına zarar vermek veya siber ortamda bulunan kişi veya kişilerce bilgisayar ve internet yani bilişim sistemleri kullanılarak gerçekleştirilen eylemler, saldırılar siber saldırı olarak ifade edilmektedir (UDHB, 2016).

Siber tehdit: Bilişim sistemlerine zarar vermek amacıyla bilgi ve iletişim teknolojileri kullanılarak gerçekleştirilen, bilişim dünyasındaki her türlü aygıta zarar vermek, engellemek, bozmak, verileri ele geçirmek amacıyla gerçekleştirilen siber saldırıların siber ortamda kullanılması olarak adlandırılmaktadır. İnternet bankacılığı kullanan bireylere yönelik gerçekleştirilen dolandırıcılık yöntemi, bilgisayar virüsleri siber tehditlere örnek olarak verilebilir. Siber tehditler yeryüzünde bireylerin işlemiş oldukları herkes tarafından bilinen suçların siber ortama aktarılmış şeklini ve bilgi ve iletişim teknolojileri kullanılarak gerçekleştirilen suçları kapsamaktadır (BTK, 2009).

Siber uzay: Dünya üzerindeki bireylerin bilgisayar, internet ve telekomünikasyon sistemleri vasıtasıyla iletişim kurdukları yer, zaman ve sınır kavramı olmayan dijital ortam olarak ifade edilmektedir. Ayrıca Siber Uzay günlük hayatta kullandığımız bilişim sistemlerinden internete, akıllı telefonlardan network üzerinden birbirine bağlı bilgisayarlara, tabletlerden yazılım ve donanımlara kadar hepsi bir bütün olarak siber uzay olarak adlandırılmaktadır (Erçağlar, 2017).

Siber casusluk: Bilişim teknolojilerinin hızla geliştiği günümüzde bilişim sistemleri konusunda farklı ülkeler arasında meydana gelen rekabet veya düşmanlık nedeniyle bilişim sistemleri kullanılarak başka bir ülkenin devlete karşı hâkimiyet sağlamak için, o ülkenin

bilgisayar ve internet gibi bilişim sistemlerine, ağ (network) sistemlerine gayri resmi bir şekilde izinsiz girilmesi sonucu ülkelerin gizli ve önemli bilgininin ele geçirilmesi işlemidir (Çifçi, 2013).

Ulusal Siber Güvenlik: Ulusal siber ortamdaki bilişim sistemleri, bilgisayar ve internet gibi bilişim aygıtlarının kullanıldığı siber ortamda gerçekleştirilen işlemlerin, bilginin ve verilerin güvenliği Ulusal Siber Güvenlik olarak ifade edilmektedir (USOM- TRCERT, 2014).

Siber Güvenlik Kavramları

Erişim Kontrolü: Bilişim sistemlerinde bilgiye erişimin kontrol altında tutulması, bilgiye izinsiz erişmek isteyen, zarar vermek isteyen kullanıcıların erişiminin engellenmesi, ayrıca uzaktan eğitim, çevrimiçi eğitim gibi platformlarda bilgi güvenliğinin korunmasıdır (USOM-TRCERT, 2014).

Kimlik Denetimi: Bilişim sistemlerindeki uygulamalarda kullanıcıya ait kimliği doğrulama işlemidir (USOM- TRCERT, 2014).

Yetkilendirme: Bilişim sektöründe kullanıcının birtakım bilgi, belge ve dokümanlara erişiminin olup olmadığının değerlendirme aşamasıdır (USOM- TRCERT, 2014).

Varlık: Bilişim sistemlerinde herhangi bir saldırı ve zararlı yazılımlara karşı korunması gereken kullanıcılara ait T.C. kimlik numarası, telefon numarası, iletişim bilgileri, kredi kartı bilgileri, personel ve kullanıcıya ait veri tabanı gibi kaynakları ifade eder (USOM- TRCERT, 2014).

Güvenlik Açığı: Bilişim sistemlerinde yazılımcıların gözünden kaçan kullanıcılar tarafından uygulamada ortaya çıkan açık kalan kısımlara veya sistemde donanımsal olarak ortaya çıkan sorunlarından yaşanan duruma güvenlik açığı denilmektedir (USOM- TRCERT, 2014).

Risk: Bilgisayar ve internette sanal ortamda yaşanabilecek olası siber saldırılar sonucu meydana gelen zararlı durum olarak adlandırılmaktadır (USOM- TRCERT, 2014).

Tehdit: Siber ortamda kötü niyetli kişilerce olumsuz sonuçlara sebebiyet verebilecek şekilde sisteme dışarıdan zararlı yazılım veya virüsler yoluyla gerçekleştirilebilecek saldırı veya saldırı türleridir (USOM- TRCERT, 2014).

Hacker & Siber Suçlular: Hackerler veya diğer bir isimle bilgisayar korsanları kullanıcıların bilgisayarlarına ve mobil aygıtlara bağlanan, kamu veya özel firmaların bilgisayarın network sistemlerine bağlanarak izinsiz erişimde bulunan kişiler olarak ifade edilmektedir. Hackerler veya siber korsanlar bilgisayar ve iletişim teknolojileri konusunda ileride düzeyde bilgiye sahip, yazılım ve network konusunda kendini geliştirmiş, yüksek düzeyde programlar tasarlayabilen ve bu programları kullanan kişi veya kişilerdir (Yılmaz ve Sağıroğlu, 2013).

İç (Dâhili) Saldırganlar: İçinde bulunduğu sistem içerisinde, belli hedefler doğrultusunda dâhili yani iç sistemlere siber saldırılarak gerçekleştiren birtakım kitlelerden oluşan siber saldırganlar olarak adlandırılmaktadır (USOM- TRCERT, 2014).

Siber Aktivistler: Ülkelerinde ve dünyada gördükleri birtakım ekonomik, siyasi ve sosyal olaylardan yaşanan sıkıntıları ifade etmek için kamu kurumlarına ve özel şirketlere veya firmaların siber güvenlik sistemlerine siber saldırı düzenleyerek bu sistemlerin yavaşlamasını, durmasını, etkilenmesini sağlayarak ülkesinde ve dünyada farkındalık yaratarak ses getirmeye çalışan kişi veya gruplar olarak belirtilmektedir (USOM- TRCERT, 2014).

İstihbarat Kurumları: Küreselleşen dünyada her geçen gün hızla gelişmekte olan bilişim dünyasında siber sistemleri kullanan ülkeler diğer ülkeleri, kendilerinin siber alt yapısına veya bilişim sistemlerine zarar verebilecekleri ihtimaline binaen siber olaylara karşı müdahale ekipleri oluşturmakta, kendi ülkelerine karşı yaşanabilecek olası siber saldırılara karşı siber güvenlik sistemlerini korumak ve siber olaylara karşı müdahale etmek için gerekli istihbarat birimleri oluşturulmaktadır. Ayrıca diğer ülkelerin siber alt yapısına ve siber sistemlerine ait önemli verilere erişmeye çalışmakta ve başka ülkelerin alt yapılarına da gerekli siber saldırılar gerçekleştirmektedirler (www.usom.gov.tr).

Siber Saldırı Türleri

Günümüzde bilinen en yaygın siber saldırı türlerini aşağıda listelenmiştir (Benzer, 2014):

- Bilgi ve veri aldatmacası (Data Diddling),
- Salam tekniği (Salami Techniques),
- Süper darbe (Super Zapping),
- Eş zamansız saldırılar (Asynchronous Attacks),
- Truva atı (Casus Yazılımlar),
- Zararlı yazılımlar (Kötücül Yazılımlar),
- Mantık bombaları (Logic Bombs);
- Oltalama (Phishing),
- Tarama (Scanning),
- Bukalemun (Chamelon),
- İstem dışı alınan elektronik postalar (Spam),
- Çöpe dalma (Scavenging),
- Gizli kapılar (Trap Doors),
- Sırtlama (Piggybacking),
- Yerine geçme (Masquerading),
- Sistem güvenliğinin kırılıp içeri sızılması (Hacking),
- Hukuka aykırı içerik sunulması,
- Web sayfası hırsızlığı ve yönlendirme,
- Sosyal mühendislik.

BÖLÜM II

KAVRAMSAL ÇERÇEVE

Bu bölümde Siber Güvenlik ölçeğinin geliştirilmesinde temel alınan Parker Altılısı modelinden ve siber güvenlik ile ilgili alanyazından bahsedilmiştir. Bu bölümde Siber Güvenlik Ölçeğinin (SGÖ) gizlilik, kontrol/sahiplik, bütünlük, gerçeklik, erişilebilirlik ve fayda olmak üzere toplam altı alt boyutu kapsamlı bir şekilde ele alınmıştır.

Henkoğlu ve Külcü (2013) bulut bilişim platformlarına ilişkin hukuksal risk ve problemleri AB direktifleri, ABD hukuk mevzuatı ve AB sözleşmelerini inceleyerek belirlemeyi amaçlamıştır. Yaptıkları literatür analizi sonucunda mevcut yasal düzenlemeler çerçevesinde Türkiye'deki bulut bilişim kullanıcılarının veri gizliliğini ve güvenliğini yeterli düzeyde koruyan bir hukuksal yapının bulunmadığı sonucuna ulaşmışlardır. Bu doğrultuda, güvenlik ve gizlilik temelli bir bulut bilişim modeli önerisi yapılmıştır.

Benzer bir çalışmada Yılmaz, Ulus ve Gönen (2015) Teknolojinin gelişmesine paralel olarak bilgisayar ve internet kullanıcı sayısının artmasıyla siber güvenlik ihtiyaçlarının artmasını buna bağlı olarak ülkemizde ve dünyada siber güvenlik ihtiyacı ve bu gereksinimi karşılamak için oluşabilecek olası siber tehditler ve risk analizlerini belirlemeyi amaçlamıştır. Yaptıkları literatür analizi sonucunda ülkemizde siber güvenlik ve risklere karşı altyapının yetersiz kaldığı, bu konuda bireylere siber güvenlik ve tehditler konusunda bilgilendirici eğitimler, konferanslar, çalıştaylar düzenlenip, siber suçlara karşı müdahale ekibinin oluşturulması, bu tehditlere karşı ulusal düzenlemeler ve çözüm önerileri sunulması, ayrıca toplumun siber suçlara ve bu tehditlere karşı önlem alma konusunda bilgilendirilmesi gerektiğini belirtmiştir.

Efendioğlu ve Sezgin (2007) gerçekleştirdikleri literatür analizi çalışmasında e-devlet uygulamalarında bilgi güvenliği ve gizliliği konusunda birtakım sorunlarla karşılaşıldığını tespit ederek bu sorunları aşmada bilgi güvenliği ve gizliliği konusunda ne gibi önlemler alınması gerektiği hususunu tartışmıştır. Diğer bir çalışmada Yılmaz ve Ezin (2017) ülkemizdeki ebeveynlerin bilgi güvenliği konusundaki farkındalıklarının tespit edilmesi amaçlamıştır. Nitel araştırma yöntemi kullanılarak yapılan bu çalışmada ülkemizdeki bir il

merkezinde ortaokulda öğrenim gören beş ve altıncı sınıf öğrencilerinin toplam 91 aile bireyi oluşturmaktadır. Bu araştırmada veri toplama aracı olarak velilerin bilgi güvenliği farkındalık anketi kullanılmıştır. Araştırma sonucunda ebeveynlerin bilgi güvenliği farkındalıklarının olduğu ancak verileri yedekleme ve yedekleme sıklığı konusundaki farkındalıklarının düşük olduğu anlaşılmıştır. Ailelerin çocuklarının bilgi güvenliğini sağlama konusunda çocuklarına sadece uyarılarda bulunmakla yetindikleri, çocuklarına bilgi güvenliği konusunda yardımcı olmada yetersiz kaldıkları, tam olarak çocuklarına bilgi güvenliği konusunda bilgi veremedikleri anlaşılmıştır.

Baykara, Daş ve Karadoğan (2013) tarafından bilgisayar ve teknoloji dünyasında kullanılan güvenlik araçları ve uygulamaları incelenmiş, bilgi güvenliği sistemlerinin, güvenlik amacıyla kullanılan araçların çalışma şekli, işlevi ve kullanım alanları detaylı bir biçimde ele alınmıştır. Ayrıca bilgisayar ve internet kullanan kişilerin ve kurumların bilgi sistemleri güvenliğinin sağlaması bakımından çeşitli önlemler ve çözüm yöntemleri anlatılmıştır. Kişi, kurum ve kuruluşlara internette bilgi güvenliği, bilgi güvenliği sistemlerinde kullanılan araçlar konusunda güvenlik önlemleri ve güvenlik politikaları konusunda almaları gereken önlemler, güvenlik stratejileri ve çözüm önerileri sunulmuştur.

Ünal (2018) siber güvenlik, siber güvenliğin nasıl sağlandığı, siber uzayda güvenli bilgi kullanımı konularını ele almıştır. Literatür analizi sonucunda siber saldırılara karşı siber güvenlik merkezi oluşturularak, siber güvenlik stratejisi politikaları doğrultusunda siber güvenlik planları uygulanması, toplumun tüm kesimlerinde siber saldırılara karşı mücadele önerileri, siber güvenlik farkındalığı ve siber güvenlik bilinci oluşturulması gerektiği hususu ifade edilmiştir.

Aksakallı (2019) bulut bilişimde yaşanan güvenlik sorunlarını inceleyerek bulut sistemlerinde yapılan saldırı şekillerini ve saldırı boyutunu analiz etmiştir. Literatür analizi sonucunda bulut bilişimdeki güvenlik sorunları tespit edilerek bulut bilişimin yaşadığı güvenlik tehditleri ve saldırılar sınıflandırılmıştır. Bulut bilişimdeki güvenlik sorunları kontrol etmek ve bu saldırıların tehditlerinin etkisini azaltmak ve en aza indirmek için alınması gereken güvenlik önemlerini açıklamıştır.

Akgün ve Topal (2015) eğitim fakültelerinde okuyan öğrencilerin bilişim güvenliği farkındalıklarını incelemiştir. Tarama modelindeki çalışmanın örneklemini Sakarya Üniversitesi Eğitim Fakültesinin farklı bölümlerinde okuyan toplam 217 öğrenci oluşturmaktadır. Veri toplama aracı olarak araştırmacılar tarafından geliştirilen "Bilişim Güvenliği Anketi" kullanılmıştır. Veriler betimleyici istatistikler kullanılarak analiz edilmiştir. Araştırma sonuçlarına göre bilişim güvenliği konuları ile ilgili farkındalıklarının yeterli olmadığını, birçok öğrencinin bu konuda yetersiz olduğu görülmüştür.

Aslanyürek (2016) Türkiye'de internet kullanan bireylerin internet güvenliği ve çevrimiçi gizlilik konularında yaşadıkları problemleri ve bu konulardaki farkındalıklarını incelemiştir. Toplam 479 kişiden toplanan veri çözümlendiğinde çevrimiçi (online) gizlilik ve güvenlik konusunda bireylerin farkındalık düzeylerinin yüksek olduğu, ancak internet ortamında yaşanan güvenlik ve gizlilik ihlalleri konusunda internet kullanan bireylerin interneti kullanmaktan vazgeçme düşüncelerinin düşük olduğu anlaşılmıştır.

Gökce, Şahinaslan ve Dincel (2014) bilişim sektörünün hızla geliştiği ülkemizde ve dünyada sürekli çoğalan mobil kullanıcı sayısı ile mobil yaşamda karşılaşabileceğimiz siber güvenlik sorunları, siber saldırılar, siber tehditler ve bu sorunlara karşı alınabilecek tedbirler ve yapılması gerekler konusunu ele alan bir literatür analizi yapmıştır. Hayatımızın bir parçası haline gelen mobil cihazları güvenli kullanabilmek için siber güvenlik sorunlarını, riskleri ve siber tehditlerin belirlenip gerekli önlem planlarının oluşturulması gerektiği ifade edilmiştir. Haberleşmenin güvenliği, verilerin gizliliğinin sağlanması, verilerin korunmasının sağlanması, güvenlik açıklarının önlenmesi konusunda mobil iletişim operatörlerinin görevleri üzerinde durulmuştur. Mobil iletişim konusunda siber güvenlik ve siber tehditler konusunda gerekli önlemlerin alınması ve güvenliğin sağlanması konusunda hem bireylerin hem de GSM operatörlerinin senkronize bir şekilde birlikte çalışması gerektiği vurgulanmıştır. Gerekli ceza ve müeyyidelerin varlığının ileride yaşanabilecek siber saldırıların önüne geçmek için caydırıcı bir husus olabileceği belirtilmiştir.

Sertçelik (2015) siber uzay ve siber güvenlik kavramlarını ele alarak incelemiştir. Literatür analizi sonuçları ile siber ortamlarda güvenlik kaygısı ve siber güvenlik sorunlarının dünyada giderek arttığına işaret edilmiştir, bu konuda alınması gereken önlemler ve tedbirler detaylı bir biçimde ortaya konulmuştur.

Atasoy ve Ormanlı (2019) teknolojinin ve bilişim sektörünün gelişmesine paralel olarak dijitalleşen dünyada toplumda bireylerin karşılayabilecekleri zorlukları, teknolojik gelişmelere bağlı olarak ortaya çıkan siber güvenlik sorunlarını ve yaşanan problemleri incelemiştir. Literatür analizi sonucunda, teknolojinin gelişmesine paralel olarak bilişim dünyasında meydana gelen ilerlemeler ve değişimler neticesinde ortaya çıkan en önemli sorunlardan birisinin teknoloji tabanlı güvenlik açıkları olduğu tespit edilmiştir. Siber güvenlikte yaşanan sıkıntılar ve toplumun bu konuda yaşayabileceği olumsuz durumlar ele alınmıştır.

Bingöl ve Karakoç (2015) internet bankacılığı ve telekomünikasyon alanında iletişimde yaşanılan siber güvenlik sorunlarını, siber saldırı şekillerini, siber saldırılara karşı farkındalık yaratmak ve siber saldırılara karşı korunma yöntemlerini incelemiştir. Literatür analizi sonucunda internet bankacılığını kullanan bireylerin bu hususta eğitilmeleri, bazı zararlı yazılımlar vasıtasıyla siber saldırıların gerçekleştiği, hatta bu zararlı yazılımların kendilerini kullanıcıların bilgisayarında kullanmış oldukları anti-virüs yazılımlarından gizledikleri, siber saldırıların internet bankacılığı kullanan kullanıcıların sistemlerini çalışamaz hale getirdikleri, bu nedenle farklı boyutlarda önlem alınması gerektiği belirtilmiştir.

Çetin, Gundak ve Çetin (2015) siber güvenlik risklerini ve işletmelere olan etkilerini, işletmeleri tehdit eden siber saldırıları, siber saldırıların işletmelere yaşattığı kayıpları ve siber saldırıların işletmelere olan maliyetlerini incelemiştir. Literatür analizi sonucunda Türkiye'de ve Dünyada siber saldırıların maliyetini, günümüzde bilhassa üretim ve hizmet sektörlerinde faaliyet gösteren şirketlerin siber tehditlere maruz kaldıkları, şirketlerin siber tehditlerden korunmak için siber güvenlik politikalarını gözden geçirmeleri gerektiği hususunu belirtilmiş, ayrıca çalışma sonuçlarına göre işletmelerin güvenlik problemlerine karşı yeni sistemler ve çözümler geliştirmesi gerektiği hususları ele alınmıştır.

Öztürk (2018) işletmelerin maruz kaldıkları siber saldırı sonucu yaşadıkları olumsuz durumları, siber saldırılar sonucu işletmelerde meydana gelen maddi zararları ve siber saldırıları önlemek için alınması gereken güvenlik tedbirlerini incelemiştir. Bu amaçla siber güvenliğe dair denetimi etkileyen faktörler belirlenerek, denetim planı ve denetim raporunun

oluşturulması amaçlanmıştır. Literatür analizi sonucunda, siber saldırılar ve siber güvenlik denetimleri konusunda bütüncül bir denetim modeli önerisi yapılmıştır.

Yanar (2014) güvenlik ve gizlilik sorunlarından dolayı firma dışı bulut depolama sistemlerini kullanmak istemeyen kurumlar için FileStream teknolojisi ile şirketlerin kendi ihtiyaçlarına uygun bulut depolama çözümü geliştirebileceklerini iddia etmiştir. Bilgiyi diğer kurum ve kuruluşlarla paylaşmadan firma bünyesinde bulunan veri merkezlerinde depolayan, firmaların güvenlik duvarı ile korunan şirkete özel bir bulut sisteminin oluşturulması ele alınmıştır. Küçük boyutlu dosyalarda FileStream teknolojisinin çalışma problemleri yaşadığı ve hibrit bir modelin geliştirilmesi gerektiği üzerinde durulmuştur.

Karabacak (2011) kritik altyapıların ülkedeki sistemin işleyişine olan etkisini ve kritik altyapıların korunması amacıyla yapılması gerekenler üzerine literatür analizi yapmıştır. Türkiye'de kritik altyapılar konusunda uygulanan yasal herhangi bir mevzuatın bulunmadığı tespit edilmiş, bu durumunda siber güvenlik konusunda gelecekte büyük bir sorun yaşanabileceği ifade edilmiştir. Ülkemizde kritik altyapıya ilişkin gerçekleştirilen siber güvenlik önlemleri ve ülkemizin kritik altyapı sorunu ve gelecekte olası yaşanabilecek siber tehditler irdelenmiştir. Dünyada gelişmiş birçok ülkenin kritik altyapı konusunda gerek teknik boyutta gerekse yasal mevzuat olarak mesafe aldıkları belirtmiştir.

Yıldırım (2018) tarafından dünyadaki birtakım ülkelerdeki değişik kurumlar tarafından hazırlanmış olan siber güvenlik raporları ve bu konuda yapılan siber güvenlik anketleri analiz edilmiştir. Siber tehditler ve bu konuda neler yapıldığı, güvenlik riskleri, güvenlik zafiyetleri analiz edilmiş, alınması gereken önlemler ve farkındalık konusunda öneriler anlatılmıştır.

Erdem ve Özocak (2019) tarafından siber güvenliğin sağlanmasında uluslararası hukuk ve Türk hukukunun etkisinin ne olduğu ve siber güvenlik konusunda devletin ne gibi önlemler alması gerektiğini araştırılmıştır. Literatür analizi sonucunda, siber güvenlik sorununun sadece bilişim sistemini kullanan bireyin güvenlik sorunu olmaktan öte, ulusal ve uluslararası bir sorun olduğu, bu nedenle, siber güvenliğin kamuda, özel sektörde ve toplumun tüm kesimlerinde düzenli ve aksamadan yürütülebilmesi ve bilişim sistemini kullanan tüm bireylerin kullandıkları bilişim sistemlerinde siber güvenliğinin sağlanması noktasında gerek ulusal hukuk gerekse uluslararası hukuk düzeninin etkisinin çok büyük

olduğu vurgulanmıştır. Dolasıyla ülkemizde ve dünyada siber güvenliğin sağlanması konusunda ulusal hukuk ve uluslararası hukuka çok büyük görevler düştüğü ifade edilmiştir.

Yılmaz ve Sağıroğlu (2013) siber güvenlik ile ilgili yapılması gereken hususlar, uyulması gereken kurallar, öneriler, siber tehdit durumunda yapılması gerekenler, risk analizi, siber tehdit konusunda bireylerin bu duruma hazırlık düzeylerinin hangi boyutta olduğunu konularını incelemiştir. Literatür analizi sonucunda, siber güvenlik konusunda bireyleri ve toplumu siber suçları işleyerek tehdit edebilecek araçlar, siber tehdit seviyeleri, siber hazırlık seviyeleri, saldırgan tipleri, siber saldırı düzenleyenlerin hedef ve amaçları, uyguladıkları yöntemler ve çözüm önerileri ile ilgili bilgiler sunulmuştur.

Arslan (2018) siber suçlar, siber suç türleri, siber güvenlik ve bilişim dünyasında siber güvenlik konusunda yapılması gereken hususlar ve siber saldırı türleri konularını incelemiştir. Literatür analizi sonucunda, siber saldırı türlerinin "Sniffing, Hizmet dışı bırakma (Denial of service) IP aldatması, Sosyal mühendislik, SQL enjeksiyonu, Arka kapılar, Oltalama (Phishing), Casus yazılım (Spyware), Virüsler, Truva atları, Solucanlar (Worms), Bot, Zombi ordular (Botnetler), Bukalemun, Klavye işlemlerini kaydeden programlar (Keyloggers)" olduğu ifade edilmiştir (Arslan, 2018). Ayrıca bu çalışmada siber suçlarla mücadele konusunda alınması gerekli tedbirler ve mücadele yolları izah edilmiştir.

Aslay (2017) Türkiye'de siber güvenlik açıklarını analiz etmiştir. Literatür analizi sonucunda, bilgisayar ve internet üzerinden çok farklı türde siber saldırıların gerçekleştirildiği, bilgisayar ve internet kullanıcılarının bu saldırılar konusunda yetersiz kaldıkları ifade edilmiş ve Türkiye'de siber güvenlik konusunda alınması gereken tedbirler anlatmıştır. Ayrıca siber güvenlik konusunda hukuki mevzuatın ve yasal düzenlemelerin de yetersiz kaldığını ifade edilmiştir.

Hekim ve Başıbüyük (2013) yaptıkları literatür analizi sonucunda Türkiye'de bilişim sistemleri ve internetin hızla geliştiği, toplumun bireylerinin internete olan bağımlılığının arttığı tespit etmiştir. Türkiye'de yaşanan siber suçlar ve alınması gereken güvenlik önlemleri üzerinde durulmuştur. Çalışma sonunda, bilişim dünyasında yaşanan siber tehdit şekillerini ölçüp bu konuda strateji geliştirmek için birtakım yeni birimlere ihtiyaç olduğu ifade edilmiştir. Siber güvenlik hususunun sadece internet güvenliği olmayıp bütün iletişim birimlerini kapsayan bir kavram olduğu belirtilmiştir. Ülkemizde kamu kurumlarında ve özel

sektörde bilişim sistemlerinde yaşanabilecek olası siber saldırıları önlemek için siber güvenlik konularında ileri boyutta siber güvenlik tedbirleri alınması için hukuki altyapının da hazırlanması gerektiği, Türk Ceza Kanunu (TCK) ve Ceza Muhakemeleri Kanununda (CMK) siber suçlarla mücadele konusunda gerekli hukuki mevzuatın yapılması ve yasaların düzenlenmesinin gerektiği ifade edilmiştir.

Ünver ve Canbay (2010) bilişim dünyasında siber saldırıların engellenmesi için gerekli yasal mevzuatın ve kanuni düzenlemelerin güncellenerek günlük hayatta işe koşulması gerektiğini ifade etmektedir. Ayrıca siber güvenlik kapsamında oluşturulacak yasal düzenlemeler noktasında ülkeyi yöneten siyasilere görevler düştüğü ifade edilmiştir. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Ocak 2013 tarihinde bilişim sistemlerine yönelik siber saldırıları önlemek amacıyla ve bilişim ortamında yaşanabilecek siber saldırılara müdahale etmek amacıyla Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı yayınlamıştır.

Bu planda bilgi ve iletişim sistemlerine yönelik saldırıların dünyanın her tarafından yapılabileceği, siber saldırıları yapan kişilerin kim olduğunun belirlenmesinin zor olduğu, siber saldırı düzenleyen saldırganların saldırı için gerekli araç ve gereçlerinin bilgi çağında ucuz ve kolayca elde etmesinin mümkün olduğu, ayrıca bu siber saldırıyı gerçekleştiren kişi veya kişilere dünyanın başka bir yerinden birçok kişinin bu saldırganlara ortak olup toplu halde başka bir ülkeye veya bölgeye siber saldırı girişiminde bulunabilecekleri ifade edilmektedir. Lakin kamu kurum ve kuruluşlarında bilgi güvenliği konusunda gerekli alt yapılarının yetersiz olduğu, birçok kurumda çalışan personelin siber güvenlik konusunda yeterli bilgi düzeyinde olmadığı, kurumlardaki siber güvenlik olaylarının sadece bilgi işlem birimlerinin sorumluluğuna bırakıldığı, bilgi işlem birimlerinde çalışan personelin de yeterli düzeyde siber güvenlik konusunda bilgiye sahip olmadığı belirtilmiştir (UDHB, 2013).

Siber Güvenlik Üzerine Yapılan Yurt Dışı Çalışmalar

Halevi ve diğerleri (2016) kullanıcıların siber güvenliğini arttırmak amacıyla siber güvenlik ile kültürel, psikolojik ve demografik değişkenler arasındaki ilişkiyi incelemiştir. Literatür analizi sonucunda dünyada siber güvenliğin artmasına bağlı olarak beraberinde güvenlik uzmanlarının birtakım zorluklarla karşılaşacaklarını belirtmiştir. Bu çalışma Amerika Birleşik Devletleri, Hindistan, Birleşik Arap Emirlikleri ve Gana isimli dört farklı ülkede gerçekleştirilmiştir. Siber güvenliğe çok kültürlü bir bakış sunmaktadır. Çalışmanın sonunda kültürler arası araştırmanın farklı ülkelerin siber güvenlikle ilgili benzer endişe ve sıkıntılar yaşadığını göstermiştir.

Giri (2019) Nepal'de siber suç, siber tehdit, siber güvenlik stratejileri ve siber hukuku araştırmıştır. Bu çalışmada içerik analizi ve anket yöntemi kullanılmıştır. Literatür analizi sonucunda Nepal ülkesindeki hükümetin siber suç, siber tehdit, siber güvenlik ve siber stratejiler konusunda profesyonel bir analiz yapması gerektiğini, ayrıca siber güvenliğin yasal gerekliliklerini araştırmıştır. İnsanların hayatını güvence altına alan sistemlerin tasarlanması gerektiğini, mevcut kullanılan çözümlerin siber güvenlik konusunda yeterli olmadığını, gelecekte gerekli önlemlerin alınmadığı takdirde bireylerin siber tehditler ve saldırılar sonucu daha olumsuz sonuçlara maruz kalacaklarını belirtmiştir. Bireylerde ortaya çıkan siber güvensizlik nedeniyle insanların mutlu ve sağlıklı olamayacaklarını açıklamıştır.

Abomhara ve Koien (2015) siber güvenlik, nesnelerin interneti, güvenlik açıkları, siber IoT altyapısına yönelik tehditler ve siber saldırıları incelemiştir. Literatür analizi sonucunda dünyada IT cihazlarına ve hizmetlerine yönelik tehditlerin ve saldırıların arttığını, siber saldırıların IT cihazlarına karşı eskiden beri gerçekleştirildiğini, IT cihazlarına karşı gerekli siber güvenlik önlemlerinin alınması gerektiğini belirtmiştir. Ayrıca IT cihazlarına karşı yapılan siber saldırıları analiz etmiştir. Özellikle IT cihazlarındaki güvenlik sorunlarına odaklanarak güvenlik sorunu olarak ortaya çıkan gizlilik, mahremiyet ve varlık gibi güvenlik sorunlarını tespit ettiklerini açıklamışlardır.

Collier (2018) siber güvenlik birimleri, siber güvenliğin sağlanması konusunu dinamik ve tartışmalı boyutlarda ele alıp incelemiştir. Literatür analizi sonucunda Siber güvenlik aktörlerinin karmaşık halini anlamak için en iyi yöntemin uygulamalar ve güvenlik araştırmalarında ve uluslararası alanda kullanılan geleneksel kamu-özel ve küresel-yerel

ayrımlarına uymamak olduğunu ifade etmiştir. Bu çalışmada siber güvenlik gruplarının nasıl geliştiğine dair farkı bir model önerilmiştir. Ayrıca siber güvenlik aktörlerinin konfigürasyonu ve aralarındaki ilişkilerin sürekli olması, siber güvenlik kavramının dinamik yapısını ve doğasını anlamak için bir kullanıcılara bir araç sağladığı hususları anlatılmıştır.

Dunn Cavelty ve Wenger (2020) siber güvenliğin güvenlik politikası ile buluştuğunu, karmaşık teknolojinin, siyasetin ve ağ bağlantılı bilimin geçmiş on yıl içerisinde siber olayların daha da çoğaldığı ve teknolojik hayatı zorlaştırdığı, siber güvenlik politikalarını bilimsel olarak ele alıp incelemiştir. Literatür analizi sonucunda siber güvenliğin evriminde etkili olan bilim siyasetin nasıl çalıştığı hususlarını anlatmıştır. Siber güvenlik araştırmaları ve siber güvenlik politikasının teknoloji ile etkileşimi sonucu gelecekte bilimin ve siyasetin yeniden şekillenmeye devam edeceğini belirtmiştir.

Humayun, Niazi, Jhanjhi, Alshayeb ve Mahmood (2020) siber güvenlik tehditleri ve güvenlik açıklarını inceleyerek ortak siber güvenliği belirlemeyi hedeflemiş ve siber güvenlik tehditlerini analiz etmiştir. Literatür analizi sonucunda siber güvenlik tehditlerinden kimlik avı, hizmet reddi ve kötü amaçlı yazılımlar gibi güvenlik açıklarının bu araştırmadaki seçilen çalışmalarının çoğunun yalnızca birkaç ortak güvenliği hedeflediğini gösterdiğini açıklamıştır. Gelecekte buna benzer siber güvenlik açıkları ile ilgili çalışmalar yapılması gerektiğini, gelecekte yapılacak araştırmalarda, anahtar siber güvenlik açıkları, hedeflenen uygulamalar, azaltma teknikleri ve altyapıları konularında yapılmasının daha uygun olacağını belirtmiştir. Böylece araştırmacılar ve uygulayıcıların siber güvenlik açıkları hakkında daha detaylı ve geniş bilgi sahibi olacaklarını belirtmiştir.

Cole ve diğerleri (2008) Afrika uluslarının siber güvenlik alanındaki yaptıkları eylemleri ve çalışmaları incelemiştir. Ulusal güvenliğin siber güvenlik için bir motivasyon olabileceğini düşünerek olaya bu şekilde yaklaşmıştır. Literatür analizi sonucunda Afrika ülkesinin dünyada gelişmiş ve gelişmekte ülkelere nazaran her anlamda az gelişmiş ülke olarak görüldüğü bu bakımdan Afrika ülkesinde siber güvenlik alanında yapılan çalışmalar ve uygulamalar incelendiğinde Afrika ülkesinde siber güvenlik alanında yapılan fazla bir çalışmanın ve uygulamanın olmadığını, bu kıtada siber güvenliğe daha fazla yatırım yapılması gerektiğini, siber güvenliğin ulusal güvenlikten daha sıkıntılı ve endişe edilecek bir durumda olduğunu gözlemlediklerini belirtmiştir. Afrika'da yalnızca birkaç önemli siber

güvenlik girişiminin olduğunu, Afrika'nın siber güvenlik konusunu ele alıp siber güvenliğe yatırım yapmasının gerektiğini, bu sayede Afrika kıtasını, bu kıtadaki ülkelerin altyapısını ve bu kıtada yaşayan bireyleri siber tehditlere ve saldırılara maruz kalmaktan kurtaracağını sonuçta Afrika kıtasının kimliğinin de dünya genelinde küresel ölçekte güçlü bir noktaya taşıyabileceği açıklanmıştır.

Howard (2018) çalışanların siber güvenlik tutumlarını ölçmek için siber güvenlik tutumları ölçeği geliştirmiş ve siber güvenlik davranışının modellenmesini incelemiştir. Literatür analizi sonucunda geliştirilen siber güvenlik tutumları ölçeği iyi psikometrik özelliklere sahip bir ölçek olduğu görülmüştür. Geliştirilen bu ölçeğin siber politika uyumu tutumları ve siber saldırı isimli iki faktörü ölçtüğü anlaşılmıştır. Bu çalışmanın ikinci aşaması olarak da planlı davranış teorisini bir kişilik yönleri arasındaki ilişkiyi modellemek için teorik çerçeve, politika uyumu tutumlar, algılanan güvenlik açığı, kontrol odağı, siber güvenlik iklimi ve siber güvenlik davranışlar olduğu anlaşılmıştır. Ayrıca bu çalışma sonunda siber politikaya bağlılık tutumları arasında güçlü iki değişkenli bir ilişki olduğu bulunmuştur.

Von Solms ve Van Niekerk (2013) bilgi güvenliği ile siber güvenlik arasındaki farkı, bilgi güvenliği ile siber güvenlik kavramlarının birlikte kullanılmasının nedenlerini incelemiştir. Literatür analizi sonucunda siber güvenlik ve bilgi güvenliği arasında benzerlik bulunmasına rağmen bu iki kavramın birbiriyle tamamen aynı olmadığını belirtmiştir. Siber güvenliğin geleneksel bilgi güvenliğinin sınırlarından daha ileride olduğunu, yalnızca bilgi kaynaklarının değil diğer varlıkların da korunmasını içerdiğini ifade etmiştir. Bilgi güvenliğinde insan faktörüne referans olarak genellikle güvenlik sürecinde insanların rolleriyle ilgili olduğu, siber güvenlikte ise bu faktörün siber saldırıların hedefi olan insanlar veya farkında olmadan siber saldırıya uğrayan kişiler olduğunu belirtmiştir. Ayrıca bilgi güvenliği bilginin korunması, bilginin tehditlerden kaynaklanan meydana gelebilecek zararlardan ve güvenlik açıklarından korunması olarak ifade edilmektedir. Siber güvenlik ise, siber alanın korunması, siber uzayda çalışanların ve varlıkların korunması olarak açıklanmıştır.

Dhawan, Gupta ve Elango (2020) 1998-2019 yılları arasında yayınlanan küresel siber güvenlik araştırmasını analiz etmiştir. Scopus veri tabanından elde edilen 10.607 yayından oluşmaktadır. Toplamda 117 ülkenin siber güvenlik araştırmalarına katılmıştır. En üretken ilk üç ülke Amerika Birleşik Devletleri (%43,75 pay), Birleşik Krallık (%7,73 pay) ve Çin (%5,33 pay)'den oluşmaktadır. Literatür analizi sonucunda siber güvenlik araştırmalarının hızla gelişen küresel bir alan olduğunu anlaşılmaktadır. Siber güvenlik araştırma çalışmalarındaki büyümenin en önemli nedenlerinden birisi ulusal güvenlik, ekonomik kalkınma, hassas verilerle ilgili konuları içerir koruma, sistem operasyonlarına ve korumaya yönelik iç ve dış tehditler olduğunu belirtmiştir. Siber güvenliğin dağılımı ülkeden ülkeye farklılık göstermektedir. Amerika Birleşik Devletleri siber güvenlikte dünyanın lideri konumundadır. Siber güvenlik alanında %43,75'lik dünyada hakimiyeti bulunmaktadır. ABD'nin siber güvenlikte en zirvede bulunmasının nedeni kişi başına düşen bilgisayarların daha fazla endüstriyel, ticari ve askeri kullanımı diğer ülkelere göre daha yüksek bir seviyede ekonomik dijitalleşmesine sahip ölçeği veya daha yüksek bir siber suç oranı veya daha yüksek siber suç kaynaklarının olması şeklinde açıklanmaktadır. Hindistan, küresel payın %4,34'ü ile araştırma üretkenliği açısından dördüncü sırada yer aldığı, siber güvenlik araştırmaları alanında merkezini geliştirmesi gerektiği, bu amaçla altyapı geliştirme, insan gücü geliştirme ve yetenek keşiflerine daha fazla odaklanmak zorunla olduğu belirtilmiştir.

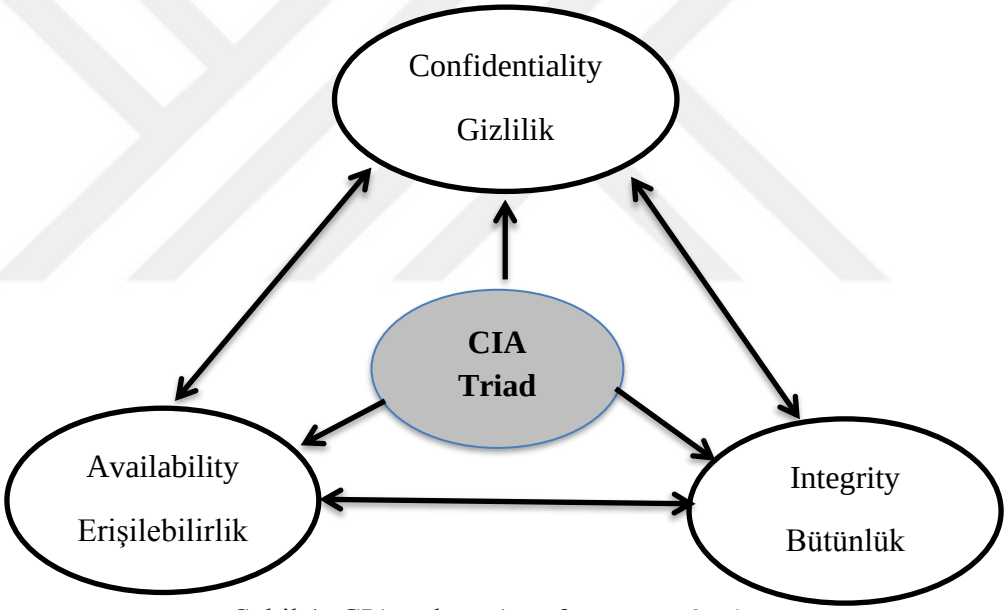
Baheti ve Gill (2011) siber fiziksel sistemleri incelemiştir. Literatür analizi sonucunda siber-fiziksel sistemler terimi, birçok yeni yöntem aracılığıyla insanlarla etkileşime girebilen entegre hesaplama ve fiziksel yeteneklere sahip yeni nesil sistemleri ifade ettiğini belirtmiştir. Siber fiziksel yöntemler kullanılarak yapılan hesaplama, iletişim ve kontrol yoluyla fiziksel dünya ile etkileşim kurma ve yeteneklerini genişletme yeteneği, gelecekteki teknolojik gelişmeler için önemli bir kolaylık sağladığını belirtmiştir. Siber-fiziksel sistemler araştırması, bilgi ve mühendislik ilkelerini hesaplama ve mühendislik disiplinleri arasında entegre etmeyi amaçladığını belirtmiştir. Ayrıca siber-fiziksel sistemlerin günümüzdeki özerklik, işlevsellik, kullanılabilirlik, güvenilirlik ve siber güvenlik düzeylerinin üzerinde yeni yeteneklerle gelecekteki mühendislik sistemlerinin tasarımında ve geliştirilmesine büyük pay sahibi olacağını ifade etmiştir.

Shafqat ve Masood (2016) yapmış oldukları çalışma ile Avusturya, Avustralya, Kanada, Çek Cumhuriyeti, Estonya, Fransa, Finlandiya, Almanya, İran, Hindistan, İsrail, Japonya, Malezya, Yeni Zelanda, Hollanda, Suudi Arabistan, İspanya, Türkiye, İngiltere ve Amerika Birleşik Devletleri dahil olmak üzere dünyanın farklı bölgelerinden yirmi ülkenin Ulusal Siber Güvenlik Stratejilerini analiz ederek değerlendirmiştir. Literatür analizi sonucunda ülkelerin siber güvenlik stratejileri incelendiğinde ulusal boyutta siber güvenlik işlemlerini yönetmek için resmi bir kurumun oluşturulması, ulusal siber uzayı hedef alan siber saldırılara karşı mücadele etmek için Bilgisayar Acil Durum Müdahale Ekiplerinin (CERT/CSIRT) kurulmasının gerektiğini belirtmiştir. Ayrıca siber güvenlik stratejileri incelenen ülkelerin siber güvenlik farkındalık programları yürüttükleri, ancak her ülkenin yürüttüğü siber güvenlik farkındalığının diğer ülkeden farklı olduğunu belirtmiştir. Bu araştırma sonunda özellikle Amerika Birleşik Devletleri, İngiltere ve Almanya'nın siber güvenlik stratejilerinin, eylem planlarının geliştirilmesi ve uygulanması noktasında diğer ülkelere göre daha iyi konumda olduğunu açıklamıştır.

Mulligan ve Schneider (2011) Siber güvenlik yapılan önceki doktrinlerin başarısızlıklarını tartışarak yeni bir doktrin olan kamu siber güvenliğinin sağlığı yöntem ile siber güvenlik konusunu incelemiştir. Literatür analizi sonucunda hükümetlerin, özel işletmelerin siber güvenlik konusunda daha fazla endişe duyduklarını, her geçen gün basın yayın organlarında siber saldırılar sonucu birçok insanın siber mağduriyet yaşadığı anlatılmaktadır. İnternette bilgisayar kullanıcılarının şifrelerinin çalındığı, büyük ölçekli firmaların müşterilerine ait kurumsal müşterilerinin kişisel bilgilerinin ele geçirildiği, web sitelerine yönelik saldırıların gerçekleştirildiği, sivil kritik altyapılar üzerine siber saldırılar gerçekleştirildiği anlatılmıştır. Bilgi çağında yetersiz siber güvenlik önlemlerinin başarıya en büyük engellerden biri olduğunu belirtmiştir. Bu nedenle hükümetlerin teknolojide çözüm politikaları üretmeleri gerektiği, bireylerin özel tercihlerinde müdahale gerektirdiği, kamu siber güvenliği konusunda topluma yeniden yön verecek uygun olan politika ve eylemleri gerçekleştirilerek siber güvenlik konusunda kamu yararını gözeterek güvensizliği ortadan kaldırmayı hedeflemek gerektiğini ifade etmiştir.

Bilgi Güvenliği Üçlüsü

Bilgi güvenliği, bilginin dijital ortamda saklanıp saklanmadığı araştırmaz. Bilgileri elektronik ortamda yetkisiz kişilerin erişmesine, sanal ortamda başkalarının istenmeyen kişilerin izin kullanımına, bilginin bozulmasına, değiştirilmesine, muhafaza edilmesine veya bilginin yok edilmesine karşı korumakla görevlidir. Bilişim sistemlerinde bilgi güvenliğinin sağlanması için gereken unsurlar gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) olarak ifade edilmektedir (Kurt Kara, 2017). Bilgi güvenliği üçlüsü olan gizlilik, bütünlük ve erişilebilirlik şekil 1'de gösterilmiştir.



Şekil 1: CIA üçlüsü (Pender-Bey, 2012).

Parker Altılısı Modeli

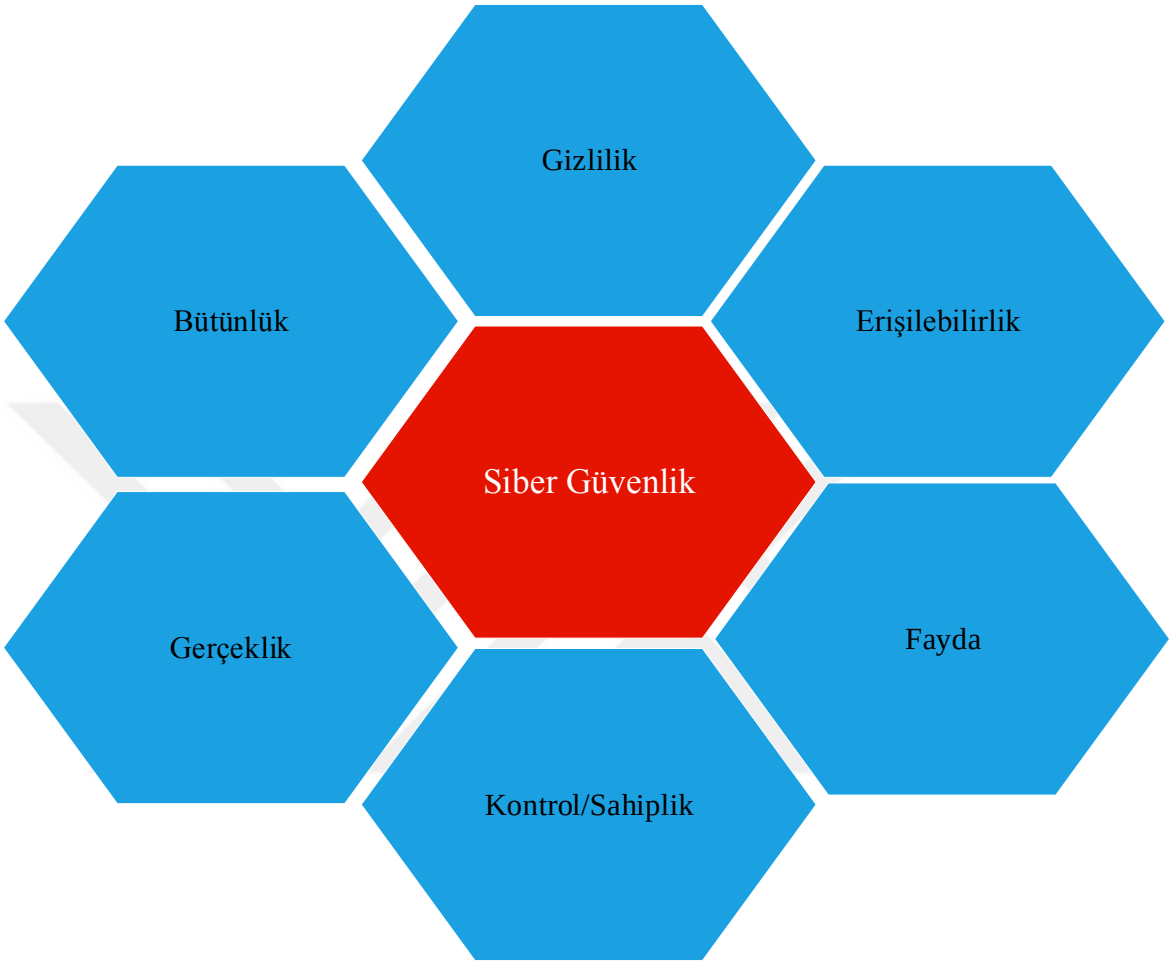
Gizlilik, bütünlük ve erişilebilirlik (CIA) bilgi güvenliği modelinin güncellenmesi ile ortaya çıkan Parker Altılısı modelidir. CIA üçlüsü, bazı kritik siber güvenlik özelliklerini göz ardı ettiği için yetersiz olarak görülmektedir. Buna göre Parker (1992), CIA üçlüsüne dayanan Parker altılısı (PH) adı verilen geliştirilmiş bir model önermiştir. PH, üç kritik özellik daha ekleyerek daha kapsamlı bir model sunarak CIA üçlüsünü geliştirir (gerçeklik, kontrol/sahiplik ve fayda). Günümüze kadar mevcut koşullarda "Bilgi güvenliği Üçlüsü" temel olarak kullanıcıların güvenlik ihtiyaçlarını yeterince cevaplar vermiş olsa da, zaman

içerisinde kullanıcıların bilgi güvenliği ile ilgili birtakım ihtiyaçları ve sorunları doğmuş, ve Bilgi Güvenliği Üçlüsünün sadece teknolojik boyutta olduğu, bilgi güvenliğini insan boyutunda değerlendirecek, insan odaklı birtakım kavramlara ihtiyaç duyulmuş, ayrıca insanın bilgi güvenliği açısından en büyük tehdit unsurlarından biri olduğu da bilindiğinden bu konu üzerinde daha kapsamlı bir çalışmanın gerekli olduğu anlaşılmıştır. Bu nedenle Donn B. Parker tarafından 1988 yılında Parker altılısı olarak yeni bir model oluşturulmuştur. Parker altılısı olarak ifade edilen bu modelde Bilgi Güvenliği üçlüsü olan Gizlilik, Bütünlük, Erişebilirlik kavramlarının üzerine, Gerçeklik, Sahiplik/Kontrol ve Fayda (Yararlılık) kavramlarından oluşan Parker altılısı adında yeni bir model oluşturulmuştur. Parter Altılısı olarak ifade edilen bu model Bilgi Güvenliği Üçlüsünün üzerine oluşturulmuş bir uygulamadır. Fakat bilgi güvenliğini daha detaylı bir biçimde incelemektedir. Parker altılısının en önemli özelliklerinden biri de bilgi güvenliğinde yaşanabilecek olası tehditlere karşı kullanıcılara koruma kalkanı oluşturup, kimlik doğrulama ve şifreleme gibi kavramlar üzerinde durmaktadır (Kurt Kaya, 2017). Parker altılısı modeli altı boyutlu bir yapıya sahiptir (Şekil 2) Tablo 1 altı boyutun tanımlarını göstermektedir.

Tablo 1. SGÖ'nün altı alt boyutu

Alt Boyutlar	Tanım
Erişilebilirlik	"Erişilebilirlik, yetkili kullanıcı kişilerin veya bilgisayar sistemlerinin herhangi bir müdahale veya engelle karşılaşmadan bilgileri erişmesini ve bilginin gerekli format ile alınmasına izin verir" (Whitman & Mattord, 2011, s. 12).
Gerçeklik	"Bilginin özgünlüğü, yeninden üretilen veya sahte değil gerçek ve orijinal kalitedeki bilgi veya bilgi durumdur" (Whitman & Mattord, 2011, p. 12).
Gizlilik	"Bilgi, yetkisiz bireylere veya sistemlere maruz kalmaya karşı korunduğunda bilginin gizliliği vardır" (Whitman & Mattord, 2011, s. 13).
Bütünlük	"Bilgi bütün, tam ve bozulmamış olduğunda bütünlüğe sahiptir" (Whitman & Mattord, 2011, s. 13).
Kontrol/Sahiplik	"Bilginin sahipliği, kontrol veya sahiplik durumu veya kalitesidir" (Whitman & Mattord, 2011, s. 15).
Fayda	"Bilginin faydası, amaç veya durum için değere sahip olma durumu veya kalitesidir" (Whitman & Mattord, 2011, s. 15).

Parker Altılısı modelinin altı boyutlu yapısı aşağıda Şekil 2'de gösterilmektedir.



Şekil 2: Parker Altılısı (Parkerian Hexad)

Gizlilik

Gizlilik, bütünlük ve erişilebilirlik üçlüsü (CIA-triad) hassas bilgi özelliklerine odaklanan temel güvenlik çerçevesidir. Bu özellik aynı zamanda siber güvenliğin en kritik yönü olarak ele alınmıştır. Örneğin gizlilik "bilgilere erişimi sınırlayan kurallar seti" olarak tanımlanmıştır (Li, Meng, ve Kwok,2016). Gizli bilginin yetkisiz bireylere veya sistemlere karşı açılmasını korumayı ifade eder (Von Solms ve Van Niekerk, 2013). Bilginin yetkisiz kişilere, tüzel kişiliklere veya süreçlere sunulmadığı veya ifşa edilmediği mülkiyeti ifade eder. Verileriniz gizli değilse güvenli değildir. Her birey veya kuruluş, yalnızca belirli kişilerin buna erişmesine izin verilmesi gereken bir tür hassas bilgiye sahiptir. Gizlilik bilişim sistemine ve verilerine sadece yetkili kişi veya sistemlerce erişilebilmesini; bilişim

sistemlerindeki gizli verinin yetkisiz kişi veya sistemlerce ifşa edilmemesi olarak da ifade edilmektedir.

Gizlilik bilgiye yetkisiz kişilerin erişememesi, ulaşamaması olarak da ifade edilmektedir. Gizlilik kavramı veri gizliliği ve mahremiyet olarak iki boyutta incelenmektedir. Vergi gizliliği olarak ifade edilmek istenen husus gizli bilginin bilgiye erişimi olmayan yetkisiz kişilerce ulaşılamadığından dolayı verinin başkalarının eline geçmediğini, başka kişi veya kişiler tarafından verilere sahip olunamadığını elde edilemediğini, verilerin kesin olarak güvende olduğunu belirten bir kavramdır. Mahremiyet ise kişilerin kendilerine has olan özel bilgilere kimlerin ulaşıp ulaşamayacağını ifade eden bir olgudur (Kurt Kaya, 2017).

Bütünlük

Bütünlük bilişim sistemlerinin ve bilginin sadece yetkili kişilerce veya sistemlerce değiştirilebilmesi olarak ifade edilmektedir. Bütünlük verilerin doğruluğu, tutarlılığı ve güvenilirliği ile ilişkilidir. "Bilginin yetkisiz taraflarca değiştirilmesini önlemek" olarak tanımlanır (Li vd. 2016, p. 131). Bütünlük aynı zamanda bilginin istenmeyen veya yetkisiz şekilde değiştirilmesini önleme yeteneğini de ifade eder (Andress, 2014). Bütünlük "bilginin yetkisiz kişilerce değiştirilmemesi, silinmemesi veya herhangi bir şekilde zarar görmesine sebep olacak saldırılardan korunuyor olması" anlamına gelmektedir (Kurt Kaya, 2017).

Erişilebilirlik

Erişilebilirlik, "yetkili tarafların istenilen durumlarda anahtarlara ve ilgili bilgilere erişebilmesi" olarak tanımlanır (Li vd. 2016, p. 131). İstenildiği zaman bilgilere erişim yeteneğini ifade eder (Reid ve Van Niekerk, 2014). Erişilebilirlik, Yetkili kişilerin ve işlemlerin ihtiyaç duyulan zaman içerisinde ve ihtiyaç duyulan kalitede bilişim sistemlerine ve bilgiye erişebilmesi olarak ifade edilmektedir. Kullanıcının ihtiyacı olduğu anda istediği an bilgiye ulaşabilmesi, kullanıcının bilgiyi elde edebilmesi için bilginin sürekli erişime açık olması durumu olarak adlandırılmaktadır. Ayrıca kullanıcının erişim yetkisi olduğu halde sistemde herhangi bir teknik arıza veya sorun oluşması durumunda dahi kullanıcının bu bilgiye erişim sağlayabilmelidir.

Gerçeklik

Gerçeklik, bilgi işlemlerinin orijinal kaynaktan geldiğine dair verilen garantiyi ifade eder (Von Solms ve Van Niekerk, 2013). Gerçeklik; doğru olma, gerçekçi olma, sistemin güvenilir olması, verilerin güvenilir, doğru orijinal bir kaynaktan geldiğini ifade eden bir kavramdır. Mesaj gönderen kişinin doğru olup olmadığına, mesajın geçerliliğine karşı güvenin sağlanması noktasında önemli ve gerekli olan bir husustur. Ayrıca kullanıcılar veya başka kişiler tarafından sisteme yapılan girişlerin doğru ve güvenilir bir kaynaktan yapıldığını teyit etme yani doğrulama olarak ifade edilmektedir (Pender-Bey, 2012).

Kontrol/Sahiplik

Kontrol/sahiplik ise gizli bilginin kontrol kalitesi veya sahiplik durumunu ifade eder. Sahiplik/Kontrol, gizli bilginin başka kullanıcılar tarafından kopyalanmasının ve yetkisiz olan kişilerce kullanımının engellenmesi olarak adlandırılmaktadır (Kabay, Whyne, Eric 2009).

Fayda

Fayda bilginin ve hizmetlerin bireye sağladığı yararları ifade eder. Fayda, amaca uygunluk veya kullanışlılık olarak da ifade edilmektedir.

BÖLÜM III

YÖNTEM VE BULGULAR

Bu çalışma, nicel ve nitel araştırma yöntemlerinin birlikte kullanıldığı karma desen kategorisinde yer alan bir ölçek geliştirme çalışmasıdır. Bu çalışmada nitel araştırma boyutunda odak grup görüşmesi kullanılmıştır. Araştırmanın odaklandığı konuya ilişkin birden fazla uzman bir araya gelinerek odak grup görüşmesi gerçekleştirilmiştir. Böylelikle, madde havuzu ve nihai ölçek formunun oluşturulmasında alan uzmanlarından istifade edilmiştir. Oluşturulan bu ölçek formu örneklem grubuna uygulanmıştır. Bu çalışmanın örneklemi bilgisayar ve interneti kullanan üniversite öğrencileridir. Ölçek geliştirme çalışmasının nicel boyutunda toplanan veriler kullanılarak birtakım analizler yapılmıştır. Bu analizler geçerlik, güvenirlik, Cronbach Alpha güvenirlik katsayısı hesaplamaları, Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizi (DFA) analizleridir. Bu ölçek geliştirme çalışmasında öncelikle kapsamlı bir literatür taraması yapılarak madde havuzu oluşturulmuştur. Maddeler tasarlanırken bir maddenin tek bir düşünceyi ölçmesine dikkat edilmiştir. Oluşturulacak madde havuzunun görünüş geçerliliği için üç alan uzmanının değerlendirmesine başvurulmuştur. Uzmanlar soruların değiştirilmesi ya da çıkarılması önerisinde bulunmuştur. Uzman görüşüne göre nihai halini alan ölçek taslağı ilk çalışmada 380 kişiden oluşan örneklem grubuna uygulanmıştır. Ölçeğin geçerlik ve güvenirlik analizleri yapılarak son hali verilmiştir. Güvenirlik için Cronbach Alfa Güvenirlik Katsayısı kullanılmıştır. Ölçek maddelerinin belirlenen alt boyutları ne derece doğru ölçtüğü ise açımlayıcı faktör analizi yapılarak tespit edilmiştir. Alt boyutları belirlenen ölçek, 613 kişiden oluşan farklı bir örneklem grubuna uygulanmıştır. SPSS AMOS yazılımı kullanılarak doğrulayıcı faktör analizi yapılmış ve yapısal eşitlik modellemesi ile ölçeğin içerdiği alt boyutlar arasındaki ilişki ortaya çıkarılmıştır.

Çalışma 1

Evren ve Örneklem

Bu araştırmanın evrenini teknolojik bir cihaz (bilgisayar, akıllı telefon, tablet gibi) ve internet kullanan üniversite öğrencilerinden oluşturmaktadır. İlk çalışmanın örneklemini Tokat Gaziosmanpaşa Üniversitesinde öğrenim gören 380 üniversite öğrencisi oluşturmaktadır. Katılımcılar kolayda örnekleme yöntemi ile seçilmiştir. İlk çalışma ortalama yaşı 21,22 (SS=2,33, 18-38 yaş arasında) olan 239 kadın ve 141 erkek katılımcıdan oluşmaktadır.

Tablo 2. Ölçeğin uygulandığı 1. çalışma grubundaki öğrencilerin demografik bilgileri

Cinsiyet	Frekans	Yüzde (%)
Kadın	239	62,9
Erkek	141	37,1
Toplam	380	100
İnternet Kullanım Süreniz		
1-2 Saat	65	17,1
3-4 Saat	178	46,8
5-7 Saat	95	25,0
8 Saat ve üzeri	42	11,1
Toplam	380	100
Mobil Cihazınızda İnternet var mı		
Evet	376	98,9
Hayır	3	1,1
Toplam	380	100

İnternet kullanım amacı		
İnternet/mobil bankacılık hizmetini kullanırım	334	87,9
E-devlet hizmetlerini kullanırım	250	65,8
E-ticaret siteleri üzerinden internet alışverişi yaparım	207	54,5
Kullanmıyorum ve kullanmayı düşünmüyorum	9	2,4

Tablo 2 incelendiğinde ilk çalışma ortalama yaşı 21,22 (SS=2,33, 18-38 yaş arasında) olan 380 katılımcıdan oluşmaktadır (239 kadın ve 141 erkek). 380 katılımcıdan oluşan 1. çalışma grubunun %62,9'unun kadın, %37,1'inin ise erkek olduğu görülmektedir. Çalışmaya gönüllü olarak katılımcılar devlet üniversitelerinde okuyan lisans öğrencileridir. Katılımcıların %17,1'i günde 1-2 saat, %46,8'i günde 3-4 saat, %25,0'i günde 5-7 saat ve %11,1'i günde 8 saatten uzun süre internet kullanmaktadır. Sonuçlar katılımcılarının çoğunun (%98,9) mobil internet kullandığını göstermektedir. Katılımcıların %65,8'i e-devlet %54,5'i e-ticaret hizmetleri için interneti kullanmaktadır.

Prosedür

Tüm araştırma prosedürleri etik standartlarla uyumludur ve araştırma Tokat Gaziosmanpaşa Üniversitesi (20/02/2020-E.11621) tarafından onaylanmıştır. Tüm katılımcılardan onam formu alınmış ve katılımcılar araştırmanın amacı hakkında bilgilendirilmiştir. Basılı enstrümanda sekiz demografik soru (ör. cinsiyet, yaş, internet kullanımı gibi) ve ölçek maddeleri bulunmaktadır. Katılımcılara deneyimlerini tarif eden ifadeleri 5 puanlı Likert tipi ölçek üzerinde "1=kesinlikle katılmıyorum" ile "5=kesinlikle katılıyorum" arasında puanlamaları istenmiştir.

Ölçme Araçları

Bu çalışmada ölçme aracı olarak Demografik Bilgi Anketi, Siber Güvenlik Ölçeği (SGÖ) kullanılmıştır. Bu tez çalışması neticesinde geliştirilen ölçek EK 1'de sunulmuştur.

Ölçeğin Formatının ve Madde Havuzunun Oluşturulması

Alanyazın incelemesi sonucu ölçeğin kavramsal çerçevesi belirlenmiş ve ölçeğin formatı oluşturulmuştur. Siber güvenlik ölçeği (SGÖ) 5'li likert tipi formatında oluşturulmuştur. Ölçeğin uygulanacak bireylerin katılma derecesi ise, 'Kesinlikle Katılmıyorum (1), Katılmıyorum (2), Kararsızım (3), Katılmıyorum (4), Kesinlikle Katılıyorum (5)' şeklinde belirlenmiştir. Alan yazın taramasından ve gerekli inceleme ve araştırmalardan elde edilen veriler neticesinde 74 maddeden oluşan bir madde havuzu araştırmacı ve danışmanı tarafından geliştirilmiştir.

Görünüş Geçerliliği

Danışman ve öğrencisi tarafından oluşturulan madde havuzu 74 maddeden oluşmaktadır. Madde havuzunun görünüş geçerliliği (psikometri, dil bilimi, bilişim sistemleri) alanında uzman üç kişi tarafından doğrulanmıştır. Alan uzmanları maddeleri çıkarılmalı, değiştirilmeli veya uygun olarak işaretlemiştir. İlk değerlendirmenin ardından uzmanlar 17 maddenin çıkarılması ve 8 maddenin değiştirilmesi gerektiğini önermiştir. İlk revizyondan sonra madde havuzu uzmanlara ikinci kere sunulmuştur. Uzmanlar 5 maddenin çıkarılması ve 6 maddenin değiştirilmesi gerektiğini önermiştir. Üçüncü aşamada uzman grubu son onayı vermiş ve 52 maddelik bir form elde edilmiştir.

Güvenilirliğe İlişkin Bulgular

Ölçeğin iç tutarlılık katsayısının hesaplanması için Cronbach alfa katsayısı (α) kullanılmıştır. Buna göre ilk çalışmada ölçeğin tamamı için güvenirlik kat sayısı .880; 1. alt boyut "Gizlilik" için .810; 2. alt boyut "Kontrol/Sahiplik" için .822; 3. alt boyut "Bütünlük" için .752; 4. alt boyut "Gerçeklik" için .771; 5. alt boyut "Erişebilirlik" için .807; 6. alt boyut "Fayda" için .704 olarak bulunmuştur.

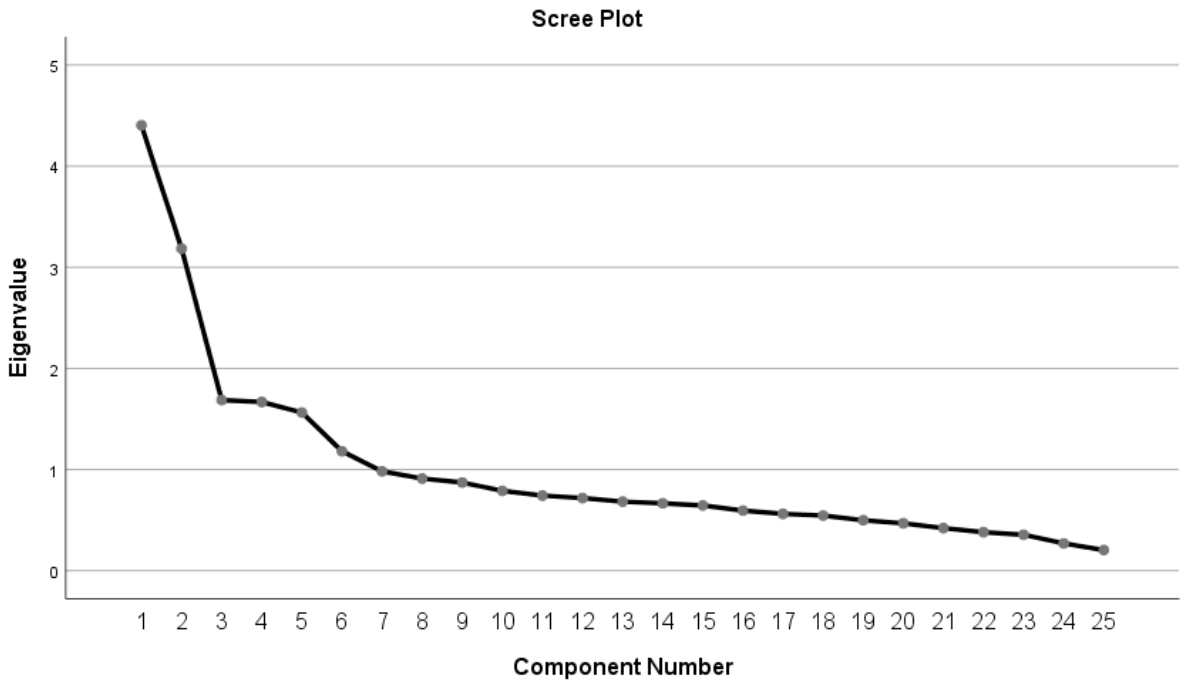
Açımlayıcı Faktör Analizi (AFA)

AFA, ölçek yapısının altında yatan faktörleri belirlemek için gerçekleştirilmiştir. İlk aşamada yükleri bir faktörden fazla olduğu için veya faktörde yeterince yük oluşturmadığı için 25 madde çıkarılmıştır. Son aşamanın sonucunda altı faktörlü çözümde 27 madde kalmıştır. Normallik testi sonuçları, iki maddenin (kontrol 2 ve 3) yüksek basıklık ve eğiklik gösterdiği için ölçekten çıkarılmasından sonra 25 madde kalmıştır.

Hazırlanan 25 maddelik ölçeğe ikinci defa ölçek yapısının altında yatan faktörleri belirlemek için AFA analizi yapılmıştır. AFA analizi sonucunda ilk aşamada yükleri bir faktörden fazla olduğu için veya faktörde yeterince yük oluşturmadığı için gizlilik alt boyutundaki 4. Madde çıkarılmıştır (faktör yükü<.40). Son aşamanın sonucunda altı faktörlü çözümde son olarak 24 madde kalmıştır. Altı faktörün öz değeri birden büyüktür ve toplam varyansın %49,344'üne karşılık gelmektedir. İlk ve ikinci faktör sırasıyla varyansın %27,538 ve %10,606'sını açıklamaktadır. Kaiser'in örnekleme uygunluğu ölçümü .865 olarak bulunmuş ve Bartlett'in test sonuçları değerlerinin anlamlı olduğunu göstermiştir (x^2 (df=300)=3570.447). Bu da değişkenlerin faktör analizi için uygun olduğunu göstermiştir. Tablo 3 Promax rotasyonuyla maksimum olasılık için oransal ortak etken varyans ve desen matrisini göstermektedir.

Yamaç Eğrisi (Scree Plot)

Yamaç eğrisi grafiği (scree plot) sonucuna bakılarak ölçeğin kaç faktörlü yapıdan oluştuğuna bakılmıştır. Yamaç eğrisi grafiği (scree plot) şekil 3'te verilmiştir. Şekilde de anlaşıldığı gibi ölçeğin altı faktörlü yapıda olduğu belirlenmiştir. Elde edilen altı faktör "erişebilirlik, gizlilik, kontrol/sahiplik, bütünlük, gerçeklik ve fayda" olarak ifade edilmiştir.



Şekil 3: Yamaç eğrisi grafiği (scree plot)

Tablo 3. Desen Matrisi

Faktör	**Madde**	**Oransal ortak etken varyans**	**1**	**2**	**3**	**4**	**5**	**6**
Gizlilik	Madde1	.613	.752					
	Madde2	.615	.737					
	Madde3	.569	.673					
Kontrol/Sahiplik	Madde4	.451		.523				
	Madde5	.427		.563				
	Madde6	.620		.856				
	Madde7	.685		.826				
	Madde8	.347		.485				
Bütünlük	Madde9	.279			.481			
	Madde10	.300			.437			
	Madde11	.680			.837			
	Madde12	.688			.850			
Gerçeklik	**Madde13**	.331				.605		
	Madde14	.410				.537		
	Madde15	.514				.758		
	Madde16	.396				.510		
	Madde17	.501				.590		

Erişilebilirlik	Madde18	.574					.784	
	Madde19	.819					.971	
	Madde20	.400					.448	
	Madde21	.441					.596	
Fayda	Madde22	.345						.596
	Madde23	.610						.797
	Madde24	.407						.645
Öz değerler			6.884	2.652	1.749	1.516	1.315	1.088
Açıklanan Varyans			25.224	8.838	5.254	4.225	2.802	3.002
Açıklanan Toplam Varyans								49.344

Tablo 3'te Açımlayıcı Faktör Analizi sonucu çıkan öz değerler 6.884, 2.652, 1.749, 1.516, 1.315, 1.088 Açıklanan Varyans 25.224, 8.838, 5.254, 4.225, 2.802, 3.002 Toplam Açıklanan Varyans 49.344 olarak bulunmuştur. Kalaycı (2009) faktör analizinde ortak varyansı .30'dan düşük olan değişkenlerin analizden çıkarılmasının açıklanan toplam varyans değerini yükselteceğini belirtmiştir. Her ne kadar ortak varyansın .30 ve üzeri olması gerektiği belirtilse de önemine binaen madde 9 analizden çıkartılmamıştır.

Tablo 4'te gösterilen normallik testi sonuçları, iki maddenin (kontrol 2 ve 3) yüksek basıklık ve eğiklik gösterdiği için ölçekten çıkarılmasından sonra elde edilmiştir. Sonuçlar basıklık ve eğiklik değerlerinin 3 ile -3 arasında değiştiğini göstermiştir; bu nedenle veri normal dağılıma sahip olarak kabul edilebilir. Güvenilirlik tahminleri kalan 24 madde üzerinden hesaplanmıştır. Son 24 maddeli ölçek, .880 Cronbach alfa değeriyle yüksek iç tutarlılık göstermektedir.

Tablo 4. Betimleyici İstatistikler ve Güvenilirlik

Faktör	**Madde sayısı**	**Ortalama**	**SS**	**Cronbach Alfa**	**Çarpıklık (SE=.136)**	**Basıklık (SE=.272)**
Gizlilik	3	4,15	.882	.810	-1,560	2,724
Kontrol/Sahiplik	5	4,25	.748	.822	-1,757	4,422
Bütünlük	4	2,92	.911	.752	.148	- .098
Gerçeklik	5	3,99	.720	.771	- .776	1,028
Erişilebilirlik	4	3,41	.992	.807	- .333	- .518
Fayda	3	3,61	.854	.704	- .661	.852

Çalışma 2

Katılımcılar ve Prosedür

İkinci çalışma ortalama yaşı 23,01 (SS=3,28 17-34 yaş arasında) olan 613 katılımcıdan oluşmaktadır (325 kadın ve 288 erkek). Katılımcıların %9,6'sı günde 1-2 saat, %40,0'ı günde 3-4 saat, %30,5'i günde 5-7 saat ve %19,9'u günde 8 saatten uzun süre internet kullanmaktadır. Tablo 5'te belirtildiği üzere katılımcıların %58,2'si e-devlet, %57,4'ü e-ticaret hizmetleri için kullanmaktadır.

Tablo 5. Ölçeğin uygulandığı 2. çalışma grubundaki öğrencilerin demografik bilgileri

Cinsiyet	Frekans	Yüzde (%)
Kadın	325	53,0
Erkek	288	47,0
Toplam	613	100
İnternet Kullanım Süreniz		
1-2 Saat	59	9,6
3-4 Saat	245	40,0
5-7 Saat	187	30,5
8 Saat ve üzeri	122	19,9
Toplam	454	100
Mobil Cihazınızda İnternet var mı		
Evet	587	95,8
Hayır	26	4,2
Toplam	454	100
İnternet kullanım amacı		

İnternet/mobil bankacılık hizmetini kullanırım	494	80,6
E-devlet hizmetlerini kullanırım	357	58,2
E-ticaret siteleri üzerinden internet alışverişi yaparım	352	57,4
Kullanmıyorum ve kullanmayı düşünmüyorum	24	3,9

Yapı Geçerliliği

SGÖ'nün uyum geçerliliği, "kompozit güvenilirlik" (CR) ve "ortalama açıklanan varyans" (AVE) değerlerini kullanarak incelenmiştir. Sonuçlar CR değerlerinin eşik değeri .70'ten yüksek olduğunu göstermiştir (Fornell & Larcker, 1981). AVE değerleri ise eşik değeri olan .50'ye yakındır. Bu durum uygun uyum geçerliliği olduğunu göstermektedir. Sonuçlar faktörlerin birbiriyle anlamlı düzeyde ilişkili olduğunu göstermektedir (p<.01). Ayrıca AVE değerlerini karekökü (köşegen dışı elemanlarda gösterilmiştir) çapraz korelasyonlardan yüksek olduğu için diskriminant geçerliliğinin doğrulandığı görülmektedir. Tablo 6 korelasyonlar matrislerini ve CR ile AVE değerlerini göstermektedir.

Tablo 6. Korelasyon matrisi, uyum geçerliliği ve diskriminant geçerliliği

	CR	AVE	1	2	3	4	5	6
1. Erişilebilirlik	.827	.548	.740					
2. Gizlilik	.796	.497	.279*	.705				
3. Kontrol/Sahiplik	.803	.450	.386*	.557*	.671			
4. Bütünlük	.789	.496	.367*	.146*	.197*	.704		
5. Gerçeklik	.796	.441	.461*	.596*	.670*	.281*	.664	
6. Fayda	.740	.489	.436*	.354*	.370*	.346*	.397*	.700

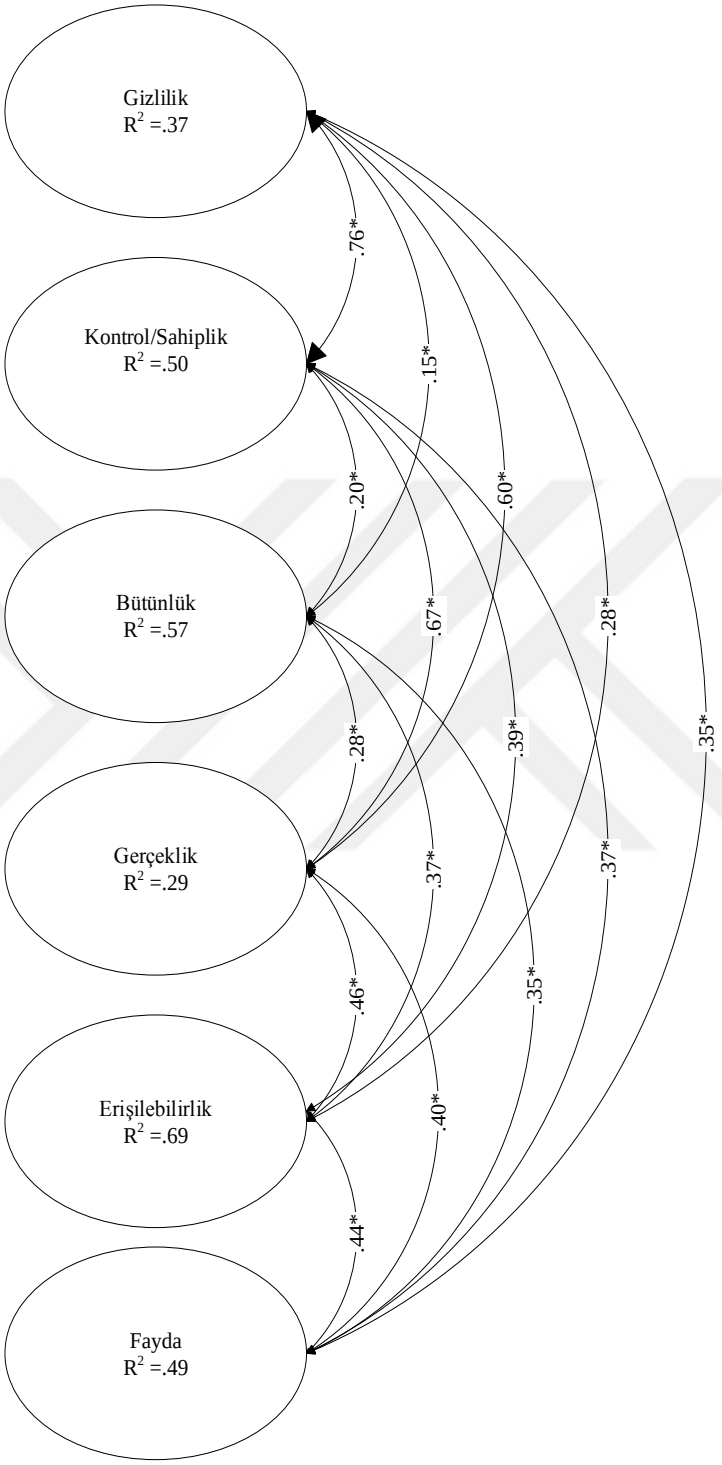
*p<.01

Ölçüm Modeli

Ölçüm modellerini SPSS AMOS (v.23) ile test etmek için DFA kullanılmıştır. Kline (2005) tarafından önerilen model uyum tahminleri ve referans değerleri, ölçüm modelleri için uygun model uyumunu göstermektedir: [χ^2/DF=2.28, GFI=.944, AGFI=.925, CFI=.932, TLI=.918, IFI=.933, RMSEA=.046]. Tablo 7, Şekil 3'te gösterilen ölçüm modelinin model uyum indislerini göstermektedir. SPSS AMOS (v.23) programı kullanılarak hazırlanan siber güvenlik ölçeğine ait ölçüm modeli aşağıda yer alan Şekil 3'te gösterilmektedir.

Tablo 7. Model uyum indisleri

Uyum İndisleri	**Ölçüm Modeli**	**Referans Değerler**
χ^2	396,734	
p değeri	< ,001	
χ^2/df	2,280	< 3
GFI	,944	≥ ,90
AGFI	,925	≥ ,80
NFI	,887	≥ ,90
TLI	,918	≥ ,90
CFI	,932	≥ ,90
IFI	,933	≥ ,90
RMSEA	,046	≤ ,08
SRMR	,045	≤ ,08



*p< .001

Şekil 4: Ölçüm Modeli

BÖLÜM VI

TARTIŞMA

Teknolojinin gelişmesine paralel olarak dünyada her geçen gün baş döndürücü bir hızla gelişen ve sürekli kendini yenileyen bilgisayar teknolojisi hayatımızı ve işlemlerimizi kolaylaştırdığı kadar birtakım güvenlik sorunlarını da beraberinde getirmektedir (Arpaci vd., 2015). Bu nedenle içinde bulunduğumuz bilgi çağında beşinci boyut olarak adlandırılan siber uzayda güvenlik çok önem kazanmaktadır (Güntay, 2018). Dünyada her geçen gün artan bilgisayar ve internet kullanıcısı göz önüne alındığında gelecekte olası yaşanabilecek siber saldırıların sonuçlarının ülkelerin ekonomisine olan maliyetinin ne kadar yüksek boyutlarda olabileceği düşündürücü bir durumdur. Fakat günümüzde ülkemizde ve dünyada yaşanan siber saldırılar sonucu ortaya çıkan ekonomik kayıplar dünyada ülkelerin siber güvenlik konusunda mücadele etmekte başarısız oldukları ve bilişim sistemlerinin korunması noktasında yeterli önlemlerin alınmadığının bir sonucu olarak karşımıza çıkmaktadır. Dünya üzerinde milyarlarca bilgisayar ve internet kullanıcısı olduğu bilinmesine rağmen gelişmiş ve gelişmekte olan ülkeler dahil birçok dünya ülkesi siber güvenlik konusunda ulaşım, haberleşme, telekomünikasyon, eğitim, sağlık, enerji vs. kritik altyapılarını korumakta zorlanmaktadırlar. Bu nedenle, bireylerin siber güvenlik algılarının ve eylemlerinin araştırılıp tespit edilmesi, siber güvenlik konusundaki eksikliklerinin detaylı bir biçimde analiz edilip bu konuda çözüm önerilerinin geliştirilmesi gerekmektedir. Bu amaçla literatürdeki bu boşluğu doldurup siber güvenlik alanında katkı sağlamak amacıyla bireylerin siber güvenlik konusundaki algı ve eylem düzeylerini ölçmeyi amaçlayan bir ölçek geliştirilmiştir.

Alanyazın incelendiğinde bireylerin bilgi güvenliği farkındalıklarını ölçen ölçeklere rastlansa da siber güvenlik pratiklerini ve algısını ölçen bir ölçme aracına rastlanmamıştır. Bu çalışma ile geliştirilen siber güvenlik ölçeği bireylerin siber güvenlik algılarını ve pratiklerini ölçmeyi amaçlanmaktadır. Araştırmanın bulgularından da anlaşılacağı üzere geliştirilen siber güvenlik ölçeği geçerli ve güvenilir bir ölçektir. Geliştirilen ölçeğin birçok araştırmacıya yol gösterici bir rehber olacağı düşünülmektedir.

Bu tez çalışmasında Parker altılısı modeli temel alınarak bireylerin siber güvenlik pratiklerini ve algılarını ölçmek için kullanılabilecek geçerli ve güvenilir bir siber güvenlik ölçeği (SGÖ) geliştirilmiştir. Geliştirilen bu ölçeğin psikometrik özellikleri test edilmiştir. Geliştirilen ölçeğin tamamı için güvenirlik kat sayısı .88 olarak, alt boyutları için ise 70 - 82 arasında bulunmuştur. Dolayısıyla, siber güvenlik ölçeğinin güvenilir bir ölçek olduğu anlaşılmaktadır. Siber güvenlik ölçeğinin faktör yapısını belirlemek için Açımlayıcı Faktör Analizi (AFA) yapılmıştır. Kaiser'in örnekleme uygunluğu ölçümü .865 olarak bulunmuş ve Bartlett'in küresellik testi sonuçları değerlerinin anlamlı olduğu görülmüştür. Bunun sonucunda ölçekteki değişkenlerin faktör analizi için uygun olduğu anlaşılmıştır. Ayrıca normallik testi sonuçları basıklık ve eğiklik değerlerinin 3 ile -3 arasında değiştiğini göstermiş, bunun sonucunda verinin normal dağılıma sahip olduğu kabul edilmiştir. Araştırmanın birinci çalışmasında yapılan açımlayıcı faktör analizi altı faktörlü bir yapıya (gizlilik, kontrol/sahiplik, bütünlük, gerçeklik, erişilebilirlik ve fayda) işaret etmektedir. Araştırmanın ikinci çalışmasında doğrulayıcı faktör analizi ile altı faktörlü yapının verilerle iyi uyum gösterip göstermediği incelenmiştir. Araştırmanın sonuçları siber güvenlik ölçeğinin yakınsak ve ayrım geçerliliği ile yapı geçerliliğine sahip olduğunu göstermektedir.

BÖLÜM VII

SONUÇ VE ÖNERİLER

Siber güvenlik IoT ve siber-fiziksel sistem çağında önemli bir kavramdır (Arpaci, 2016). Birbiriyle ilişkili hesaplama cihazlarının dağıtılmış doğası, siber saldırı zafiyeti oluşturarak bilginin bütünlük, gizlilik ve erişilebilirlik özelliklerini hedef alarak güvenlik ve gizliliği ihlal etme girişimlerinde bulunmaya neden olmaktadır (Arpaci, 2017). Bu nedenle herkes siber güvenlik risklerinin farkında olmalı ve proaktif eylemlerle siber saldırılara karşı hazır olmalıdır.

Bu çalışma ile bilişim sistemlerini kullanan tüm bireylerin siber güven algılarını ve pratiklerini ölçmeye yönelik bir ölçek (SGÖ) geliştirilmiştir. Geliştirilen bu ölçek ile bireylerin siber güvenlik konusundaki algılarını ve eylemlerini ölçmek, böylelikle bireylerin siber güvenlik seviyelerini tespit etmek amaçlanmıştır. Sonuçlar SGÖ'nün yüksek iç tutarlılık gösterdiğini ortaya koymaktadır. Ölçeğin altı faktörlü yapısı (gizlilik, kontrol/sahiplik, bütünlük, gerçeklik, erişilebilirlik ve fayda) doğrulanmıştır. Ekte 1'de sunulan ölçek bireylerin siber güvenliğe ilişkin algılarını ve pratiklerini ölçen güvenli ve geçerli bir ölçektir. Geliştirilen bu ölçek bireylerin siber güvenlik pratikleri ve algıları konusunda kendilerini daha iyi tanımalarını sağlayabilir. Ayrıca sanal ortamda kullanmış oldukları bilişim sistemlerine ve teknolojik aygıtlara karşı dışarıdan gelebilecek olası siber saldırılara karşı kendilerini hazır hissetmelerine, gerekli önlemleri almalarına ve siber güvenlik konusunda kendilerini geliştirmelerine katkı sağlayabilir.

Siber uzayda meydana gelen gelişmeler ekonomiden sağlığa, endüstriden ticarete, finans işlemlerinden sosyal ağlara kadar yaşamın her alanını doğrudan etkilemektedir (Al-Emran vd., 2021; Arpaci, 2021). Siber güvenlik ve siber uzay interneti bünyesinde barındırmakla beraber donanım sistemlerini, yazılım sistemlerini, enformasyon sistemlerini ve bu sistemlerle ilgilenen kurum ve kuruluşları, ağ sistemlerini kapsayan bir kavramdır (Erdem ve Özocak, 2019). Dünyadaki birçok ülke ulusal ve uluslararası boyutta siber güvenliğe gerekli önemi verip, siber güvenliğin küresel boyutta dünya ülkelerini ekonomik, sosyal ve psikolojik olarak etkilediklerine dikkat çekmektedirler (Arpaci, 2019; Arpaci,

2020). Geliştirilen ölçek siber güvenliğin psikolojik ve davranışsal boyutlarının daha iyi anlaşılmasına katkı sağlayabilir.

Bu çalışmada geliştirilen ölçek Tokat Gaziosmanpaşa Üniversitesinde öğrenim gören toplam 993 üniversite öğrencisine uygulanmıştır. Ölçek daha farklı örneklem gruplarına uygulanabilir. Örneğin siber güvenlik ölçeği kamu ve özel sektörde çalışan personele uygulanarak siber güvenlik konusundaki pratikleri ve algıları tespit edilebilir.

Toplumdaki bireylerde siber güvenlik kültürünün yerleşmesi ve toplumdaki bilişim sistemlerini kullanan bireylerin siber güvenlik konusunda yeterince donanımlı ve bilgi sahibi olması elzemdir (Arpaci, 2018). Bu tez çalışması öncelikle siber güvenlik kavramının toplumda daha iyi anlaşılmasına ve toplumun bu konuda bilinçlenmesine katkı sağlayabilir.

Siber güvenlik kültürünün bireylerde tam olarak yerleşmemiş olması bilgi güvenliği riskini doğurmaktadır. Bu nedenle ülkemizdeki toplumun bütün fertlerinde siber güvenlik kültürünün oluşturulması gerekmektedir (Erçağlar, 2017). Bu tez çalışması bireylerde siber güvenlik kültürünün oluşturulmasına katkı sağlayabilir.

Siber güvenlik kavramı 21. yüzyılın başından itibaren bilişim teknolojisinde yaşanan gelişmelere bağlı olarak yeni bir ivme kazanmıştır. Bu konuda ulusal ölçekte ve uluslararası alanda ülkelerin siber güvenliğinin yeterince sağlanamamasının yalnız kişisel bilgisayar kullanıcıları ve kamu kurumları için değil ülkelerin geleceği ve bilişim alt yapısı için de önemli bir sorun teşkil edeceği anlaşılmaktadır. Ayrıca siber güvenlik konusunda yaşanan sıkıntılar ülkelerin kritik altyapıları için çok büyük risk olarak görülmektedir. Bu nedenle ülkemizde siber güvenlik kültürünün ve bilincinin toplumun tüm bireylerinde oluşturulması önem arz etmektedir. Bu nedenle bireylere ilkokul seviyesinden başlamak üzere bilişim teknolojileri dersinde siber güvenlik konusu kapsamlı bir biçimde ele alınmalı, hatta ortaöğretim ve liselerde ders olarak okutulmalıdır. Bu sayede öğrencilerin siber güvenlik kavramını içselleştirmesi sağlanmalıdır. Siber güvenlik konusunda yeterli bilgiye sahip olan bireylerde her geçen gün bilgisayarın, internetin ve teknolojik aygıtların ve programların geliştirildiği bilgi çağında bireylerin güvenli bir biçimde internette işlemlerini gerçekleştirebileceği, gelecekte ülkemizde yaşayan bireylerin kamu kurumları ve özel işletmelerle olan ilişkilerinde interneti ve bilgisayarı aktif olarak daha çok kullanılacağı

düşünüldüğünde bireylerde siber güvenlik konusunda alt yapının oluşturulmasının ne derece önemli bir husus olduğu anlaşılacaktır. Bu sayede toplumdaki tüm bireylerde siber güvenlik kültürü gelişecek, bireylerin kişisel verilerini koruma konusunda bakış açısı değişecek, siber güvenlik konusunda risk boyutu en az seviyeye indirilecektir.

Siber güvenlik kavramı ile ilgili kamu ve özel sektör iş birliğinde bireylerin farkındalıklarını geliştirici eğitimler, uygulamalar ve aktiviteler gerçekleştirmelidirler. Kamu kurumlarında siber güvenlik konusunda uygulamalı faaliyetler gerçekleştirilmelidir. Siber güvenlik tatbikatları düzenlenmeli, kamu ve özel sektör olarak tüm kuruluşların bu faaliyetlere katılımının sağlanması teşvik edilmelidir. Ayrıca kamu kurumlarında siber güvenliğin sağlanması konusunda teknik personel bulundurulması zorunlu olmalıdır. Bu konuda gerekli denetim ve inceleme ülkemizde siber güvenlikten sorumlu en üst makamlar ve birimler tarafından gerçekleştirilmelidir. Siber güvenlik konusunda kamu kurumlarında ve özel kurumlarda belirli periyotlarda durum tespiti ve değerlendirmeler yapılmalıdır. Ayrıca ilkokul seviyesinden başlayarak ortaokul, lise ve üniversitelerde tüm eğitim kademelerinde öğrencilere siber güvenlik eğitim verilmelidir.

Siber güvenlik konusunda ülkemizde kalifiye personel yetiştirilmesi için yöneticiler tarafından bu konuda gerekli eğitim ve teknik harcamalar için devlet bütçesinden gerekli ödeneklerinin ayrılması gerekmektedir. Ayrıca siber güvenlik konusunda ülkemizdeki teknolojik altyapının geliştirilmesi de gerekmektedir. Ülkemizin kritik altyapılarının siber saldırılara karşı korunması noktasında donanımlı ve nitelikli personele ihtiyaç duyulması akabinde bu konuda teknolojik altyapının da geliştirilmesi hassasiyetle üzerinde durulması gereken konuların başında gelmelidir. Ayrıca siber güvenlik konusunda kamu kurumları ve özel işletmeler tarafından AR-GE çalışmalarının yapılması da ülkemizdeki siber güvenliğin gelişimi açısından gerekli bir hususdur (Polat, 2020).

Siber güvenlik konusunda devlet kurumları ve özel sektör arasında iş birliğinin sağlanması ülkenin siber güvenlik politikalarının gelişimini sağlayacak ve siber saldırılara karşı risk boyutunu aşağıda seviyelere çekecektir. Bu nedenle kamu kurumları ile özel sektör arasında bilgi paylaşımı, siber saldırılara karşı müşterek hareket, ortak siber güvenlik tatbikatlarının yürütülmesi için birliğinin sağlanması gerekmektedir. Siber güvenlik

konusunda birçok gelişmiş dünya ülkesi bilişim teknolojileri konusunda geleceğe yönelik stratejik hedefler belirlemektedirler. Bu nedenle ülkemizde de siber güvenlik konusunda stratejik hedefler ve taktikler geliştirilmeli, kamu ve özel sektör iş birliğinde siber güvenliğe yönelik bir dizi faaliyetler yürütülüp bunların kullanıcılar tarafından uygulanmasını sağlamak için gerekli adımlar atılmalıdır (Bilgi Güvenliği Derneği, 2012)

Literatür incelendiğinde siber güvenlik konusunda bilimsel birçok yayın, makale ve tez hazırlandığı görülmüş ancak siber güvenlik konusunda hazırlanmış yeterince ölçek tespit edilememiştir. Bu amaçla hem literatürde bu boşluğu doldurmak hem de siber güvenlik ile ilgili kamu kurum ve kuruluşlarında, özel sektörde ve akademik alanda bilimsel çalışma yapmak isteyenlere, siber güvenlik konusunda farklı türde ölçek hazırlamak isteyen araştırmacılara kaynak oluşturması ve yol göstermesi adına uygulayıcılar için örnek teşkil etmesi bakımından kullanabilecekleri bir ölçek olabilir.

KAYNAKÇA

Abomhara, M. ve Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.

AFAD (2020). Açıklamalı afet yönetimi terimleri sözlüğü. https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu.html adresinden alınmıştır.

Akgün, Ö. ve Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları, Sakarya Üniversitesi Eğitim Fakültesi Örneği. *Sakarya University Journal of Education, 5*(2), 98-121.

Aksakallı, I. K. (2019). Bulut bilişimde güvenlik zafiyetleri, tehditleri ve bu tehditlere yönelik güvenlik önerileri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *5*(1), 8-34.

Al-Emran, M., Al-Maroof, R., Al-Sharafi, M. A., & Arpaci, I. (2021). What impacts learning with wearables? An integrated theoretical model. *Interactive Learning Environments*. https://doi.org/10.1080/10494820.2020.1753216.

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice*. Syngress, Elsevier, USA.

Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Computers in Human Behavior, 58*, 150-157. https://doi.org/10.1016/j.chb.2015.12.067.

Arpaci, I. (2017). The role of self-efficacy in predicting use of distance education tools and learning management systems. *The Turkish Online Journal of Distance Education, 18*(1), 52-62. https://doi.org/10.17718/tojde.285715.

Arpaci, I. (2018). An investigation of the relationship between university students' innovativeness profile and their academic success in the project development course. *Journal of Entrepreneurship and Innovation Management, 7*(2), 79-95. https://dergipark.org.tr/tr/pub/jeim/issue/52607/692543

Arpaci, I. (2019). Culture and nomophobia: The role of vertical versus horizontal collectivism in predicting nomophobia. *Information Development, 35*(1), 96-106. https://doi.org/10.1177/0266666917730119

Arpaci, I. (2020). What drives students' online self-disclosure behavior on social media? A hybrid SEM and artificial intelligence approach. *International Journal of Mobile Communications, 18*(2), 229-241. https://doi.org/10.1504/IJMC.2020.105847

Arpaci, I. (2021). Relationships between early maladaptive schemas and smartphone addiction: The moderating role of mindfulness. *International Journal of Mental Health and Addiction*. https://doi.org/10.1007/s11469-019-00186-y.

Arpaci, I., Cetin Yardimci, Y., & Turetken, O. (2015). The impact of perceived security on organizational adoption of smartphones. *Cyberpsychology, Behavior, and Social Networking, 18*(10), 602-608. https://doi.org/10.1089/cyber.2015.0243.

Arslan, M. E. (2018). Siber Güvenlik ve Siber Saldırı Türleri.

Ashibani, Y. ve Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security, 68*, 81-97. https://doi.org/10.1016/j.cose.2017.04.005

Aslanyürek, M. (2016). İnternet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik ile ilgili kanaatleri ve farkındalıkları. *Maltepe Üniversitesi İletişim Fakültesi Dergisi*,*3*(1), 80-106.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies, 1*(1), 24-28.

Atasoy, İ. ve Ormanlı, O. (2019). Teknoloji ve siber güvenlik: Dijital toplumun geleceği. *İstanbul Aydın Üniversitesi Dergisi*,*11*(4), 399-409.

Baheti, R. ve Gill, H. (2011). Cyber-physical systems. *The impact of control technology*, *12*(1), 161-166.

Baykara, M., Daş, R. ve Karadoğan, İ. (2013, 20-21 Mayıs). *Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi.* I. Uluslarlarası dijital adli ve güvenlik sempozyumunda sunuldu, Elazığ.

Benzer, R. (2014). *Siber Suçlar ve Teorik Yaklaşımlar*. H. Çakır, M.S. Kılıç (Editörler). Güncel Tehdit: Siber Suçlar. Birinci Baskı. Ankara: Seçkin Yayıncılık, 21-41.

Bilişim Teknolojileri ve Siber Güvenlik Derneği (2018). Bilgi Güvenliği Farkındalık Eğitimi,http://www.bs.org.tr/egitimlerimiz/bilgiguvenligifarkindalikegitimi adresinden alınmıştır.

Bilgi Güvenliği Derneği (2012). Ulusal Siber Güvenlik Stratejisi. https://www.bilgiguvenligi.org.tr/ /Ulusal_Siber_Guvenlik_Stratejisi.pdf adresinden alınmıştır.

BTK (2009). Siber güvenliğin sağlanması: Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler.https://www.btk.gov.tr/File/Documents/Sayfalar/SiberGuvenlik Fsg.pdf adresinden alınmıştır.

Bingöl, H. ve Karakoç, M. M. (2015). İnternet bankacılığı ve telekomünikasyon alanında siber güvenliğe genel bakış. *Türk Doğa ve Fen Dergisi*, 23.

Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance*, *6*(2), 13-21.

Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., & Atlanta, G. A. (2008). Cybersecurity in africa: An assessment. *Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology*.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56,* 1-27. https://doi.org/10.1016/j.cose.2015.09.009

Çetin, H., Gundak, İ. ve Çetin, H. H. (2015). E-işletme güvenliği ve siber saldırılar üzerine bir araştırma. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *6*(2), 223-240.

Çifçi, H. (2013). *Her yönüyle siber savaş*. İstanbul: Tübitak Popüler Bilim Kitapları.

Dunn Cavelty, M. ve Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32.

Dhawan, S. M., Gupta, B. M., & Elango, B. (2020). Global Cyber Security Research Output (1998–2019): A Scientometric Analysis. *Science & Technology Libraries*, 1-18.

Efendioğlu, Ö. G. A. ve Sezgin, Ö. G. E. (2007). E-devlet uygulamalarında bilgi ve paylaşım güvenliği. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *16*(2), 219-236.

EGM (2019). Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. https://www.egm.gov.tr/siber/sibersucnedir adresinden alınmıştır.

Erdem, M. ve Özocak, G. (2019). Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, *68*(1), 127-212.

Erçağlar, E. (2017). *Siber Güvenlik Operasyon Merkezi Gereksinimleri*, Çevre ve Şehircilik Bakanlığı Uzmanlık Tezi, Ankara.

Fornell, C. ve Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. https://doi.org/10.1177/002224378101800104

Giri, S. (2019). Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal. *Pramana Research Journal*, *9*(3), 662-672.

Gökce, K. G., Şahinaslan, E. ve Dincel, S. (2014, 17-18 Ekim). *Mobil Yaşamda Siber Güvenlik Yaklaşımı*. VII. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nda sunuldu, İstanbul.

Güntay, V. (2018). Siber güvenliğin uluslararası politikada etki aracına dönüşmesi ve uluslararası aktörler. *Güvenlik Stratejileri Dergisi*, *14*(27), 79-111.

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., ... & Chen, J. (2016). Cultural and psychological factors in cyber-security. In *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services* (pp. 318-324).

Hekim, H. ve Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 135-158.

Henkoğlu, T. ve Külcü, Ö. (2013). Bilgi erişim platformu olarak bulut bilişim: Riskler ve hukuksal koşullar üzerine bir inceleme. *Bilgi Dünyası*, *14*(1), 62-86.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(4), 3171-3189.

Howard, D. J. (2018). Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents.

ISO/IEC. (2012). ISO/IEC 27032: Information technology-security techniques-guidelines for cybersecurity.

ITU. (2008). International Telecommunications Union, ITU -TX.1205: Series X: Data networks, open system communications and security: Telecommunication security: Overview of cybersecurity. https://www.itu.int/rec/T -REC -X.1205 -200804-I adresinden alınmıştır.

ITU. (2008). International Telecommunications Union," ITU-T-Rec.X.500". 2015. Cybersecurity.

Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü (2020). https://istanbulism.saglik.gov.tr/TR,65214/bilgi-guvenligi.html adresinden alınmıştır.

Kabay, M., Whyne E. ve Bosworth S. (2009). Computer Security Handbook. Fifth. https://safaribooksonline.com/library/view/computer-security-handbook adresinden alınmıştır.

Kalaycı, Ş. (2009). SPSS uygulamalı çok değişkenli istatistik teknikleri(4. Baskı). Ankara: Asil Yayın Dağıtım.

Karabacak, B. (2011). Kritik altyapılara yönelik siber tehditler ve Türkiye için siber güvenlik önerileri. Siber Güvenlik Çalıştayı, Bilgi Güvenliği Derneği, 29.

Kurt Kaya, G.D. (2017). Bilgi Güvenliği ve Siber Güvenlik Kapsamında Bakanlık Uygulamaları İçin Güvenli Yazılım Geliştirme Metedolojisi Önerisi, Çevre ve Şehircilik Bakanlığı Uzmanlık Tezi, Ankara.

Kline, R. B. (2005). *Principles and practice of structural equation modeling* (2nd ed). New York: Guilford.

Li, W., Meng, W. ve Kwok, L. F. (2016). A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. *Journal of Network and Computer Applications, 68,* 126-139. https://doi.org/10.1016/j.jnca.2016.04.011

Mulligan, D. K. ve Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus, 140*(4), 70-92.

Öztürk, M. S. (2018). Siber Saldırılar, Siber Güvenlik Denetimleri ve Bütüncül bir denetim modeli önerisi. *Muhasebe ve Vergi Uygulamaları Dergisi*, 208-232.

Parker, D. B. (1992). Fighting Computer Crime: A New Framework for Protecting Information. New Jersey, ABD: John Wiley & Sons.

Pender-Bey, G.(2012). The Parkerian Hexad: The CIA Expanded, 4-20.

Polat, S. (2020). *Milli Güvenlik Açısından Siber Güvenlik*. Yayımlanmış Yüksek Lisans Tezi. Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Ankara.

Reid, R. ve Van Niekerk, J. (2014). From information security to cyber security cultures. *IEEE Information Security for South Africa* (pp. 1-7). Doi: 10.1109/ISSA.2014.6950492

Sağıroğlu, Ş. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*. Ankara: Grafiker Yayınları

Sertçelik, A. (2015). Siber Olaylar Ekseninde Siber Güvenliği Anlamak. *Medeniyet Araştırmaları Dergisi*, *2*(3), 25-42.

https://sibertehdit.com/siber-guvenlik-nedir adlı siteden 08 Haziran 2020 tarihinde alınmıştır.

Solomon, M. G. ve Chapple, M. (2005). Information security illuminated. Jones & Bartlett Publishers.

Shafqat, N. ve Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129.

USOM-TRCERT (2014). Ulusal Siber Olaylara Müdahale Merkezi, www.usom.gov.tr adresinden alınmıştır.

USOM (2020). Ulusal Siber Olaylara Müdahale Merkezi, www.usom.gov.tr adresinden alınmıştır.

UDHB(2016).2016-2019 Ulusal Siber Güvenlik Stratejisi. http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf adresinden alınmıştır.

UDHB (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. http://www.udhb.gov.tr/doc/siberg/2013-2014guvenlik.pdf adresinden alınmıştır.

Ünal, A. N. (2018). Bilgi yönetim sistemleri ve siber güvenlik. *International Journal of Social Inquiry, 11*(2), 375-394.

Ünver, M. ve Canbay, C. (2010). Ulusal ve uluslararası boyutlarıyla siber güvenlik. *Elektrik Mühendisliği*, (438), 94-103.

Von Solms, R. ve Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wikipedia (2017). Bilgi güvenliği. https://tr.wikipedia.org/wiki/Bilgi_guvenligi adresinden alınmıştır.

Whitman, M. E. ve Mattord, H. J. (2011). *Principles of Information Security*. Cengage Learning, Nelson Education, CA.

Yanar, Ö. (2014). Güvenlik ve Gizlilik Temelinde Şirketlere Özel Bulut Depolama Çözümü (Private Cloud Storage). In *UYMS*.

Yıldırım, E. Y. (2018). Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması. *Mesleki Bilimler Dergisi (MBD)*, *7*(2), 24-33.

Yılmaz, E. N., Ulus, H. İ. ve Gönen, S. (2015). Bilgi toplumuna geçiş ve siber güvenlik. *International Journal Of Informatics Technologies*, *8*(3), 133.

Yılmaz, F.G.K. ve Ezin, Ç.Ç. (2017). Ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama*, *7*(2), 41-57.

Yılmaz, S. ve Sağıroğlu, Ş. (2013, 20-21 Eylül). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri. VI. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansında sunuldu, Ankara.

EKLER

Ek1. Bilgi Formu ve Ölçme Araçları SGÖ Öğeleri ve Puanlama

Faktörler	**Maddeler**
Gizlilik	1-Siber ortamda paylaştığım kişisel bilgiler konusunda temkinliyimdir.
	2-Gerçek hayatta üçüncü şahıslarla paylaşmak istemediğim bilgi ve belgeleri siber ortamda da paylaşmam.
	3-Siber ortamda paylaştığım verilerin sadece gerekli kişilerce görüntülenmesini sağlarım.
Kontrol/Sahiplik	4-Hesaplarıma ait şifrelerin güvenliği konusunda dikkatliyim.
	5-Şifremi oluştururken sembol, rakam ya da büyük küçük harflerden oluşan tahmini zor bir şifre seçerim.
	6-E-posta şifremin güvenliği için telefon doğrulaması hizmetini kullanırım.
	7-Cevabını hatırlayacağım bir güvenlik sorusu seçmeye özen gösteririm.
	8-Kredi kartı bilgilerimin kaydedilmemiş olmasına dikkat ederim.
Bütünlük	9-Siber ortamda veri saklamak güvenli değildir.
	10-Siber ortamda sakladığım bilgi ve belgeler kaybolabilir ya da silinebilir.
	11-Siber ortamda veri paylaşımı yapmak herhangi bir risk içermez (T: Ters Madde).
	12-Siber ortamda saklanan bilgi ve belgelere üçüncü şahısların erişme olasılığı vardır.
Gerçeklik	13-Tanımadığım kişilerden gelen e-postalardaki linkleri ve eklentileri açarım (T).
	14-Girdiğim web sitesinin güvenlik sertifikası olmadığı yönünde bildirim gelse de kullanmaya devam ederim (T).
	15-E-postama gelen istenmeyen (spam) postaları açtığım olmuştur (T).
	16-E-postama gelen müşteri edinme/oltalama amaçlı postaları açtığım olmuştur (T).
	17-Belirsiz kaynaklardan gelen bağlantıları (linkleri) ve dosyaları açtığım olmuştur (T).

Erişilebilirlik	18-Cihazımda güncel bir anti virüs programı var.
	19-Cihazımı düzenli olarak anti virüs programı ile taratırım.
	20-Cihazıma kurulu gelen güvenlik duvarı açık.
	21-İnternetten indirdiğim dosyaları cihazımda yüklü anti virüs programı olmasa da açarım (T).
Fayda	22-Siber ortamda sosyal medya uygulamalarını bilgi paylaşımı için kullanırım.
	23-Günlük hayatta karşılaştığım problemleri çözmek için siber ortamı yaygın olarak kullanırım.
	24-Siber ortamda sunulan hizmetlerden bilgi yönetimi (bilgiyi elde etmek, saklamak, paylaşmak ve kullanmak) için faydalanırım.

Puanlama: SGÖ, 24 maddeden oluşturan siber güvenlik seviyesini değerlendiren "beş puanlı Likert tipi bir ölçektir. Tüm öğeler 5 puanlı ölçekle "kesinlikle katılmıyorum (1) ile "kesinlikle katılıyorum (5) arasında puanlanmaktadır. Ölçek puanları 25 ila 125 arasında değişmektedir ve yüksek puan, yüksek siber güvenlik algısını ve eylemini göstermektedir.

Ek2. İzinler

Evrak Tarih ve Sayısı: 20/02/2020-E.11621

T.C.
TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü
Enstitüsü Sekreterliği

Sayı :71584433-044/
Konu :Anket izin isteği (Kadir SEVİNÇ)

Sayın Doç. Dr. İbrahim ARPACI
Öğretim Üyesi

İlgi : Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Başkanlığı; 18/12/2019 Tarihli, 68035 sayılı yazı.

Enstitümüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı 189912007 numaralı yüksek lisans öğrencisi Kadir SEVİNÇ'in Doç.Dr.İbrahim ARPACI danışmanlığında hazırlamış olduğu "Siber Güvenlik Algısı Ölçeği Geliştirme, Geçerlik ve Güvenlik Çalışması" başlıklı ve Üniversitemiz **Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu** tarafından uygun görülen tez çalışması kapsamında Tokat Gaziosmanpaşa Üniversitesine bağlı tüm Fakülte ve Meslek Yüksekokullarında **01.02.2020-30.05.2020** tarihleri arasında uygulama yapabilmesi için, ilgilinin başvurması halinde gerekli kolaylığın sağlanması hususunda;

Gereğini bilgilerinize arz/rica ederim.

e-imzalıdır
Doç. Dr. Kerem KILIÇER
Enstitü Müdürü

EK :
İlgi yazı ve ekleri (20 Sayfa)

DAĞITIM
Gereği:
Diş Hekimliği Fakültesi Dekanlığına
Erbaa Sosyal ve Beşeri Bilimler Fakültesi Dekanlığına
Spor Bilimleri Fakültesi Dekanlığına
Erbaa Sağlık Bilimleri Fakültesi Dekanlığına
Eczacılık Fakültesi Dekanlığına
Turhal Uygulamalı Bilimler Fakültesi Dekanlığına
Eğitim Fakültesi Dekanlığına
Fen Edebiyat Fakültesi Dekanlığına
Güzel Sanatlar Fakültesi Dekanlığına
İktisadi ve İdari Bilimler Fakültesi Dekanlığına
İlahiyat Fakültesi Dekanlığına
Mühendislik ve Doğa Bilimleri Fakültesi

Bilgi:
Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Başkanlığına

Tokat Gaziosmanpaşa Üniversitesi Taşlıçiftlik Kampüsü Eğitim Fakültesi Kat:1
Tel: 0 (356) 2521616 Faks: 0 (356) 2521609
E-Posta: ebilen@gop.edu.tr Elektronik ağ: http://ebilen.gop.edu.tr
Ayrıntılı bilgi için irtibat: M.Erdoğan Veri Hazırlama ve Kontrol İşletmeni