**Siber Saldırganlık Ölçümü: Lise Öğrencileri Üzerine Bir Çalışma[[1]](#footnote-1)**

**Sevilay SERYOL[[2]](#footnote-2)\*\*, Mustafa Serkan GÜNBATAR[[3]](#footnote-3)\*\*\***

**Öz:** Bu çalışmanın amacı siber saldırganlık ölçeği geliştirmek ve çeşitli değişkenlere göre öğrencilerin siber saldırganlıklarını karşılaştırmaktır. Araştırmanın katılımcıları Van ilinde 2018-2019 yılında eğitim öğretime devam eden öğrenciler olmuştur. Araştırma iki aşamadan oluşmaktadır. Birinci aşamada açıklayıcı faktör analizi yapılmıştır. Açıklayıcı faktör analizine 1573 öğrenci katılmıştır. Bu analize katılanlardan %54,2’si kadın, %45,8’i erkektir. İkinci aşama ise doğrulayıcı faktör analizi aşamasıdır. Doğrulayıcı faktör analizine 188 öğrenci katılmıştır. Doğrulayıcı faktör analizine katılan öğrencilerin %32’si kadın, %68’i erkektir. Doğrulayıcı faktör analizi sonrasında ortaya çıkan uyum değerlerinin (*X2*=898,79, Sd=433, *X2*/ Sd=2.07, RMSEA=0.076, CFI=0.94, NNFI=0.93, NFI=0.91, AGFI=0,72, GFI=0,77) modeli doğruladığı görülmüştür. Bu sonuçlara göre ölçeğin geçerli ve güvenilir bir ölçme aracı olduğu tespit edilmiştir. Elde edilen verilen analizinde öğrencilerin siber saldırganlık eğilimleri okul türü, cinsiyet, internet kullanım süresi, ebeveynlerin internet kullanması, kullandıkları sosyal ağlar, sosyal ağlarda anonim olması, ebeveynlerin sosyal ağ tutumu, odaya sahip olması, sosyal ağlarda etkileşimli olması ve bilgisayara sahip olmasına göre anlamlı bir fark olduğu görülmüştür.

**Anahtar Kelimeler:** siber saldırganlık, siber zorbalık, Lise öğrencileri, saldırganlık.

**Cyber Aggression Measurement: A Study on High School Students**

**Abstract:** The aim of this study is to develop cyber aggression scale and compare students' cyber aggressiveness according to various variables. Students who continued their education in 2018-2019 participated in the study. The research consists of two stages. Of these stages, 1573 students participated in the exploratory factor analysis. Of those participating in this analysis, 54.2% are women and 45.8% are men. The other stage is the confirmatory factor analysis stage. 188 students participated in the confirmatory factor analysis. Confirmatory factor analysis included students that were 32% women and 68% men. It was seen that the fit indices (X2=898,79, Sd =433, X2/ Sd =2.07, RMSEA=0.076, CFI=0.94, NNFI=0.93, NFI=0.91, AGFI=0,72, GFI=0,77) after confirmatory factor analysis confirmed the model. According to these results, the scale was determined to be a valid and reliable measurement tool. In the analysis of the data obtained, it has been seen that the students 'cyber aggression tendencies are significant difference according to the type of school, gender, duration of internet usage, parents’ internet usage, social networks they use, being anonymous in social networks, social networking attitude towards parents, having a room, being interactive in social networks and having a computer.

**Keywords:** Cyber aggression, Cyberbullying, High school students, Aggression.

**Giriş**

Çağdaş toplumlarda gelişmişlik düzeyi toplumun teknolojiye erişim imkânına göre değişmektedir (Karasar, 2004). Bilgi teknolojileri, günümüz bireyleri arasında gittikçe yaygınlaşmaktadır. Günümüz bireyleri bilgi teknolojilerini kullanma becerileri konusunda uzmanlaşmıştır (Akkoyunlu, 1995). Bilgi ve iletişim teknolojilerindeki gelişmeler bilginin yaygınlaşmasını sağlayarak hayatımızı kolaylaştırmıştır (Güleç, Çelik & Demirhan, 2012). Bilgi ve iletişim teknolojilerinin yaygınlaşması sınıf kavramını ve eğitim kavramını da değiştirmiştir (Erdur-Baker ve Kavşut, 2007; Yılmaz ve Horzum, 2005).

Bilgi ve İletişim Teknolojilerindeki (BİT’deki) hızlı gelişmeler yeni medya ve sosyal medya gibi kavramları hayatımıza sokmuştur (Başlar, 2013). Sosyal medya, zamana ve mekâna bağlı olmaksızın paylaşım yapılabilen bir iletişim şeklidir. İnsanların internette birbirleriyle kuruduğu diyaloglar sosyal medyayı oluşturur (Vural ve Bat, 2010). Sosyal medyanın yaygın kullanımı ile birlikte bazı sorunlar da ortaya çıkmıştır (Yaman ve Sönmez, 2015). İnternet ve sosyal medya kullanımı kimliği belirsiz zararlı e-postaların kullanımı yaygınlaştırmıştır, hakaret saldırı ve tehdit içeren mesajları, sosyal medya mesajlarını yaygınlaştırmıştır (Sabancı, 2018). İnternet ve sosyal medya yaygın olarak bilinen zorbalık ve saldırganlığa yeni bir boyut kazandırmıştır (Aksaray, 2011).

Zorbalık ve Saldırganlık kavramlarını tanımlayacak olursak: Zorbalık kavramı bir kişiye veya birden çok kişinin kendilerinden daha güçsüz kişilere kasıtlı ve sürekli saldırganca davranışlarda bulunmasıdır. Mağdur kişinin çaresiz olması ve zorba kişinin güçlerini kullanmak için mağdura fizikseli sosyal ve psikolojik acı çektirmesi olarak açıklanmaktadır (Hoşgörür ve Orhan, 2017; Kepenekçi, 2003; Olweus, 1993). Saldırganlık kavramı ise canlıların temel dürtülerinden biri olarak tanımlanmıştır (Gökler,2009). Saldırganlık genellikle başkalarına zarar vermek için kullanılan davranışlar şeklinde açıklanmaktadır (Anderson ve Bushman,2002; Crick ve Grotpeter ,1995).

İnternet ve sosyal medya kullanımı her geçen gün dünyada ve ülkemizde artmaktadır. Bu şekilde yaygın kullanılan iletişim ortamları sorunlu hala gelebilmektedir (Cicioğlu, 2014). BİT teknolojileri öğrenciler denetimsiz, yasaksız ve sınırsız kullanım sunmaktadır. Bu duruma bağlı olarak öğrenciler depresyon, öfke, stres ve düşmanlık gibi sorunlarla karşılaşmaktadır. Bu durumlar da siber saldırganlık kavramını ortaya çıkarmıştır (Colwell ve Kato, 2003; Corcoran, Guckin, ve Prentice ,2015; Hinduja ve Patchin, 2014; Raskauskas ve Stoltz, 2007).

Corcoran, Guckin ve Prentice (2015)’ in araştırması siber saldırganlık kavramını ortaya koyan çalışmalardan biridir. Bu çalışmaya göre internet ve sosyal medyanın kötüye kullanılması sonucu bazı kavramları ortaya çıkmıştır. Bu kavramlardan biri de Siber zorbalık kavramıdır. Siber zorbalık kavramı belirli özelliklerden oluşmaktadır. Siber zorbalığa ait bu özellikler ise davranışın tekrarlanması, zarar vermesi ve siber zorba ile mağdur arasında güç dengesizliğinin olması şeklinde belirtilebilir. Siber saldırganlık kavramsallaştırılırsa ve siber saldırganlığa ait özellikler belirtilirse şu şekilde açıklanabilir: davranışın zarar verme amacı taşıması, zarar veren davranışın tekrarlanmaması ve zarar veren kişi ile zarar gören kişi arasında güç eşitsizliğinin olmaması olarak belirtilebilir. Siber dünyada bir davranış hızlı bir şekilde yayılabilir ve mağdur aynı davranışa bu yayılmadan dolayı maruz kalabilir. Bununla birlikte, siber dünyada “iktidar” yani güç algısı tespit edilememektedir. Bu güç algısı bilgi iletişim teknolojilerini iyi kullanma becerisi ya da siber dünyada anonim olabilme olarak belirtilebilir.

Alanyazında siber saldırgan kavramı farklı araştırmacılar tarafından tanımlanmıştır ve araştırmacılar siber saldırganlık kavramının farklı boyutları üzerinde durmuşlardır. Örneğin, Grigg (2010) siber saldırganlığı, yaşa bakılmaksızın bir kişiye veya bir gruba saldırgan, küçük düşürücü ve istenmeyen davranışları BİT ya da elektronik aygıtlarla kullanarak kasıtlı zarar vermek olarak tanımlamıştır. Wright ve diğ. (2015) siber saldırganlığı siber zorbalığın daha geniş bir tanımı olarak almış ve siber saldırganlıkta davranışın tekrarı üzerinde durulmamıştır. Buna ek olarak, siber saldırganlığın yöntemleri ve bu bağlamda BİT teknolojilerinin kullanıldığından bahsedilmiştir (Corcoran, Guckin ve Prentice, 2015; Patterson, Allan ve Cross 2016 ).

Siber saldırganlık yöntemleri ve davranışları incelendiğinde Urban Dictionary (2019) siber saldırgan ile mağdur arasında güçlerinin aynı olmasının gerekli olmadığından, davranışlar bakımından ise çevrimiçi olan kişinin gözünü korkutmak, duygusal olarak zarar vermek, sahte hesaplarla insanları manipüle etmek gibi davranışlar olarak sıralamıştır. Vale, Pereira, Gonçalves ve Matos (2018) siber saldırganlık davranışlarını doğrudan ve dolaylı olarak ikiye ayırmışlardır. Buna göre doğrudan siber saldırganlık davranışları tehdit etmek, kötü mesajlar göndermek, cinsel taciz gibi eylemler doğrudan bir bireye yapılan siber saldırganlık eylemleri olarak belirtmişlerdir. Dolaylı olarak gerçekleştirilen siber saldırganlık eylemleri ise çevrimiçi dedikodu yapma, isim yayma, sahte hesaplarla hedeflene bireyi izleme “stalking” gibi dolaylı eylemler olarak söylemişlerdir. Bu davranışlardan yola çıkarak yapılan siber saldırganlık tanımlarında saldırganlık eylemlerinin taciz, saldırganlık, iftira, aşağılama veya saptırma gibi özellikler taşıması, eylemde bulunan kişiler arasında güç eşitsizliği aranmaması ve saldırganlıktaki temel amacın hedefteki kişiye acı çektirmek, rahatsızlık vermek gibi amaçların olması siber saldırganlık tanımının çerçevesini oluşturduğunu söylemişlerdir.

Alanyazında incelenen çalışmalar sonunda ortaya çıkan siber saldırganlık tanımı ve çerçevesi ise şu şekilde özetlenebilir: Siber saldırganlık yaşa bakılmaksızın, bir kimseye veya bir gruba BİT araçları ile kasıtlı olarak yapılan ve saldırganlığı yapan bile maruz kalan arasında herhangi bir güç eşitsizliğinin bulunmadığı, siber saldırgan kişi tarafından saldırgan davranış sürekli tekrarlanmayan ve zarar vermek amacıyla yapılan saldırgan davranıştır. Bu tanıma göre siber saldırganlık aynı zamanda alan yazında saldırganlık içeren davranışın birden çok olabildiği fakat süreklilik arz etmeyen ve güç eşitsizliği kavramı bağlamında saldırgan kişinin BİT araçlarını iyi kullanan kişi olarak tanımlandığı bir kavramdır (Bauman, Underwoo ve Card, 2012; Corcoran, 2015; Grigg, 2010; Hinduja ve Patchin, 2009; Kopecký ve Szotkowski, 2017, Modecki, Barber ve Vernon, 2013; Pyzalski, 2012; Schoffstall ve Cohen, 2011; Ybarra, Diener-West ve Leaf, 2007; Ybarra ve Mitchell, 2004;).

Alanyazında Siber saldırganlık ile ilgili yapılan çalışmalara bakıldığında Patterson, Allan ve Cross (2016) çalışmalarında 13-16 yaş aralığındaki bireylerle çalışmıştır. Bu çalışmada odak grup görüşmesi yapılmıştır. Bu yapılan odak grup görüşmelerinde iki tema oluşturulmuştur. Bu temalar siber dünyada fiziksel olarak varlığın tespit edilemeyeceğinden ve bu nedenle saldırganın niyetinin siber dünyada belirlenemeyeceği söylenmiştir. Bu çalışma sonucunda diğer tema ise siber dünyada yetkinin kimde olacağının belli olmaması olduğunu söylemişlerdir. Kokkinos ve Voulgaridou (2017) araştırmasında kişilik özelliklerinin siber saldırganlıktaki rolünü tespit etmeye çalışmışlardır. Bu araştırmada siber saldırganlık tanımını yaparken gerçek hayatında saldırgan bir kişiliğe sahip ergenlerin (14-18 yaş grubu) siber dünyada daha saldırgan olabileceğini belirtmiştir. Aynı zamanda ergenlik döneminde daha saldırgan davranışların olduğu yapılan çalışmalarda görüldüğü üzere bu saldırganlığı siber dünyaya da aktarılabileceği söylenmiştir. Modecki, Barber ve Vernon (2013) çalışmalarında 12-14 yaş grubundaki öğrencilerle çalışmıştır. Bu çalışmada düşük benlik algısı ve yüksek depresif ruh hali ile siber saldırganlık arasında bir ilişki olduğu belirtilmiştir. Bu çalışma sonucunda problemli davranışların gelişimsel dönemlere bağlı olarak arttığını ve buna bağlı olarak siber saldırganlığın bu dönemlerde gerçekleştiği tespit edilmiştir.

Çeşitli ülkelerde ve Türkiye’de alanyazında siber saldırganlık ve siber zorbalık kavramlarının iç-içe geçtiği, çalışmalar görülmüştür. Dünyada siber saldırganlık / siber agresyon kavramı yeni bir kavramdır. Alan yazına bakıldığında Álvarez-García, Barreiro-Collazo, Núñez, ve Dobarro (2016) “CYBA” ve Runions, Bak ve Shaw (2017) “CATQ” adlarında siber saldırganlık kavramı üzerinde duran ölçekleri bulunmaktadır. Ancak Türkiye’de bu kavram ile ilgili ölçek bulunmamaktadır. Bu durum çalışmanın gerekliliğini artırmaktadır.

Bu araştırmanın problemi “Lise öğrencilerinin siber saldırganlık eğilimleri nasıldır?” şeklinde belirlenmiştir. Bu problem doğrultusunda alt problemler ise şu şekilde belirlenmiştir:

1. Siber Saldırganlık Ölçeği geçerli ve güvenilir mi? .

2. Siber Saldırganlık eğilimlerini okul türüne, cinsiyete, internet kullanım süresine göre, yaşa göre, sosyal ağlarda anonim olmasına göre, ebeveynin sosyal ağları kontrol etmesine göre, odaya sahip olmasına göre ve sosyal ağlarda etkileşimli olmasına göre farklılık göstermekte midir?

**Yöntem**

 **Araştırmanın Deseni**

Bu çalışma tarama modelinde yürütülen betimsel ve nicel bir araştırma niteliği taşımaktadır. Tarama modeli ise, “geçmişte ya da halen var olan bir durumu var olduğu şekliyle betimlemeyi amaçlayan bir araştırma yaklaşımıdır” ve bu model araştırmanın konusu olan olayı, bireyi ya da nesneyi kendi koşulları çerçevesinde tanımlamaya çalışır (Karasar, 2010).

**Çalışma Grubu**

 Bu araştırmanın çalışma grubu 2 gruptan oluşmaktadır. Bu gruplar sırasıyla açımlayıcı faktör analizi çalışma grubu ve doğrulayıcı faktör analizi çalışma gruplarıdır. Araştırmanın açımlayıcı faktör analizi grubu 2018-2019 eğitim öğretim yılında öğrenim gören 1573 lise öğrencisinden oluşmaktadır. Doğrulayıcı faktör analizi çalışma grubu 2018-2019 eğitim öğretim yılında öğrenim gören 188 lise öğrencisinden oluşmaktadır.

**Tablo 1**. Açımlayıcı faktör analizi çalışma grubu

|  |  |  |  |
| --- | --- | --- | --- |
| **Okul Türü** | **Okul Adı** | **Öğrenci Sayısı** | **Toplam Öğrenci Sayısı** |
| Anadolu Lisesi | Mesut Özata Anadolu Lisesi | Kadın | 111 | 194 |
| Erkek | 83 |
| Anadolu Lisesi | Atatürk Anadolu Lisesi | Kadın | 127 | 231 |
| Erkek | 104 |
| Fen Lisesi | İMKB Fen Lisesi | Kadın | 101 | 190 |
| Erkek | 89 |
| Ticaret Lisesi | Eminpaşa MTAL | Kadın | 57 | 167 |
| Erkek | 110 |
| Kız Meslek Lisesi | Nene Hatun MTAL | Kadın | 144 | 144 |
| Erkek | - |
| Sağlık Meslek Lisesi | Borsa İstanbul MTAL | Kadın | 189 | 268 |
| Erkek | 79 |
| İmam Hatip Lisesi | Van Anadolu İmam Hatip Lisesi | Kadın | 49 | 118 |
| Erkek | 69 |
| Endüstri Meslek Lisesi | Mehmet Erdemoğlu MTAL | Kadın | 42 | 182 |
| Erkek | 140 |
| Kolej | Hürriyet Koleji | Kadın | 32 | 79 |
| Erkek | 47 |

**Tablo 2**. Doğrulayıcı faktör analizi çalışma grubu)

|  |  |  |  |
| --- | --- | --- | --- |
| Okul Türü | Okul Adı | Öğrenci Sayısı | Toplam Öğrenci Sayısı |
| Ticaret Lisesi | Eminpaşa MTAL | Kadın | 60 | 188 |
| Erkek | 128 |

**Veri Toplama Aracı ve Verilerin Analizi**

Araştırmanın verileri bilgisayar ortamına aktarılarak SPSS ve LISRELL paket programları ile analizler yapılmıştır. Ölçeğin tamamı ve alt boyutları için Cronbach’s alpha güvenirlik katsayısı ile iç tutarlılık katsayısı hesaplanmıştır. Ölçeğin yapı geçerliği için ise doğrulayıcı faktör analizi yapılmıştır. Öğrencilerin toplanan demografik özelliklerine göre t-testi, varyans analizi gibi parametrik analizler yapılmıştır.

Araştırmacılar tarafından alanyazın taraması yapılmıştır. Ancak Türkiye’de siber saldırganlık kavramı ile ilgili geçerli ve güvenilir bir ölçme aracı bulunamamıştır. Bunun üzerine araştırmanın amaçlarına yönelik bir ölçme aracı geliştirmeye karar verilmiştir. Ölçme aracının geliştirilmesinde alanyazının ölçek geliştirme için önerdiği yol izlenmiştir (Crocker ve Algina, 1986; Cohen ve Swerdlik 2013; Şeker ve Gençdoğan, 2014;). Bu kapsamda öncelikle siber saldırganlık) tanımlanmıştır. Álvarez-García ve diğ. (2016) çalışmasında siber saldırganlık özelliği bulunan bir ölçek görülmüştür. Bu ölçeğin maddelerinden yola çıkarak 65 lise öğrencisine “İnternette Karşılaştığınız Olumsuz Durumları Kompozisyon Halinde Yazınız.” görevi verilmiştir. Aynı zamanda Álvarez-García ve diğ. (2016)’nin yaptığı çalışmadaki ölçek maddeleri Türkçeye uzmanlarca çevrilmiştir. Bu çalışmalar kapsamında öğrencilerin yazdığı kompozisyonlardan oluşturulan maddeler ve Álvarez-García ve diğ. (2016) çalışmasındaki kullanılan maddeler bir araya getirilmiştir. Bu kapsamda oluşturulan maddelerin aynı anlama gelecek 3 muadil madde oluşturulmuştur. Bu işlemden sonra 99 maddelik bir ölçek oluşturulmuştur. Alanında uzman bir Psikolojik Rehberlik Danışmanı ile maddeler incelenmiştir, kullanılması uygun maddeler üç alan uzmanına gönderilmiştir gerekli düzenlemeler yapılmış, bazı maddelerdeki ifadeler değiştirilmiş ve dilbilgisi ile ilgili düzeltmeler yapılmıştır. Ölçek yanıtlamaya kolaylık sağlayacak şekilde düzenlendikten sonra 69 madde oluşturulmuştur ve öğrencilere uygulanmaya başlamıştır.

Veriler çalışma kapsamında geliştirilen Siber Saldırganlık Ölçeği ile elde edilmiştir. Yapılan analizler sonucunda ölçek 32 maddeden oluşmaktadır. “SON 3 AY içerisinde aşağıda belirtilen davranışı kaç kez yaptığınızı işaretleyiniz.” sorusuna 0 (Hiç yapmadım) 1(Bir kez yaptım) 2 (İki kez yaptım) 3 (üç kez yaptım) 4 (Dört kez yaptım) şeklinde yanıtlar vermiştir. Ölçeğin nihai halinin 6 tane alt faktörleri vardır. Birinci alt faktörün adı Görsel ve Cinsel Siber Saldırganlık, ikinci alt faktörün adı Huzursuzluk Verme ve Alay Etme, üçüncü alt faktörün adı Kullanıcı Hesabına Yönelik Siber Saldırganlık, dördüncü alt faktörün adı Tehdit, beşinci alt faktörün adı Dışlama ve altıncı alt faktörün adı Sahte Hesap olmuştur. Alt faktörlere ait Cronbach’s Alpha Güvenirlik Katsayıları ise birinci alt faktör 0.905, ikinci alt faktör 0.836, üçüncü alt faktör 0.835, dördüncü alt faktör 0.861, beşinci alt faktör 0.738 ve altıncı alt faktör 0.718 olmuştur. Ayrıca bağımsız değişkenlere göre Demografik bilgi formu oluşturulmuştur.

**Tablo 3**. Siber saldırganlık ölçeğinin faktörlerinin güvenirlik katsayıları

|  |  |  |
| --- | --- | --- |
| **Alt Faktörleri** | **Madde Sayısı** | **Cronbach’s Alpha Güvenirlik Katsayısı** |
| Görsel ve Cinsel Siber Saldırganlık | 8 | 0.905 |
| Huzursuzluk Verme ve Alay Etme | 8 | 0.836 |
| Kullanıcı Hesabına Yönelik Siber Saldırganlık | 7 | 0.835 |
| Tehdit | 3 | 0.861 |
| Dışlama | 3 | 0.738 |
| Sahte Hesap | 3 | 0.718 |

**Bulgular**

**Siber Saldırganlık Ölçeğinin Geçerlik ve Güvenirliğine Ait Bulgular**

Siber saldırganlık ölçeği 1573 öğrenciye uygulanmıştır. Faktör analizi ilk uygulandığında 13 faktörlü bir ölçek olduğu görülmüştür. Faktör analizinde temel bileşenler analiz yöntemi uygulanarak ve maddelerin boyutlara ayrılması için yapılan analiz esnasında varimax eksen döndürmesi (rotation) uygulanmıştır. Alan yazından döndürme yönteminin boyutlaşmada önemli bir aşama olduğu belirtilmiştir (Büyüköztürk,2013; Şeker ve Gençdoğan, 2014). Farklı boyutlara aynı yük verilen maddeler çıkarılmıştır. Bu yöntem 20 kez tekrarlanmıştır ve bir defada birden fazla madde çıkarılmıştır. Bu yöntemle boyut sayısı 6’ya düşürülmüştür ve madde sayısı 32’ye düşürülmüştür. Bu yöntemle 2, 5, 8, 9, 14, 15, 16, 18, 20, 24, 25, 28, 29, 30, 31, 36, 37, 38, 39, 40, 41, 42, 44, 46, 47, 49, 50, 52, 53, 54, 56, 57, 59, 60, 62, 63, 67 numaralı maddeler çıkarılmıştır. Kalan 32 madde ile faktör analizine devam edilmiştir. Varimax eksen döndürmesi sonucunda en son oluşan 6 alt faktör varyansın %59,35’ini açıkladığı belirlenmiştir. Maddeler çıkarıldıktan ve alt faktörler oluştuktan sonra ortaya çıkan yığın grafiği görünümü şu şekildedir:



Şekil 1. *Son analiz sonucuna göre özdeğer grafiği*

Şekil 1’de ortaya çıkan yığın grafiğinde 6. faktörden sonra eğimin plato yaptığı görülmüştür.

Son analiz sonucuna göre faktör bileşenlerinin varyans katkıları şu şekildedir:

**Tablo 4.** Son analize göre toplam varyans tablosu

|  |  |  |  |
| --- | --- | --- | --- |
| **Bileşenler** | **İlk Özdeğerler** | **Yüklerin Kareleri Toplamı Çıkarımı** | **Döndürülmüş Kare Yüklerin Toplamları** |
| **Toplam** | **% Varyans** | **% Birikimli** | **Toplam** | **% Varyans** | **% Birikimli** | **Toplam** | **% Varyans** | **% Birikimli** |
| 1 | 11,334 | 35,419 | 35,419 | 11,334 | 35,419 | 35,419 | 4,949 | 15,466 | 15,466 |
| 2 | 2,313 | 7,227 | 42,647 | 2,313 | 7,227 | 42,647 | 3,858 | 12,057 | 27,523 |
| 3 | 1,520 | 4,749 | 47,396 | 1,520 | 4,749 | 47,396 | 3,354 | 10,480 | 38,003 |
| 4 | 1,390 | 4,344 | 51,740 | 1,390 | 4,344 | 51,740 | 2,408 | 7,525 | 45,528 |
| 5 | 1,319 | 4,121 | 55,861 | 1,319 | 4,121 | 55,861 | 2,335 | 7,298 | 52,826 |
| 6 | 1,117 | 3,489 | 59,350 | 1,117 | 3,489 | 59,350 | 2,088 | 6,524 | 59,350 |

Tablo 4’te görüldüğü üzere ilgilenilen özelliği ölçek (Siber saldırganlık) altı faktör altında ve %59,35 varyans ile açıklanmaktadır. Ölçek bu haliyle alanyazında (Büyüköztürk, 2013) kabul edilen düzeyde açıklama yapmaktadır. Siber Saldırganlık Ölçeği için yapılan yapı geçerliği çalışmaları kapsamında birinci çalışma grubu ile açımlayıcı faktör analizi (AFA) ikinci çalışma grubu ile verileri ile de doğrulayıcı faktör analizi (DFA) yapılmıştır. Doğrulayıcı faktör analizi LISREL 8.8 ile programın önerileri doğrultusunda iyileştirmeler yapılmıştır. **Tablo 5.** DFA sonucunda elde edilen uyum değerleri

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **X2** | **Sd** | **X2/ Sd** | **RMSEA** | **CFI** | **NNFI** | **NFI** | **AGFI** | **GFI** |
| 898,79 | 433 | 2,07 | 0,076 | 0,94 | 0,93 | 0,91 | 0,72 | 0,77 |

DFA’nın temel amacı faktörler arasındaki ilişki, faktörlerin birbirlerinden bağımsız olup olmadığını sınamaktır (Erkorkmaz, Etikan, Demir, Özdamar ve Sanisoğlu, 2013). Bu bağlamda Siber Saldırganlık Ölçeği 6 faktörlü yapısının doğrulayıcı faktör analizinden elde edilen uyum istatistiklerine göre doğrulandığı söylenebilir.

Tablo 5’e bakıldığında DFA sonucundan elde edilen ki-kare ve serbestlik derecesi değerlerinin x2= 898,79, sd=433 olduğu ve x2/sd= 2,07 oranının elde edildiği görülmüştür ve aynı zamanda p<0,00 ile anlamlılık değeri tespit edilmiştir. Seçilen örneklemden elde edilen veriler modifikasyonla birlikte bulunan oranın 3’ün altında çıkması mükemmel uyum olduğunu göstermektedir (Jöreskog ve Sörbom, 1993; Sümer, 2000). Bu araştırmada DFA sonucunda elde edilen sonuçta görüldüğü gibi model ile veri arasında mükemmel bir uyum olduğu söylenebilir. RMSEA indeksinin 0,05 ve daha küçük bir değer olması gerekmektedir. Ancak bu değer 0,08’e kadar da kabul edilebilir bir değerdir (Bayrak, 2010). Bu çalışmadaki RMSEA değeri 0,076 olarak bulunan kabul edilebilir bir değer olduğu söylenebilir. DFA’ da AGFI (Adjusted Goodness of Fit Index) değeri 0 ile 1 arasında değer almaktadır. Bu değer 1’e yaklaştıkça iyi uyuma işaret etmektedir (Erkorkmaz, Etikan, Demir, Özdamar ve Sanisoğlu, 2013). DFA analizinde AGFI indeksi 0,72 bulunmuştur. AGFI değeri örneklem arttıkça artar (Doğan, 2013). Bu çalışmada DFA için çalışma grubu 188 kişi olmuştur. AGFI değerinin artması için çalışma grubundaki katılımcı sayısı artması gerekmektedir. Bu bağlamda AGFI değeri model veri uyumunda kabul edilebilir ölçüde olduğu söylenebilir. DFA’da NNFI (Non-Normed Fit Index), CFI (Comparative Fit Index), NFI (Normed Fit Index) değerlerinin 0,95 ve üzerinde olması model veri uyumunun “mükemmel uyuma” karşılık geldiğinin göstergesidir (Sümer, 2000; Erkorkmaz, Etikan, Demir, Özdamar ve Sanisoğlu, 2013). Bu bağlamda yapılan analiz sonucunda NNFI=0,93, NFI=0,91 ve CFI=0,94’tür. Bu sonuçlara göre 0-1 aralığındaki yüksek değerler iyi uyumu göstermektedir (Erkorkmaz, Etikan, Demir, Özdamar ve Sanisoğlu, 2013).

Bu çalışmada yapılan analizler öğrencilerin siber saldırganlık ortalama puanları üzerinden yapılmıştır ve 6 alt boyut bu kapsamda incelenmemiştir.

Lise Öğrencilerinin Yaşına Göre Siber Saldırganlık Eğilimleri

**Tablo 6**. Siber saldırganlık ölçeğinin yaşa göre karşılaştırılmasının gruplar arası sonuçları

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Varyasın****Kaynağı** | **Kareler****Toplamı** | **sd** | **Kareler****Ortalaması** | **F** | **P** |
| **Gruplararası** | 1,253 | 3 | 0,418 | 1,766 | 0,152 |
| **Gruplariçi** | 371,043 | 1569 | 0,236 |
| **Toplam** | 372,296 | 1572 |  |

Tablo 6’da görüldüğü üzere öğrencilerin yaşlarının siber saldırganlık eğilimlerinin yaşa göre anlamlı bir fark oluşturmadığı görülmüştür (p>0,05). Bu sonucun katılımcıların yaşlarının oransal olarak yakın olmasından kaynaklanacağı gibi aynı zamanda siber dünyada yaşın artık bir önemi olmadığını da gösterebilir..

Lise Öğrencilerinin Okul Türüne Göre Siber Saldırganlık Eğilimleri

**Tablo 7**. Siber saldırganlık ölçeğinin okul türüne göre karşılaştırılmasına ait betimsel istatistikler

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Okul Türü** | **N** | **%** | **X̅** | **SS** |
| **Anadolu Lisesi (AL)** | 425 | 27 | 0,2963 | 0,41295 |
| **Fen Lisesi (FL)** | 190 | 12.1 | 0,3497 | 0,50325 |
| **Karma Meslek Lisesi (ML)** | 349 | 22.2 | 0,4110 | 0,58992 |
| **Kız Meslek Lisesi (KML)** | 144 | 9.2 | 0,1539 | 0,30183 |
| **Sağlık Meslek Lisesi (SML)** |  268 | 17 | 0,3102 | 0,54810 |
| **İmam Hatip Lisesi (İML)** |  118 | 7.5 | 0,2749 | 0,37495 |
| **Özel Eğitim Kurumu (ÖEK)** | 79 | 5 | 0,3663 | 0,41797 |
| **Toplam** | 1573 | 100 | 0,3194 | 0,48665 |

Tablo 7’de katılımcıların okul türleri, frekans ve yüzdelik değerleri gösterilmiştir. Bu değerlere bakıldığında Anadolu Lisesine devam eden öğrencilerin siber saldırganlık puanı ortalaması (SSPO) 0,2963, Fen Lisesine devam eden öğrencilerin SSPO 0,3497, Karma Meslek Lisesine devam eden öğrencilerin SSPO 0,4110, Kız Meslek Lisesine devam eden öğrencilerin SSPO 0,1539, Sağlık Meslek Lisesine devam eden öğrencilerin SSPO 0,3102, İmam Hatip Lisesine devam eden öğrencilerin SSPO 0,2749 ve Özel Eğitim Kurumuna devam eden öğrencilerin SSPO 0,3663 olmuştur.

**Tablo 8.** Siber saldırganlık ölçeğinin okul türüne göre karşılaştırılmasının gruplar arası sonuçları

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Varyasın** **Kaynağı** | **Kareler** **Toplamı** | **Sd** | **Kareler****Ortalaması** | **F** | **P** | **Anlamlı Fark** |
| **Gruplararası** | 7,706 | 6 | 1,284 | 5,517 | 0,000\* | FL-KML; ML-KML; |
| **Gruplariçi** | 364,590 | 1566 | 0,233 | KML-FL-ML |
| **Toplam** | 372,296 | 1572 |  |  |

\*p<0,05.

Tablo 8’e bakıldığında okul türünün, öğrencilerin siber saldırganlık puanları arasında anlamlı bir fark olduğunu göstermektedir (F(6,1566)=5,517, p<0,05). Başka bir deyişle, öğrencilerin siber saldırganlık eğilimleri okul türüne göre değişmektedir. Okul türlerinin hangileri arasında bir fark olduğu anlamlı fark sütununda gösterilmiştir. Bu bağlamda yapılan birimler arasındaki farkların hangi gruplar arasında fark olduğunu bulabilmek için yapılan Scheffe testinin sonuçlarına göre Fen Lisesi öğrencileri ile Kız Meslek Lisesi öğrencileri arasında anlamlı fark Fen Lisesi öğrencisi lehine çıkmıştır ve Meslek lisesi öğrencileri ile Kız Meslek Lisesi öğrencileri arasında Meslek Lisesi lehine anlamlı bir fark çıkmıştır. Kız Meslek Lisesi ile Fen Lisesi ve Meslek Lisesi öğrencileri arasında anlamlı fark bulunmuştur. Bu farkta Kız Meslek Lisesi öğrencilerinin siber saldırganlıkları diğer öğrencilere göre daha düşüktür.

Lise Öğrencilerinin Cinsiyetine Göre Siber Saldırganlık Eğilimleri

**Tablo 9.** Siber saldırganlık ölçeğinin cinsiyete göre karşılaştırılmasına ait betimsel istatistikler

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Cinsiyet** | **N** | **X̅** | **SS** | **sd** | **t** | **p** |
| **Kadın** | 852 | 0,2372 | 0,36536 | 1571 | 7,404 | 0,000\* |
| **Erkek** | 721 | 0,4165 | 0,58469 |
| **Toplam** | 1573 |  |  |  |  |  |

\*p<0,05

Tablo 9’da Siber Saldırganlık Ölçeğinden elde edilen toplam puanların cinsiyete göre anlamlı bir fark gösterdiği görülmektedir (t(1571)=7,404, p<0,05). Bu bulgu cinsiyet değişkeni açısından katılımcıların siber saldırganlıklarının farklılaştığı söylenebilir. Bu farklılaşmanın erkek öğrenciler lehine olduğu görülmüştür.

Lise Öğrencilerinin İnternet Kullanım Süresine Göre Siber Saldırganlık Eğilimleri

**Tablo 10.** Siber saldırganlık ölçeğinin internet kullanım süresine göre karşılaştırılmasına ait betimsel istatistikler

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **İnternet Kullanım Süresi** | **N** | **%** | **X̅** | **SS** |
| **1 saatten az (a)** | 582 | 37 | 0,1651 | 0,32799 |
| **1 saat (b)** | 241 | 15,3 | 0,2121 | 0,32319 |
| **2 saat (c)** | 254 | 16,1 | 0,3182 | 0,36949 |
| **3 saat (d)** | 177 | 11,3 | 0,4345 | 0,45948 |
| **4 saat (e)** | 89 | 5,7 | 0,4747 | 0,52146 |
| **4 saat ve üzeri (f)** | 230 | 14,6 | 0,6750 | 0,77879 |
| **Toplam** | 1573 |  |  |  |

Tablo 10’da katılımcıların internet kullanım süreleri, frekans ve yüzdelik değerleri gösterilmiştir. Bu değerlere bakıldığında 1 saatten az kullanan öğrencilerin siber saldırganlık puan ortalamaları (SSPO) 0,1651; 1 saat kullanan öğrencilerin SSPO 0,2121; 2 saat kullanan öğrencilerin SSPO 0,3182; 3 saat kullanan öğrencilerin SSPO 0,4345; 4 saat kullanan öğrencilerin SSPO 0,4747 ve 4 saat ve üzeri kullanan öğrencilerin SSPO 0,6750 olmuştur.

**Tablo 11.** Siber saldırganlık ölçeğinin internet kullanım süresine göre karşılaştırılmasının gruplar arası sonuçları

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Varyasın****Kaynağı** | **Kareler** **Toplamı** | **Sd** | **Kareler****Ortalaması** | **F** | **P** | **Anlamlı Fark** |
| **Gruplararası** | 50,204 | 5 | 10,041 | 48,849 | 0,000\* | a-b,d,e,f;  b-d,e,f;  c-a,f;d-a,b,f;e-a,b,f;f-a,b,c,d,e |
| **Gruplariçi** | 322,092 | 1567 | 0,206 |
| **Toplam** | 372,296 | 1572 |  |

\*p<0,05

Tablo 11’e bakıldığında analiz sonuçları, öğrencilerin siber saldırganlık eğilimlerinin internet kullanım sürelerine göre anlamlı bir fark olduğunu göstermiştir (F(5,1567)=48,849, p<0,05). Bu bağlamda öğrencilerin siber saldırganlık eğilimlerinin internet başında geçirdikleri süreye bağlı olarak anlamlı bir şekilde değiştiği söylenebilir. İnternet kullanım süreleri arasındaki farkları tespit edebilmek için Scheffe testi uygulanmıştır. Bu testin sonucunda göre gruplar arasındaki anlamlı fark olanlar Tablo 11’de belirtilmiştir.

Lise Öğrencilerinin Sosyal Ağlarda Anonim Olmasına Göre Siber Saldırganlık Eğilimleri

Tablo 12.Siber saldırganlık ölçeğinin sosyal ağlarda anonim olmasına göre karşılaştırılmasına ait betimsel istatistikler

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sosyal Ağlarda Anonim Olma** | **N** | **%** | **X̅** | **SS** |
| **Evet (E)** | 1035 | 65,8 | 0,3557 | 0,47116 |
| **Hayır (H)** | 346 | 22 | 0,1372 | 0,39709 |
| **Bazılarında (B)** | 192 | 12,2 | 0,3194 | 0,48665 |
| **Toplam** | 1573 |  |  |  |

Tablo 12’de katılımcıların sosyal ağlarda anonim olmaları (Sosyal ağlarda kendi kimlikleriyle hesap açmamaları durumu), frekans ve yüzde değerleri gösterilmiştir. Bu değerlere bakıldığında “Evet” cevabını verenlerin siber saldırganlık puan ortalaması (SSPO) 0,3557, “Hayır” cevabını verenlerin SSPO 0,1372 ve “Bazılarında” cevabını verenlerin SSPO 0,3194 olmuştur.

Tablo 13.Siber saldırganlık ölçeğinin sosyal ağlarda anonim olmasına göre karşılaştırılmasının gruplar arası sonuçları

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Varyasın****Kaynağı** | **Kareler** **Toplamı** | **Sd** | **Kareler****Ortalaması** | **F** | **P** | **Anlamlı Fark** |
| **Gruplararası** | 16,235 | 2 | 8,117 | 35,792 | 0,000\* | E-H,B; H-E-B; B-E,H |
| **Gruplariçi** | 256,061 | 1570 | 0,227 |
| **Toplam** | 372,296 | 1572 |  |

\*p<0,05

Tablo 13’teki analiz sonuçları sosyal ağlarda anonim olmaları ile siber saldırganlık puanları arasında anlamlı fark olduğunu göstermektedir (F(2,1570)=35,792, p<0,05). Başka bir deyişle öğrencilerin siber saldırganlık eğilimleri sosyal ağlarda anonim olma durumuna göre değişmektedir. “Evet” cevabını veren öğrencilerin SSPO “Hayır” ve “Bazılarında” cevabını verenlerin ortalamasından farklıdır. “Hayır” cevabını veren öğrencilerin SSPO “Evet” ve “Bazılarında” cevabını verenlerin ortalamasından farklıdır. “Bazılarında” cevabını veren öğrencilerin SSPO “Hayır” ve “Evet” cevabını verenlerin ortalamasından farklıdır.

Ebeveynin Sosyal Ağları Kontrol Etme Durumuna Göre Siber Saldırganlık Eğilimleri

Tablo 14.Siber saldırganlık ölçeğinin ebeveynin sosyal ağları kontrol etme durumuna göre karşılaştırılmasına ait betimsel istatistikler

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ebeveynin Sosyal Ağları Kontrol Etmesi** | **N** | **X̅** | **S** | **sd** | **t** | **p** |
| **Evet** | 446 | 0,2904 | 0,45520 | 1571 | 1,490 | 0,101\* |
| **Hayır** | 1127 | 0,3309 | 0,49828 |
| **Toplam** | 1573 |  |  |  |  |  |

\*p>0,05

Tablo 14’te Siber Saldırganlık Ölçeğinden elde edilen toplam puanların ölçeğinin ebeveynin sosyal ağları kontrol etme durumuna göre anlamlı bir fark olmadığı görülmektedir (t(1571)=1,490, p>0,05). Sosyal ağları ebeveyni tarafından kontrol edilen öğrencilerin siber saldırganlık puan ortalaması (SSPO) 0,2904, kontrol edilmeyen öğrencilerin SSPO 0,3309’dur. Analiz sonucuna göre anlamlı bir fark görülmediği anlaşılmaktadır.

Lise Öğrencilerinin Kendilerine Ait Oda Olup Olmamasına Göre Siber Saldırganlık Eğilimleri

Tablo 15.Siber saldırganlık ölçeğinin öğrencilerin odaları olmasına göre karşılaştırılmasına ait betimsel istatistikler

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Oda** | **N** | **X̅** | **S** | **sd** | **t** | **p** |
| **Var** | 949 | 0,3837 | 0,53837 | 1571 | 6,549 | 0,000\* |
| **Yok** | 624 | 0,2216 | 0,37504 |
| **Toplam** | 1573 |  |  |  |  |  |

\*p<0,05

Tablo 15’de Siber Saldırganlık Ölçeğinden elde edilen toplam puanların ölçeğinin öğrencilerin odası olmasına göre anlamlı bir fark olduğu görülmektedir (t(1571)=6,549, p<0,05). Araştırmaya katılan öğrencilerden odaya sahip olan öğrencilerin siber saldırganlık puan ortalaması (SSPO) 0,3837; odaya sahip olmayan öğrencilerin SSPO 0,2216’dır. Öğrencilerin siber saldırganlık eğilimleri odaya sahip olmasına göre anlamlı bir fark göstermektedir (p<0,05). Bu sonuca göre öğrencinin odaya sahip olması siber saldırganlık üzerinde etkisi olduğu görülmektedir.

Lise Öğrencilerinin Sosyal Ağlarda Etkileşimli Olmasına Göre Siber Saldırganlık Eğilimleri

Tablo 16.Siber saldırganlık ölçeğinin öğrencilerin sosyal ağlarda etkileşimli olmasına göre karşılaştırılmasına ait betimsel istatistikler

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sosyal Ağlarda Etkileşimli Olma** | **N** | **X̅** | **S** | **sd** | **t** | **p** |
| **Evet** | 715 | 0,4680 | 0,56149 | 1567 | 11,477 | 0,000\* |
| **Hayır** | 854 | 0,1957 | 0,37207 |
| **Toplam** | 1573 |  |  |  |  |  |

\*p<0,05

Tablo 16’da Siber Saldırganlık Ölçeğinden elde edilen toplam puanların ölçeğinin öğrencilerin sosyal ağlarda etkileşimli olmasına göre göre anlamlı bir fark olduğu görülmektedir (t(1567)=6,549, p<0,05). Araştırmaya katılan öğrencilerden sosyal ağlarda etkileşimli olanların siber saldırganlık puan ortalaması (SSPO) 0,4680; sosyal ağlarda etkileşimli olmayan öğrencilerin SSPO 0,1957’dir. Öğrencilerin siber saldırganlık eğilimleri sosyal ağlarda etkileşimli olmasına göre anlamlı bir fark göstermektedir (p<0,05). Bu sonuca göre öğrencinin sosyal ağlarda etkileşimli olması siber saldırganlık üzerinde etkisi olduğu söylenebilir.

**Tartışma ve Sonuç**

Yapılan çalışmada siber saldırganlık ölçeği geliştirilmiş ve bu bağlamda lise öğrencilerinin siber saldırganlık eğilimleri demografik değişkenlere göre belirlenmeye çalışılmıştır.

Araştırmanın geçerlik ve güvenirlik çalışmaları kapsamında veriler SPSS 22 ve LISREL 8.80 programlarında analiz edilmiştir. BÖTE bölümünden üç doktoralı uzmanın görüşüne ölçeğin ilk hali ile başvurulmuştur. Uzman görüşleri çerçevesinde ölçek düzenlenmiştir. Geçerlik kapsamında yapı geçerliği analiz edilmiştir. Yapı geçerliği sağlaması için öncelikler birinci çalışma grubu ile (1573 öğrenci) açımlayıcı faktör analizi (AFA) ikinci çalışma grubu ile verileri ile de doğrulayıcı faktör analizi (DFA) yapılmıştır. Açımlayıcı faktör analizine uygunluğun ve örneklem büyüklüğü yeterliliğinin belirlenmesi amacıyla Kaiser-Meyer-Olkin ve Bartlett testi uygulanmıştır. Açımlayıcı faktör analizi yaparken faktör yükü düşük olan maddeler çıkarılmış ve bütün analizler sonucunda elde edilen Siber Saldırganlık Ölçeği toplam varyansın %59.35’ini açıklayan altı faktör altında toplanan 32 maddelik bir ölçek oluşturulmuştur. Ölçeğin alt faktörlerinin güvenirlik değerleri: Görsel ve Cinsel Siber Saldırganlık adlı alt faktörün güvenirlik katsayısı 0.905, Huzursuzluk Verme ve Alay Etme adlı alt faktörün güvenirlik katsayısı 0.836, Kullanıcı Hesabına Yönelik Siber Saldırganlık adlı alt faktörün güvenirlik katsayısı 0,835, Tehdit adlı alt faktörün güvenirlik katsayısı 0.861, Dışlama adlı alt faktörün güvenirlik katsayısı 0.738 ve Sahte Hesap adlı alt faktörün güvenirlik katsayısı 0.718 olarak tespit edilmiştir. Doğrulayıcı faktör analizi ile programın önerileri doğrultusunda iyileştirmeler yapılmıştır. Siber Saldırganlık ölçeğinin doğrulayıcı faktör analizinin uyum indeksleri: RMSEA değeri 0,076, AGFI indeksi 0,72, NNFI değeri 0,93, NFI değeri 0,91 ve CFI değeri 0,94’tür. Siber Saldırganlık Ölçeği 6 faktörlü yapısının doğrulayıcı faktör analizinden elde edilen uyum istatistiklerine göre doğrulanmıştır. Bu verilerden hareketle ölçeğin siber saldırganlık ölçümü yapabilmek için geçerli ve güvenilir olduğu görülmüştür.

Araştırma bulgularında siber saldırganlık ile yaş arasında anlamlı bir fark olmadığı görülmüştür. Bu bağlamda alan yazında yapılan araştırmalarda (Patterson, Allan ve Cross, 2016; Wright ve Li, 2013; Schoffstall ve Cohen, 2011; Pornari ve Wood, 2010; Toledano, Werch ve Wiens, 2015) siber saldırganlık ile yaş arasında anlamlı bir fark olmadığını ortaya koymuştur. Buna göre yaşa göre anlamlı bir farklılık göstermemesinin muhtemel nedeni öğrencilerin yaşlarının birbirine yakın olmasından kaynaklandığı söylenebilir.

Siber saldırganlık ile cinsiyet arasında anlamlı bir fark olup olmadığı ile ilgili alanyazında tartışmalar bulunmaktadır. Buna göre Alvarez-Garcia, Barreiro-Collazo ve Nuez (2017) ergenlerle yaptığı araştırma sonucunda anlamlı bir fark bulunmadığını söylemiştir. Ancak siber saldırganlık ile cinsiyet arasında anlamlı bir fark bulunduğunu söyleyen çalışmalar bulunmaktadır (Lamb, 2015; Musharraf ve Anis-ul-Haque, 2018; Wright, Aoyama, Kamble, Li, Soudi, Lei ve Shu, 2015). Bu sonuçlara bağlı olarak siber saldırganlık ile cinsiyet arasında anlamlı bir fark olup olmadığı ile ilgili çalışmalar tutarlı bir şekilde erkeklerde daha yüksek olduğunu söylemektedir. Bu çalışmada da yapılan analiz sonucunda erkeklerin siber saldırganlık puan ortalamalarının yüksek olduğu görülmüştür. Bu çalışma bu anlamda alanyazını desteklemektedir. Buna bağlı olarak erkeklerde siber saldırganlık eğiliminin daha yüksek olmasının nedeni internet kullanım süresi, ebeveynlerin internet kullanımı, en çok kullanılan sosyal ağlar gibi nedenler olabileceğini söylenebilir. Bu bağlamda öğrencilere bilinçlendirici eğitimlerin verilmesi önerilebilir.

Sosyal ağlarda anonim olmaya göre siber saldırganlık ve kullandıkları sosyal ağlara göre siber saldırganlık arasında anlamlı bir fark görülmüştür. Bu bağlamda alan yazın incelendiğinde sosyal ağları kullanımla ilgili Mishna, Regehr, Lacombe-Duncan, Daciuk, Fearing ve Van Wert (2018) çalışmalarında siber dünyada anonim olan katılımcıların siber saldırganlık eğilimleri ile ilgili anlamlı bir fark görülmüştür. Araştırmanın bulgularına bakıldığında siber dünyada anonim olma, sahte hesap kullanma lise öğrencileri arasında gittikçe artan bir durum olduğu söylenebilir. Siber dünyada bunun bir suç olduğu öğrencilere anlatılabilir. Bu kapsam bilişim suçları ile ilgili bilgiler öğrencilere sunulabilir. Bu sonuçlardan hareketle bilinçli internet kullanma rehberi hazırlanabilir, ailelere Bu rehber dağıtılabilir, bilinçli internet kullanımı ile ilgili seminerler ailelere ve öğrencilere verilebilir.

Öğrencilerin odaya sahip olmasına göre siber saldırganlık arasında anlamlı bir fark görülmüştür. Bu bağlamda alan yazındaki çalışmalar incelendiğinde Law, Shapka ve Olson (2010) odası olan ve aynı zamanda odasında kendine ait bilgisayar sahibi olan kişilerin siber saldırganlıklarının arttığını belirtmişlerdir. Bu bağlamda bu araştırmada da bir odaya sahip olma ile siber saldırganlık arasında anlamlı bir fark tespit edilmiştir. Demografik olarak hem odaya sahip olma hem de odada bilgisayar bulunma değişkenleri de ayrı ayrı incelenebilir.

Okul türüne göre siber saldırganlık düzeyinin değiştiği görülmüştür. Bu bağlamda alan yazındaki çalışmalar incelendiğinde (Schoffstall ve Cohen, 2011; Parti, Kiss ve Koplányi, 2018; Wright ve Li, 2013) bu sonucu destekleyen çalışmalar olduğu görülmektedir. Alanyazında yapılan çalışmalar incelendiğinde üniversite öğrencileri, lise öğrenciler, ilkokul öğrencileri arasında farklı okul türleri ve farklı yaş grupları arasında yapılan çalışmalar da bu sonucu desteklemektedir.

Ebeveynlerin sosyal ağları kontrol etme durumu ile siber saldırganlık arasında anlamlı fark olmadığı görülmüştür. Alanyazın incelendiğinde (Goldstein, 2016; Law, Shapka ve Olson, 2010; Vale, Pereira, Gonçalves ve Matos, 2018; Wright, 2015) farklı sonuçlara ulaşmıştır. Goldstein (2016) çalışmasında ebeveynlerin internet kullanırken ergenlere olan yaklaşımı kontrol edilmiştir. Bu kapsamda siber saldırgan arkadaşları olan ya da ailelerinin denetimleri dışında çevrimiçi ortamda sosyalleşen ergenlerde siber saldırganlık riskinin arttığı görülmüştür. Vale, Pereira, Gonçalves ve Matos (2018) çalışmasında ebeveyn tutumunun siber saldırganlığı etkilediği görülmüştür. Bu çalışmada ise ebeveyn tutumunun siber saldırganlık üzerinde anlamlı farkı görülmemiştir. Bunun nedeni kültürel yapı olarak söylenebilir ayrıca bu çalışmalara bağlı olarak ebeveynlerin siber dünyaya bakış açısının değişmesi gerektiği söylenebilir.

İnternet kullanım süresi ile siber saldırganlık arasında anlamlı bir fark görülmüştür. Bu sonuçla ilgili araştırmalar genellikle internet bağımlılığı üzerinde yoğunlaşmıştır. Alanyazına bakıldığında (Erdur-Baker ve Kavşut, 2007; Peker, Eroğlu, ve Ada, 2012; Türkoğlu, 2013) siber zorbalık ile internet kullanım süresi arasında anlamlı fark tespit edilmiştir. Siber saldırganlık ile internet kullanım süresi arasındaki anlamlı fark alanyazına bu anlamda katkıda bulunmuştur. Aynı zamanda internet kullanım süresinin azaltılması ile siber saldırganlığın azalabileceği ya da interneti doğru kullanımla ilgili eğitimler ile bu durumun azaltılabileceği söylenebilir.

Sosyal ağlarda etkileşim ile siber saldırganlık arasında anlamlı bir fark görülmüştür. Alanyazındaki araştırmalar (O'Keeffe ve Clarke-Pearson, 2011; Whittaker ve Kowalski, 2015) bu sonucu desteklemektedir. Alanyazına bakıldığında Kwan ve Skoric (2013) Facebook’u aktif kullananlar; Hosseinmardi, Mattson, Rafiq, Han, Lv ve Mishra (2015) ise Instagram’ı aktif kullananların siber saldırganlık eğilimlerinin fazla olduğunu belirtmişlerdir. Sosyal ağ paylaşma durumu ile siber saldırganlık arasında anlamlı bir fark görülmüştür. Alanyazında Mesch (2009) sosyal ağlarda aktif olma ile ilgilenmiştir. Buna göre bu araştırma sosyal ağ türü ve siber saldırganlık eğilimi ilişkisini inceleyen araştırma olarak alanyazına katkı sağlamıştır. Ebeveynin sosyal ağları kontrol etme durumu ile siber saldırganlık arasında anlamlı bir fark olmadığı görülmüştür. Alanyazında ise durum tam tersidir (Legate, Weinstein ve Przybylski, 2019; Katz, Lemish, Cohen ve Arden, 2019) Ebeveynin internet kullanması ile siber saldırganlık arasında anlamlı bir fark olduğu görülmüştür. Alanyazındaki çalışmalar incelendiğinde (Baldry, Sorrentino ve Farrington, 2019; Elsaesser, Russell, Ohannessian ve Patton, 2017; Horner, Asher ve Fireman, 2015; Nocentini, Fiorentini, Di Paola ve Menesini, 2018) ebeveynlerin siber dünyaya katılımlarının önemli olduğu söylemişlerdir.

Bu çalışmanın sonuçlarına bağlı olarak alanyazına çeşitli önerilerde bulunulabilir. Örneğin siber saldırganlık ile ilgili ebeveyn tutumu üzerinde durulabilir, okul türlerindeki bu farklılığın nedeni sosyolojik anlamda araştırılabilir, internet kullanım süresi ve siber saldırganlık arsındaki bu anlamlı farkı destekleyecek araştırmalar yapılabilir. Bu sonuçlardan hareketle bilinçli internet kullanma rehberi hazırlanabilir, ailelere bu rehber dağıtılabilir, bilinçli internet kullanımı ile ilgili seminerler ailelere ve öğrencilere verilebilir.

**Makalenin Bilimdeki Konumu**

Bilgisayar ve Öğretim Teknolojileri Eğitimi

**Makalenin Bilimdeki Özgünlüğü**

Alanyazında siber saldırganlık kavramı çalışmanın yapıldığı tarih itibariyle henüz incelenmemiş ve genel olarak siber zorbalık kavramına rastlanmıştır. Ancak siber saldırganlık ölçek oluşturma çalışması ile ilgili Türkçe alanyazında yeterli çalışmanın yer almadığı tespit edilmiştir. Bu nedenle lise öğrencilerine uygulanan ve geliştirilen bu ölçek kavramın alanyazında kullanılması ve boyutları açısından incelemeye alınabilmektedir

**Kaynaklar**

Akkoyunlu, B. (1995). Bilgi teknolojilerinin okullarda kullanımı ve öğretmenlerin rolü. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, *11*(11), 105-109

Aksaray, P. D. S. (2011). Siber zorbalık. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *20*(2), 405-432.

Álvarez-García, D., Barreiro-Collazo, A., & Núñez, J. C. (2017). Cyberaggression among adolescents: Prevalence and gender differences. *Comunicar*, *25*(50), 89-97. https://doi.org/10.3916/C50-2017-08

Anderson, C. A., & Bushman, B. J. (2002). Human aggression. *Annual review of psychology*, *53*. 27-51. https://[10.1146/annurev.psych.53.100901.135231](http://dx.doi.org/10.1146/annurev.psych.53.100901.135231)

Baldry, A. C., Sorrentino, A., & Farrington, D. P. (2019). Cyberbullying and cybervictimization versus parental supervision, monitoring and control of adolescents' online activities. *Children and Youth Services Review*, *96*, 302-307. <https://doi.org/10.1016/j.childyouth.2018.11.058>

Bauman, S., Underwood, M. K., & Card, N. A. (2012). Definitions: Another perspective and a proposal for beginning with cyberaggression. In *Principles of Cyberbullying Research: Definitions, Measures, and Methodology* (pp. 41-45). Taylor and Francis. <https://doi.org/10.4324/9780203084601>

Corcoran, L., Guckin, C. M., & Prentice, G. (2015). Cyberbullying or cyber aggression?: a review of existing definitions of cyber-based peer-to-peer aggression. *Societies*, *5*(2), 245-255. https://doi.org/[10.3390/soc5020245](http://dx.doi.org/10.3390/soc5020245)

Crick, N. R., & Grotpeter, J. K. (1995). Relational aggression, gender, and social‐psychological adjustment. *Child development*, *66*(3), 710-722. https://doi.org/10.2307/1131945

Elsaesser, C., Russell, B., Ohannessian, C. M., & Patton, D. (2017). Parenting in a digital age: A review of parents' role in preventing adolescent cyberbullying. *Aggression and violent behavior*, *35*, 62-72. <https://doi.org/10.1016/j.avb.2017.06.004>

Erdur-Baker, Ö., & Kavşut, F. (2007). Akran zorbalığının yeni yüzü: Siber zorbalık. *Eurasian Journal Of Educational Research (EJER)*, *27*. 31-42

Goldstein, S. E. (2015). Parental regulation of online behavior and cyber aggression: adolescents’ experiences and perspectives. *Cyberpsychology: Journal Of Psychosocial Research On Cyberspace, 9*(4). Article 2. <https://doi.org/10.5817/CP2015-4-2>

Goldstein, S. E. (2016). Adolescents’ disclosure and secrecy about peer behavior: links with cyber aggression, relational aggression, and overt aggression. *Journal Of Child And Family Studies, 25*(5), 1430-1440. https://doi.org/10.1007/s10826-015-0340-2

Gökler, R. (2009). Okullarda akran zorbalığı. *Uluslararası İnsan Bilimleri Dergisi*, *6*(2), 511-537.

Grigg, D. W. (2010). Cyber-aggression: definition and concept of cyberbullying. *Journal Of Psychologists And Counsellors İn Schools*, *20*(2), 143-156. https://doi.org/10.1375/ajgc.20.2.143

Güleç, İ., Çelik, S., & Demirhan, B. (2012). Yaşam boyu öğrenme nedir? Kavram ve kapsamı üzerine bir değerlendirme. *Sakarya University Journal Of Education*, *2*(3), 34-48.

Hinduja, S.& Patchin, J.W. (2009). *Bullying beyond the schoolyard: preventing and
responding to cyberbullying,* California: Carwin Pres.

Hinduja, S., & Patchin, J. W. (2014). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*, California: Corwin Press.

Horner, S., Asher, Y., & Fireman, G. D. (2015). The impact and response to electronic bullying and traditional bullying among adolescents. *Computers in human behavior*, *49*, 288-295. <https://doi.org/10.1016/j.chb.2015.03.007>

Hosseinmardi, H., Mattson, S. A., Rafiq, R. I., Han, R., Lv, Q., & Mishra, S. (2015). Detection of cyberbullying incidents on the instagram social network. *arXiv preprint arXiv:1503.03909*.

Hoşgörür, V., & Orhan, A. (2017). Okulda zorbalık ve şiddetin nedenleri ve önlenmesinin yönetimi (Muğla merkez ilçe örneği). *Bayburt Eğitim Fakültesi Dergisi, 12*(24), 859-880.

Karasar, S. (2004). Egitimde yeni ıletisim teknolojileri-ınternet ve sanal yüksek egitim. *TOJET: The Turkish Online Journal Of Educational Technology*, *3*(4).117-125

Katz, I., Lemish, D., Cohen, R., & Arden, A. (2019). When parents are inconsistent: Parenting style and adolescents' involvement in cyberbullying. *Journal of Adolescence*, *74*, 1-12. <https://doi.org/10.1016/j.adolescence.2019.04.006>

Kepenekçi, Y. K., & Çınkır, Ş. (2003). Öğrenciler arası zorbalık. *Kuram Ve* *Uygulamada Eğitim Yönetimi, 34*(34), 236-253.

Koçer, M. (2012). Erciyes üniversitesi öğrencilerinin internet ve sosyal medya kullanım alışkanlıkları. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi,* 18. 70-85

Kopecký, K., & Szotkowski, R. (2017). Cyberbullying, cyber aggression and their impact on the victim–the teacher. *Telematics And Informatics, 34*(2), 506-517. https://doi.org/[10.1016/j.tele.2016.08.014](http://dx.doi.org/10.1016/j.tele.2016.08.014)

Kwan, G. C. E., & Skoric, M. M. (2013). Facebook bullying: An extension of battles in school. *Computers in human behavior*, *29*(1), 16-25. <https://doi.org/10.1016/j.chb.2012.07.014>

Law, D. M., Shapka, J. D., & Olson, B. F. (2010). To control or not to control? Parenting behaviours and adolescent online aggression. *Computers İn Human Behavior, 26*(6), 1651-1656. <https://doi.org/10.1016/j.chb.2010.06.013>

Legate, N., Weinstein, N., & Przybylski, A. K. (2019). Parenting strategies and adolescents’ cyberbullying behaviors: evidence from a preregistered study of parent–child dyads. *Journal of youth and adolescence*, *48*(2), 399-409. https://doi.org/[10.1007/s10964-018-0962-y](https://doi.org/10.1007/s10964-018-0962-y)

Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *CyberPsychology & Behavior*, *12*(4), 387-393. https://doi.org/[10.1089/cpb.2009.0068](https://doi.org/10.1089/cpb.2009.0068)

Mishna, F., Regehr, C., Lacombe-Duncan, A., Daciuk, J., Fearing, G., & Van Wert, M. (2018). Social media, cyber-aggression and student mental health on a university campus. *Journal Of Mental Health, 27*(3), 222-229. https://doi.org/[10.1080/09638237.2018.1437607](https://doi.org/10.1080/09638237.2018.1437607)

Modecki, K. L., Barber, B. L., & Vernon, L. (2013). Mapping developmental precursors of cyber-aggression: trajectories of risk predict perpetration and victimization. *Journal Of Youth And Adolescence, 42*(5), 651-661. https://doi.org/[10.1007/s10964-012-9887-z](https://doi.org/10.1007/s10964-012-9887-z)

Nocentini, A., Fiorentini, G., Di Paola, L., & Menesini, E. (2018). Parents, family characteristics and bullying behavior: A systematic review. *Aggression and violent behavior*. *45*, 41-50. <https://doi.org/10.1016/j.avb.2018.07.010>

O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, *127*(4), 800-804. https://doi.org/[10.1542/peds.2011-0054](https://doi.org/10.1542/peds.2011-0054)

Olweus, D. (1993). Bullying at school: what we know and what we can do?Oxford and Cambridge, MA: Blackwll Publishers.

Pabian, S., De Backer, C. J., & Vandebosch, H. (2015). Dark triad personality traits and adolescent cyber-aggression. *Personality ZAnd Individual Differences, 75*, 41-46. <https://doi.org/10.1016/j.paid.2014.11.015>

Parti, K., Kiss, T., & Koplányi, G. (2018). Architecture of aggression in cyberspace. Testing cyber aggression in young adults in hungary. *International Journal Of* *Cybersecurity Intelligence & Cybercrime, 1*(1), 56-68. https://doi.org/[10.52306/01010618QOSG3191](http://dx.doi.org/10.52306/01010618QOSG3191)

Patterson, L. J., Allan, A., & Cross, D. (2016). Adolescent bystanders' perspectives of aggression in the online versus school environments. *Journal Of Adolescence, 49*, 60-67. <https://doi.org/10.1016/j.adolescence.2016.02.003>

Peker, A., Eroğlu, Y., & Ada, Ş. (2012). Ergenlerde siber zorbalığın ve mağduriyetin yordayıcılarının incelenmesi. *Abant İzzet Baysal Üniversitesi Eğitim Fakültesi Dergisi, 12,* 185-206

Pornari, C. D., & Wood, J. (2010). Peer and cyber aggression in secondary school students: the role of moral disengagement, hostile attribution bias, and outcome expectancies. *Aggressive Behavior: Official Journal Of The International Society For Research On Aggression, 36*(2), 81-94. https://doi.org/[10.1002/ab.20336](http://dx.doi.org/10.1002/ab.20336)

Pyżalski, J. (2012). From cyberbullying to electronic aggression: typology of the phenomenon. *Emotional and behavioural difficulties*, *17*(3-4), 305-317. https://doi.org/10.1080/13632752.2012.704319

Raskauskas, J. & Stoltz, A.D. (2007). Involvement in traditional and electronic
bullying among adolescents. *Developmental Psychology*, *43*, 564-575. https://doi.org/[10.1037/0012-1649.43.3.564](http://dx.doi.org/10.1037/0012-1649.43.3.564)

Runions, K. C., Bak, M., & Shaw, T. (2017). Disentangling functions of online aggression: The cyber‐aggression typology questionnaire (CATQ). *Aggressive Behavior, 43(*1), 74-84. https://doi.org/[10.1002/ab.21663](http://dx.doi.org/10.1002/ab.21663)

Sabancı, Y. (2018). *Ergenlerde siber zorbalık ve siber mağduriyetin yordayıcıları olarak akılcı olmayan inançlar psikolojik sağlamlık ve psikolojik ihtiyaçlar.* Gaziantep Üniversitesi: Yayımlanmamış Yüksek Lisans Tezi.

Schoffstall, C. L., & Cohen, R. (2011). Cyber aggression: The relation between online offenders and offline social competence. *Social Development, 20*(3), 587-604. https://doi.org/[10.1111/j.1467-9507.2011.00609.x](http://dx.doi.org/10.1111/j.1467-9507.2011.00609.x)

Tokunaga, R. S. (2010). Following you home from school: a critical review and synthesis of research on cyberbullying victimization. *Computers İn Human Behavior, 26*(3), 277-287. <https://doi.org/10.1016/j.chb.2009.11.014>

Toledano, S., Werch, B. L., & Wiens, B. A. (2015). Domain-specific self-concept in relation to traditional and cyber peer aggression. *Journal Of School Violence, 14*(4), 405-423. https://doi.org/[10.1080/15388220.2014.935386](http://dx.doi.org/10.1080/15388220.2014.935386)

Türkoğlu, S. (2013). Ergenlerin problemli internet kullanımları ile siber zorbalık eğilimleri arasındaki ilişkinin incelenmesi. Marmara Üniversitesi: Yayımlanmamış Yüksek Lisans Tezi.

Urban Dictionary (2019). (Https://Www.Urbandictionary.Com/Define.Php?Term=Cyber%20Aggression . Adresinden 06.02. 2019 Tarihinde Alınmıştır.

Vale, A., Pereira, F., Gonçalves, M., & Matos, M. (2018). Cyber-aggression in adolescence and internet parenting styles: a study with victims, perpetrators and victim-perpetrators*. Children And Youth Services Review, 93*, 88-99. <https://doi.org/10.1016/j.childyouth.2018.06.021>

Vural, Z., & Bat, M. (2010). Yeni bir iletişim ortamı olarak sosyal medya: Ege Üniversitesi İletişim Fakültesi’ne yönelik bir araştırma. *Journal Of Yasar University*, *5*(20). 3348-3382

Whittaker, E., & Kowalski, R. M. (2015). Cyberbullying via social media. *Journal of School Violence*, *14*(1), 11-29. <https://doi.org/10.1080/15388220.2014.949377>

Wright, M. F., & Li, Y. (2013). Normative beliefs about aggression and cyber aggression among young adults: A longitudinal investigation. *Aggressive Behavior, 39*(3), 161-170. https://doi.org/[10.1002/ab.21470](https://doi.org/10.1002/ab.21470)

Wright, M. F., Aoyama, I., Kamble, S. V., Li, Z., Soudi, S., Lei, L., & Shu, C. (2015). Peer attachment and cyber aggression involvement among Chinese, Indian, and Japanese adolescents*. Societies, 5*(2), 339-353. https://doi.org/[10.3390/soc5020339](http://dx.doi.org/10.3390/soc5020339)

Yaman, E., & Sönmez, Z. (2015). Ergenlerin siber zorbalık eğilimleri. *Online Journal Of Technology Addiction & Cyberbullying*, *2*(1), 18-31.

Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics. *Journal Of Child Psychology And Psychiatry, 45*(7), 1308-1316. https://doi.org/[10.1111/j.1469-7610.2004.00328.x](https://doi.org/10.1111/j.1469-7610.2004.00328.x)

Ybarra, M. L., Diener-West, M., & Leaf, P. J. (2007). Examining the overlap in Internet harassment and school bullying: Implications for school intervention. *Journal of Adolescent Health*, *41*(6), S42-S50. https://doi.org/[10.1016/j.jadohealth.2007.09.004](https://doi.org/10.1016/j.jadohealth.2007.09.004)

Yılmaz, K., & Horzum, M. B. (2005). Küreselleşme, bilgi teknolojileri ve üniversite. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, *6*(10), 103-121.

**Summary**

**Introduction**

Fast developments in information communication technologies have introduced concepts such as new media and social media into our lives (Başlar, 2013). Social media is a form of communication that can be shared regardless of time and place. The dialogues people have with each other on the internet make up social media. With the widespread use of social media that some problems have emerged (Yaman ve Sönmez, 2015) Internet and social media usage has widespread the use of anonymous malicious emails. Therefore spread insulting, attacking and threatening messages and social media messages (Sabancı, 2018). Internet and social media have brought a new dimension to the widely known bullying and aggression (Aksaray, 2011). According to Corcoran, Guckin, and Prentice (2015), some concepts have emerged as a result of the abuse of the internet and social media. The concept of cyberbullying consists of certain features. These features include the repetition and harm of cyberbullying behavior and the imbalance of power between the cyberbully and the victim; It was stated as the characteristics of cyberbullying behavior. When cyber-aggression is conceptualized, it is stated that the behavior has the purpose of harm, the harmful behavior is not repeated, and there is no inequality of power between the offender and the victim. Cyber aggression is also a concept in the literature in which aggressive behavior can be more than one, but not continuous and in the context of power inequality, the aggressor is defined as the person who uses ICT tools well.

The aim of this study is to define the concept of cyber aggression and to examine the tendency of cyber aggression of high school students according to various variables. The Cyber Aggression Scale was developed for this purpose.

**Method**

This research is an example of a descriptive survey model. The study group of the research consists of students who continue their education in Ipekyolu and Edremit districts of Van province in 2018-2019 academic year. The scale included 1573 students for exploratory factor analysis and 188 students for confirmatory factor analysis. It was applied to a total of 1761 students. The exploratory factor analysis research group consisted of 1573 students including 852 girls and 721 males who attended 9th, 10th, 11th and 12th grades in nine state schools in Van. The data of the study were collected by using the Cyber Aggression Scale and demographic information form which were prepared by the researcher. KMO and Bartlett test, exploratory and confirmatory factor analysis were performed to investigate the validity of the scale. The data were analyzed by using SPSS 22.0 and LISREL 8.8 package programs. As a result of the analyzes, Cronbach’s Alpha reliability coefficient was determined as 0,92 (> 0,70). It was found that the 6-factor structure of the scale was validated according to the compliance statistics obtained from confirmatory factor analysis. Compliance indexes of confirmatory factor analysis of Cyber Aggression Scale: RMSEA value is 0.076, AGFI index is 0.72, NNFI value is 0.93, NFI value is 0.91 and CFI value is 0.94. The 6-factor structure of the scale was determined according to the compliance statistics obtained from confirmatory factor analysis, t- test, ANOVA and Scheffe tests were used for data analysis. In addition, the analyzes revealed that the scale was composed of 6 factors: “Visual and Sexual Cyber Aggression ”, “Unrest and Irrison” , “Cyber Aggression towards User Account ”, “Threat”, “Exclusion” and “Fake Account”. In this context, the Cyber Aggression Scale is a 32-items scale which is collected under of these six factors. The analyzes revealed that the scale is a valid and reliable to measure the individuals’ behavior of Cyber Agrression.

**Result and Discussion**

According to the findings of the study: It was seen that the age of students' cyber aggression tendency does not make a significant difference according to age. In this context, in the literature studies (Patterson, Allan & Cross, 2016; Wright & Li, 2013; Schoffstall & Cohen, 2011; Pornari & Wood, 2010; Toledano, Werch & Wiens, 2015), there was no significant difference between cyber aggression and age. There was a significant difference between students' cyber aggression scores and type of school. It has been seen that students show a significant difference according to their genders. According to this result, there are studies show that there is a significant difference between cyber aggression and gender (Musharraf and Anis-ul-Haque, 2018; Wright, Aoyama, Kamble, Li, Soudi, Lei, and Shu, 2015; Lamb, 2015). There was a significant difference between cyber aggression tendencies of students according to their internet usage time. Research on this outcome has generally focused on internet addiction. When we look at the literature (Türkoğlu, 2013; Erdur-Baker & Kavşut, 2007; Peker, Eroğlu, & Ada, 2012), There was a significant difference between cyberbullying and internet usage time. There was a significant difference between cyber aggression tendencies of students according to being anonymous on social networks. In this context, when the literature is examined, Mishnah, Regehr, Lacombe-Duncan, Dacia, Fearing and Van Wert (2018) support the results. There was no significant difference between cyber aggression tendencies of students according to the parent checking social networks. There was a significant difference between cyber aggression tendencies of students according to students' room. There was a significant difference between cyber aggression tendencies of students according to being interactive in social networks.

EK: Siber Saldırganlık Ölçeği

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SON 3 AY** içerisinde aşağıda belirtilen davranışı kaç kez yaptığınızı işaretleyiniz. | 0 | 1 | 2 | 3 | 4 |
| M-01 Sosyal medyada farklı bir kimlikle yorumlar yazdım  |  |  |  |  |  |
| M-02 Sahte hesap açıp arkadaşlarımın neler yaptıklarını gizlice takip ettim.  |  |  |  |  |  |
| M-03 Sahte hesap açıp kendimi olduğum kişiden farklı biri olarak tanıttım. |  |  |  |  |  |
| M-04 İnternette arkadaşlarımı rahatsız ettim. |  |  |  |  |  |
| M-05 Hoşlanmadığım arkadaşımın sosyal medya hesabını ele geçirdim. |  |  |  |  |  |
| M-06 Sosyal medya veya anlık mesajlaşma listemden hiçbir şey yapmadığı halde kişileri sildim veya reddettim.  |  |  |  |  |  |
| M-07 Sosyal medya kullanarak herhangi bir kişiye hakaret ettim. |  |  |  |  |  |
| M-08 Hoşlanmadığım birini sosyal medyada görmezden geldim. |  |  |  |  |  |
| M-09 Sosyal medyada birisi hakkında asılsız söylentiler yaydım. |  |  |  |  |  |
| M-10 Sosyal medyada arkadaşlarımla alay ettim |  |  |  |  |  |
| M-11 Birinin sosyal medya hesabını almak için bir ekip oluşturup ona saldırdım. |  |  |  |  |  |
| M-12 Bir kişiyi sevmediğimde onu dışlamak için interneti kullandım. |  |  |  |  |  |
| M-13 Arkadaşlıkları bozmak için sosyal medyada başka biri gibi davrandım. |  |  |  |  |  |
| M-14 Birilerini küçük düşürmek için interneti kullandım. |  |  |  |  |  |
| M-15 İnternette arkadaşlarımla alay ettim. |  |  |  |  |  |
| M-16 İnternete bağlanırken ip adresimi değiştirerek başka hesapları ele geçirmeye çalıştım |  |  |  |  |  |
| M-17 Başkalarının özel konuşmalarını paylaşmakla tehdit ettim. |  |  |  |  |  |
| M-18 Başkalarının özel fotoğraflarını paylaşmakla tehdit ettim. |  |  |  |  |  |
| M-19 Başkalarının özel fotoğraflarını paylaşmakla tehdit ettim ve istemediği şeyler yapmaya zorladım. |  |  |  |  |  |
| M-20 Sahte hesap açıp insanları buluşmaya çağırıp sonra da buluşmaya gitmedim. |  |  |  |  |  |
| M-21 Birisiyle alay etmek için izni olmadan paylaşımasını istemediği fotoğraflarını paylaştım. |  |  |  |  |  |
| M-22 İnternette başka insanlara kötü görüntülerden oluşan fotoğraf yolladım. |  |  |  |  |  |
| M-23 Hoşlanmadığım birini internette görmezden geldim. |  |  |  |  |  |
| M-24 Forum, sosyal medya ya da çevrimiçi oyunda yalan şikayette bulunarak başka birinin oyundan çıkarılmasına neden oldum. |  |  |  |  |  |
| M-25 İnternette beğenmediğim bir yorumu yapan hesabı kapattırdım. |  |  |  |  |  |
| M-26 İnternette kendimle ilgili hoşlanmadığım bir paylaşım görünce paylaşandan intikam aldım |  |  |  |  |  |
| M-27 İnternette sahte hesap aracılığıyla kişilerin uygunsuz fotoğraflarını paylaştım. |  |  |  |  |  |
| M-27 Sevmediğim insanların sosyal medya hesaplarını kendi sosyal medya hesabımda izinsiz paylaştım. |  |  |  |  |  |
| M-29 Başka insanların uygunsuz fotoğraflarını internette izinsiz olarak paylaştım. |  |  |  |  |  |
| M-30 İnternette açtığım sahte hesaplarda bağımlılık yapan maddelere ait fotoğraflar paylaştım. |  |  |  |  |  |
| M-31 İnternette sahte hesap aracılığıyla insanların cinsel içerikli fotoğraflarını paylaştım. |  |  |  |  |  |
| M-32 Cinsel içerikli fotoğraflar veya videolar çekerek bunları paylaştım. |  |  |  |  |  |

1. Çalışma birinci yazarın ikinci yazar danışmanlığında 2019 yılında tamamlamış olduğu Yüksek Lisans tezinin bir bölümünden faydalanılarak üretilmiştir [↑](#footnote-ref-1)
2. \* \* **Sorumlu Yazar,** Doktora Öğrencisi, MEB, İstanbul, TÜRKİYE; sevilayseryol@hacettepe.edu.tr, https://orcid.org/0000-0002-2107-9315 [↑](#footnote-ref-2)
3. \*\*\* Van Yüzüncü Yıl Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Van, Türkiye; mustafaserkan@yyu.edu.tr, <https://orcid.org/0000-0003-0485-3038>

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Gönderim:****21.08.2021****Kabul:****29.10.2021* ***Yayın****:15.02.2022*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* [↑](#footnote-ref-3)