

SİBER UZAYDA YAŞLI BİREYLERİN SİBER GÜVENLİK SORUNLARI ÜZERİNE BİR SWOT ANALİZİ

A SWOT ANALYSIS ON CYBER SECURITY PROBLEMS OF ELDERLY INDIVIDUALS IN CYBER SPACE

Öğr. Gör. Emir Hasan ÖLMEZ

Beykent Üniversitesi Meslek Yüksekokulu, Yönetim ve Organizasyon Bölümü, Sağlık Kurumları İşletmeciliği Programı, İstanbul/Türkiye
ORCID: 0000-0001-8587-0926

Öğr. Gör. Ülkü Melike ALPTEKİN

İskenderun Teknik Üniversitesi Dörtyol Sağlık Hizmetleri Meslek Yüksekokulu, Tıbbi Hizmetler ve Teknikler Bölümü, Tıbbi Dokümantasyon ve Sekreterlik Programı, Hatay/Türkiye
ORCID: 0000-0002-4465-2428

Prof. Dr. Özgür ASLAN

İstanbul Üniversitesi-Cerrahpaşa, Sağlık Bilimleri Fakültesi, Sağlık Yönetimi Bölümü, İstanbul/Türkiye
ORCID: 0000-0002-8780-5463

Cite As Ölmez, E.H.; Alptekin, Ü.M. & Aslan, Ö. (2021). "Siber Uzayda Yaşlı Bireylerin Siber Güvenlik Sorunları Üzerine Bir Swot Analizi", International Academic Social Resources Journal, (e-ISSN: 2636-7637), Vol:6, Issue:25; pp:772-781

ÖZET

Siber uzay, İnternet'in gelişimi ve yaşamımızın bir parçası haline gelmesiyle birlikte dahil olduğumuz modern dünyadır. Literatürde de ifade edildiği üzere, bu dijital temelli dünyadaki, bilgisayarı bir araç, hedef veya daha fazla suçu devam ettirmek için kullanan siber taciz, siber para akama, siber dolandırıcılık ve siber terörizm gibi yasadışı faaliyetler siber suç kapsamına girmektedir. Bu kapsamdaki suçlardan korunmak için alınan önlemler ise siber güvenlik önlemleri olarak isimlendirilmektedir.

Özellikle batı toplumlarında demografik değişimler dolayısıyla yaşlı bireylerin oranı hızla artmaktadır. İnternet, yaşlıların hayat kalitelerini artırabilecek iletişim, sağlık ve finans gibi birçok alandaki fırsatları da beraberinde getirmektedir. Bu açıdan değerlendirildiğinde siber uzayın, yaşlılara özellikle toplumun bir parçası olarak sosyalleşmek ve işlerini evlerinde yürütmek konusunda sağladığı yararlar göz ardı edilemez. Buna karşın, yaşlılar siber uzayda en savunmasız gruplardan biri olarak dikkat çekmektedir. Literatüre bakıldığında yaşlı bireylerin siber dünyada yaşayabilecekleri siber suçlara ilişkin çalışmalar sınırlı düzeydedir. Siber uzayın ortaya çıkardığı fırsatların yaşlılar açısından gerçekleştirilebilmesi için siber güvenlik kaçınılmaz olarak üzerinde durulması gereken konulardan biri olarak son yıllarda daha fazla dikkat çekmeye başlamıştır. Bu çalışmada, yaşlıların siber uzayda yaşadıkları siber güvenlik sorunları SWOT analizi ile incelenmeye ve çözümler önerilmeye çalışılmıştır. Bu bağlamda çalışma kapsamında siber uzay, siber suç ve siber güvenlik konularına değinilmiştir. Daha sonra ise konu üzerine SWOT analizi yapılmış ve yaşlıların siber uzaydaki güvenlikleri için gerekli hususlar, konu üzerine yapılmış literatür incelenmek suretiyle açıklanmaya çalışılmıştır.

Anahtar Kelimeler: Siber Uzay, Siber Güvenlik, Siber Suç, Yaşlılar

ABSTRACT

Cyberspace is the modern world we are involved in with the development of the Internet and becoming a part of our lives. As stated in the literature, in this digital-based world, illegal activities such as cyber harassment, cyber money laundering, cyber fraud and cyber terrorism that use the computer to perpetuate a tool, target or more crime fall under the scope of cybercrime. The measures taken to protect against crimes in this context are called cyber security measures.

Especially in western societies, the ratio of elderly individuals is increasing rapidly due to demographic changes. The Internet brings with it opportunities in many areas such as communication, health and finance that can improve the quality of life of the elderly. From this point of view, the benefits of cyberspace for elderly people, especially as a part of society, in socializing and running their jobs at home cannot be ignored. In contrast, the elderly stand out as one of the most vulnerable groups in cyberspace. When the literature is reviewed, studies on cybercrime that elderly people can live in the cyber world are limited. In order to realize the opportunities created by cyber space for the elderly, cyber security has inevitably started to attract more attention as one of the issues that need to be emphasized. In this study, the cyber security problems experienced by the elderly in cyber space were examined with SWOT analysis and solutions were tried to be proposed. In this context, cyber space, cybercrime and cyber security issues were discussed within the scope of the study. Then, a SWOT analysis was made on the subject and the necessary issues for the security of the elderly in cyber space were tried to be explained by examining the literature on the subject.

Key Words: Cyber Space, Cyber Security, Cyber Crime, Seniors.

1. GİRİŞ

Büyük icatlardan biri olarak İnternet teknolojisi, dünyayı hızla değiştirmektedir. İnternet'e erişimin artması ve düşen bilgisayar maliyetleri ile İnternet, günlük hayatımızın ayrılmaz bir parçası haline gelmiştir (Chang ve Grabosky, 2014: 321). İnternet temelli çevrimiçi dünya artık 21. yüzyılın iletişim ve alışveriş merkezi durumundadır. Çevrimiçi dünyadaki "yabancı tehlike" ve beraberindeki güvenli davranışlar, gerçek dünyada olduğu kadar çevrimiçi dünyada da geçerlidir (Grose, 2011: 1). Diğer yandan, bu değişime paralel olarak bireylerin, kurumların ve ülkelerin bilgisayar sistemlerinin hem donanımına hem de yazılımına yönelik

saldırılarda artış yaşanmaktadır (Pool, 2013). Tüm dijital teknoloji kullanıcıları, siber saldırıların potansiyel kurbanıdır ve farkında olmadan bu saldırılara da katılabilirler (Morrison vd., 2020).

Günümüzde İnternet kullanma yeteneği, bilgi toplumu olmanın ön koşulu olarak kabul edilmektedir. Bilgi toplumu, aynı zamanda yaşlanan bir toplumdur. Son yıllarda doğurganlığın azalması ve artan yaşam süresi demografik bir değişime neden olmuştur. Dünya nüfusu hızla yaşlanırken aktif yaşlanma için bireysel anlamda da gelişme sağlanması gerekmektedir. Yaşlıların İnternet'e erişiminin olması ve avantajlarından yararlanması sayesinde yaşlıların yaşam kalitesi artmaktadır (Boz ve Karataş, 2015: 183).

Yaşlıların bir açıdan yaşam kalitesini artıran bu teknolojik gelişmeler, diğer yandan güvenlik risklerini de ortaya çıkarmaktadır. Dijital dünyadaki gelişmeleri takip etmekte sorun yaşayan ve bu açıdan dezavantajlı durumda olan yaşlı ilerlemiş bireyler için siber güvenliğin sağlanması çok büyük önem taşımaktadır. Yaşlıların tehlike ve tehditlerden uzak bir siber uzayda dolaşabilmelerinin ilk koşulu kendilerini korumalarıdır. Bunun yanında topluma ve ülkelere düşen görev, yaşlıları İnternet ve teknoloji konusunda eğitmek ve doğru yönlendirmektir. Bu çalışmada, yaşlıların siber güvenlik sorunlarına ilişkin SWOT analizi yapılmakta ve çözümler önerilmektedir.

2. KAVRAMSAL ÇERÇEVE

2.1. Siber Uzay

Siber kelimesinin kökenlerinin Yunanca-yönlendirmek, kontrol etmek-fiili olan κυβερειω (kybereo)'ya dayandığı düşünülmektedir (Lehto, 2015). Mekanik bilimlerde geliştirilen sibernetik kuram, makine ve insanların geri-besleme ile denetlenmesi ve yönetilmesi ilkesine dayanmaktadır (Avcıoğlu, 2017: 515). 1940'lı yılların sonunda Amerikalı bir matematikçi olan Norbert Wiener, bilgisayarlı kontrol sistemlerini tanımlamak için sibernetik kelimesini kullanmaya başlamıştır. Wiener'e göre sibernetik, makinelerin ve canlı organizmaların kontrolünü iletişim ve geri bildirim yoluyla ele alan bilimlerle ilgilenmektedir. Sibernetik paradigmaya göre, biyolojik, fiziksel ve kimyasal sistemlerin kontrolünde bilgi paylaşımı ve manipülasyonu kullanılmaktadır. Sibernetik, yalnızca sistemin işleyişinin ve nihai sonucun matematiksel olarak modellenip belirlenebildiği veya en azından tahmin edilebildiği makine benzeri sistemler için geçerlidir (Lehto, 2015).

Bir bilim-kurgu yazarı olan William Gibson, "Neuromancer" adlı romanında "siber uzay" terimini ortaya atmıştır. Bilim kurgu edebiyatı ve filmleri, Gibson siber uzayını veya matrisini, verilerin üç boyutlu, çok renkli bir biçimde kodlandığı küresel, bilgisayarlı bir bilgi ağı olarak tasvir etmektedir. Kullanıcılar bir bilgisayar arayüzü aracılığıyla siber uzaya girer, siber uzayda "avatar" olarak "uçabilir" veya verilerle tasvir edilen binalara girerek kentsel alanları keşfedebilirler. Diğer bir ifadeyle "siber uzay, birbirine bağlı bilgi teknolojisi ağları ve bu ağlardaki bilgiler tarafından oluşturulan elektronik dünyadır" (Lehto, 2015).

Siber uzay terimi, iletişimin gerçekleştiği siber dünyanın çevrimiçi ortamını tanımlamak için kullanılmaktadır. Aslında, siber uzayda bilgiye, iletişime ve işbirliğine haftanın yedi günü 24 saat erişimimiz bulunmaktadır. Siber uzayın gerçek boyutu, çevrimiçi ortamda herkesin erişebileceği birçok bilgi olduğu anlamına gelmektedir. Bilgisayarlardan önce, insanlar bilgiye erişmek istediklerinde, bir kütüphanede kitap aramak veya tavsiye için bir uzmana gitmek zorundaydılar. Ancak siber uzay, çevrimiçi araştırma yapmayı ve hem hızlı hem de verimli bir şekilde bilgi edinmeyi mümkün kılmaktadır (Mulka, 2014: 5).

Siber uzay terimi henüz küresel olarak kabul edilmiş bir tanıma sahip değildir, ancak bazen İnternet kavramına veya dijital sanal alan görüşüne denk olarak ifade edilmektedir. Siber uzay, "İnternet, telekomünikasyon ağları, bilgisayar sistemleri dahil olmak üzere birbirine bağlı bilgi teknolojisi altyapı ağından oluşan bilgi ortamı içinde küresel bir etki alanıdır". Tanım, siber uzayın bilginin kaydedilmesine, depolanmasına, geri alınmasına ve iletilmesine izin veren İnternet ve telekomünikasyon teknolojilerinin kombinasyonunu kapsamaktadır (Mbanaso ve Dandaura, 2015: 18).

Tablo 1: Siber Uzay Yerine Kullanılan Farklı Kavramlar

Siber dünya: Yeryüzündeki insan post-modern varoluşunun varlığı.
Siber alan: Birileri tarafından kontrol edilen, kesin olarak belirlenmiş bir alan.
Siber ekosistem: Bir siber topluluğun sistemleri ve çevresi.
Siber çevre: İnsan siber aktivitesi için ortam sağlayan inşa edilmiş çevre ve etkileşimde buldukları kişiler, kurumlar ve fiziksel sistemler.

Kaynak: Lehto, 2015.

Siber uzay faaliyetlerinin en temel bileşenleri; siber ticaret, siber öğrenme, siber sosyalleşme, siber oyun, siber eğlence, siber gazetecilik, siber yayın, siber reklam, siber politika, siber turizm, siber tıp, siber yönetim olarak dikkat çekmektedir (Oluga vd., 2014: 66).

2.2. Siber Suç ve Siber Güvenlik

İnternet aynı zamanda meşhur “iki ucu keskin kılıç” olarak görülmektedir. İnternetin getirdiği kolaylığın yanı sıra İnternet ve teknoloji temelli bilgisayar suçları da hızla ortaya çıkmaktadır. Yaşanan bu hızlı dönüşüm, siber suçlulara ve siber sapkın girişimcilere benzeri görülmemiş fırsatlar sunmaktadır (Chang ve Grabosky, 2014: 321).

“Siber suç” terimi, “siber uzay” teriminden sonra ortaya çıkmıştır. “Sibernetik” ve “uzay” kelimeleri, 1980’lerde ve 1990’larda siber kafe, siber dünya ve tabii ki “siber suç” gibi çok çeşitli siber bileşiklerin öncüsü olmuştur. Siber suç yerine “bilgisayar suçu”, “bilgisayarla ilgili suç”, “yüksek teknolojili suç”, “teknoloji destekli suç”, “e-suç” veya “siber uzay suçu” da denilmektedir (Chang ve Grabosky, 2014: 321).

Siber suç, İnternet dünyasındaki en son ve belki de en karmaşık sorun olarak ifade edilmektedir. Bilgisayarı bir araç, hedef veya daha fazla suçu devam ettirmek için bir araç olarak kullanan her türlü yasadışı faaliyet siber suç kapsamına girmektedir (Arfi ve Agarwal, 2014: 7).

Siber suç, bireylerin ve toplumumuzun yaşamları üzerinde ciddi bir etki potansiyeline sahiptir. Siber suç, siber uzayda meydana gelen, yani İnternet ve bilgisayar dünyasında gerçekleşen bir tür suçtur. Birçok insan siber suç konusunda sınırlı bilgiye sahip olsa da, bu tür bir suç yaşamlarımız üzerinde ciddi bir etki potansiyeline sahiptir, çünkü toplumumuz “siber uzayda” gerçekleşen bilgi alışverişiyle dolu bir bilgi toplumu haline gelmektedir (Arfi ve Agarwal, 2013b: 1).

İnternet, cep telefonları ve diğer bilgisayar teknolojileri geliştikçe suçlular hırsızlık, dolandırıcılık, taciz gibi amaçları için bu gelişen teknolojiyi kullanmanın yollarını bulmuşlardır. Her bireyin karşılaştığı yaygın siber suçlar aşağıdaki gibidir (Arfi ve Agarwal, 2013a: 1-2):

Tablo 2: Siber Suçlar

Tehdit yoluyla saldırı: Bir kişiyi kendisinin, ailesinin ya da güvenliğinden sorumlu olduğu kişilerin hayatları ile korkutarak tehdit etmek.
Çocuk pornografisi: Çocukları cinsel olarak istismar eden içerikleri oluşturmak, dağıtmak veya bunlara erişmek suçu.
Siber para aklama: Yasadışı olarak elde edilen paranın kaynağını ve hedefini gizlemek amacıyla yapılan elektronik transfer.
Siber taciz/şantaj: İnternet teknolojileri ile korku yaratacak bilgilerin paylaşılması.
Siber terörizm: Belirli bir politik ve sosyal amaca ulaşabilmek için İnternet teknolojileri yoluyla bireylere ve toplumu tehdit etme, yıldırma, baskı altında tutma.
Siber dolandırıcılık: Zimmete para geçirme, casusluk, kimlik hırsızlığı, dolandırıcılık, kötü niyetli bilgisayar korsanlığı ve intihal gibi hırsızlıklar için İnternet’in kullanılması.
Donanım hırsızlığı: Yazıcılar gibi donanımlardaki güvenlik açıklarını İnternet aracılığıyla kötü amaçlı kullanma.
Spam ve kimlik avı: Spam olarak bilinen istenmeyen toplu e-postalar insanları rahatsız etmenin ötesindedir. İstenmeyen e-postalar önemli kişisel bilgileri alabilmek için kişileri dolandırma aracı olarak kullanılabilir.
Hackerlığa özenme: Teknik uzmanlıkları olmayan ve hacker olmak isteyenlerin çok zayıf güvenli sistemlere saldırması.
Üyeler/içeridekiler: Bir organizasyona dahil olan içeriden üyelerin sistemlere saldırması. Bu tehdit az rastlansa da büyük oranda hasar yaratmaktadır.

Kaynak: Arfi-Agarwal, 2013a: 1-2.

Siber uzaydaki İnternet kullanıcılarının sayısı her geçen gün artarken yaşa bakılmaksızın herkesin öncelik vermesi gereken konu “siber güvenlik”tir (Eric, 2018; Humayun vd., 2020: 3171-3173). Çünkü siber suçlar, bireylerin hayatlarını kaybetmelerine dahi sebep olabilecek bir dizi kötü sonuçlar ortaya çıkarmaktadır. Örneğin, sağlık alanı bağlamında harici olarak kontrol edilebilen kalp pilleri gibi elektronik tıbbi cihazlara yapılan müdahalelerin ölümcül sonuçları olabilir (Fourie vd., 2014: 175). Siber güvenlik, İnternet kullanıcılarını her türlü kötü sonuçlardan korumak için araçlar, teknikler, politikalar, güvenlik önlemleri, riskleri azaltma stratejileri, eğitim, güvenlik güvenceleri ve son teknolojilerin bir araya getirilmesidir. Siber güvenlik, bireylerin, kuruluşların ve ülkelerin varlıklarını yetkisiz erişimden koruyan bir mekanizma olarak düşünülebilir (Humayun vd., 2020: 3171-3173).

Kurnaz (2016: 58)’a göre siber uzayın ortaya çıkardığı karmaşık ve çok boyutlu ortam, siber güvenliği öncelikli güvenlik alanlarından biri olarak hayatımıza dahil etmiştir. Siber güvenlik, hem siber uzaydaki bilgilerin korunması hem de bilginin üretilmesi, depolanması, işlevsel hale getirilmesi ve gönderilmesiyle alakalı her türlü durumu içermektedir. Siber güvenlik kavramı, bilgi güvenliği ve bilgisayar güvenliği ile bazen aynı anlamlarda kullanılmakla birlikte odaklandıkları konular açısından farklılık taşıyabilmektedir.

Siber uzayın daha güvenli bir yer haline gelebilmesi için bilginin gizlilik, bütünlük ve erişilebilirlik özelliklerini sağlaması gerekmektedir. Bu özelliklerin ne ifade ettiğine bakıldığında gizlilik, bilgiye yalnızca ilgili kişilerin ulaşmasını; bütünlük, bilişim sistemleri aracılığıyla depolanan bilginin değiştirilmemesi,

kaybedilmemesi ve yok edilmemesini; erişilebilirlik, depolanan bilginin gerektiğinde ilgili kişiler tarafından ulaşılabilir olmasını ifade etmektedir (Hekim ve Başbüyük, 2013: 137).

Pek çok ülke, ulusal strateji belgelerinde siber dünya veya siber güvenlik ile ne demek istediklerini tanımlamaya çalışmaktadır. Bununla birlikte, tüm bu değişken tanımların ortak teması, siber güvenliğin, 21. yüzyılın küresel ekonomisine nüfuz eden ve yönlendiren kritik altyapıları korumanın yanı sıra hem devlet sırlarını korumak hem de ulusal savunmayı sağlamak için temel unsur olduğudur (Lehto, 2015). Birleşik Krallık, siber güvenliği ulusal savunmaları için en önemli konu olarak görmekte olup Ulusal Siber Güvenlik Programı'na 650 milyon sterlin kaynak ayırmıştır (Solms ve Niekerk, 2013: 97). De Groot (2020) çalışmasında ifade edildiği üzere etkili bir siber güvenlik aşağıda yer alan şekildeki unsurların tümünü kapsamalıdır.



Şekil 1: Siber Güvenliğin Unsurları
Kaynak: De Groot, 2020.

Siber suçlular, bilgisayarları, akıllı cihazları ve iletişim ağı altyapısını sabote etmek için kötü amaçlı yazılım ve bilgisayar korsanlığı araçlarını kullanmaktadır. Koruyucu amaçlı araçlar genellikle siber güvenlik ihlallerini tamamen azaltmamaktadır. Bunun nedeni, kuşkusuz siber güvenlik zincirindeki en zayıf halkanın insan olmasından kaynaklanmaktadır (Zwilling vd., 2020: 1). Siber güvenlikte insanın öneminin anlaşılmasına başlanmasıyla birlikte insanların, siber suçların kurbanı olma davranışlarını etkileyen faktörleri daha iyi anlamaya yönelik araştırmalar yapılmıştır. Bireysel farklılıkların siber güvenlik davranış niyetlerini nasıl etkilediğini anlamak ve eğitim çabaları geliştirmek büyük önem taşımaktadır (Gratian vd., 2018: 345).

2.3. Siber Uzayda Yaşlılar

Siber uzay faaliyetlerindeki gelişmelerin yaşlılar için temel sonucu, bu devrime katılacak donanıma sahip olanlar için “yaşlıların ihtiyaçlarını karşılayan yeni, daha erişilebilir ürün ve hizmetlere yol açmasıdır” (Commonwealth of Australia, 2013: 7). Yaşlı bireyler, yeni teknolojileri benimsemeye heveslidirler. Artık birçok yaşlı birey, yalnızlığa ve izolasyona karşı koymak, sosyal olarak bağlı kalmak, aileyle etkileşim kurmak ve daha sağlıklı bir emekliliğin tadını çıkarmak için çevrimiçi teknolojilerle ilgilenmektedir (Morrison vd., 2020).

İnternet, yaşlı bireyleri haber ve bilgiye, devlet hizmetlerine, sağlık kaynaklarına ve sosyal destek fırsatlarına bağlamada giderek daha önemli bir rol oynamaktadır. Yaşlı bireylerin aile bağlarını sürdürebilmeleri, arkadaşlarıyla mevcut ilişkilerini güçlendirebilmeleri veya yeni sosyal ağlar geliştirebilmeleri için bir araç sağlamaktadır (Zhang ve Kaufman, 2015).

İnternet, yaşlı bireylerin bağımsız ve sosyal bir yaşam sürmelerine yardımcı olmaktadır. Yaşlıların ilgilendikleri konular hakkında bilgi sahibi olmaları ve benzer ilgi alanlarına sahip diğer yaşlı bireylerden oluşan bir ağa katılmaları için bir yol sağlamaktadır. İnternet, e-posta ve çevrimiçi sohbet yoluyla iletişim kurmanın bir yoludur. İnternet'in ticaret ve iletişim için artan kullanımıyla birlikte, yaşlı bireylerin siber uzaya katılımının önemi artmıştır. Siber uzayda seyahat etmek fiziksel hareket gerektirmemekte, bu nedenle

engelli yaşlı insanlar evlerinden çıkmadan sosyal ve ticari etkileşimlere girebilmektedir (Sum vd., 2009: 189).

İnsan ömrünün artması ve azalan doğurganlık oranları, dünya genelindeki popülasyonların yaş dağılımını daha yaşlı yaş gruplarına doğru kaydırmaktadır. Yaşlı bireylerin İnternet’i kullanmasının önündeki birkaç engel şunlardır: Şu anda yaşlı bireylerin yaşam sürelerinin çoğunda kişisel bilgisayar teknolojisi mevcut değildi; bu gruptaki düşük gelir ve eğitim seviyeleri teknolojinin erişilebilirliğini azaltmakta; fiziksel ve zihinsel bozukluklar yaşlı bireylerin İnternet’i kullanma becerilerini azaltmaktadır. Gelecek nesil yaşlı bireylerin İnternete ve teknolojiye daha aşina olacağı beklenmektedir. Bu nedenle bazı engeller kaldırılacaktır; ancak gelir ve eğitim seviyeleri gibi sosyoekonomik faktörler yine de erişilebilirliği etkileyebilecektir (Sum vd., 2009: 189).

Özellikle bilgisayar dünyasındaki en son teknolojiler ve yeniliklerle ilgili her türlü bilgiden mahrum kalan ve İnternet hakkında bilgi eksikliği olan ve farklı siber suç türlerinin kurbanı olan savunmasız grup, yaşlılardır (Arfi ve Agarwal, 2013a: 1). Tele-pazarlama ile dolandırıcılık yapanlar, sosyal izolasyonları, başkalarına güvenmeye istekli olmaları, görece saflıkları ve emeklilik birikimleri nedeniyle yaşlıları hedef almaktadırlar. Federal Bureau of Investigation (FBI), dolandırıcı tele-pazarlama şirketlerinin % 80’inin yaşlıları dolandırmaya odaklandığını tahmin etmektedir (Grimes vd., 2010: 177-178). Yaşlılar, tele-pazarlama dolandırıcılığı; çekiliş ve piyango aracılığıyla bir ödül kazanıldığını ve bu ödülü elde etmek için öncesinde belli bir para ödemeyi gerekli kılan çekiliş ve piyango dolandırıcılığı; iyi bir amaca yönelik e-posta, telefon ve İnternet aracılığıyla para talep eden hayır dolandırıcılığı; yatırım dolandırıcılığı; eşini kaybetmiş yaşlıları hedef alan flört ve evlilik dolandırıcılığı gibi siber suçlar için hedef alınmaktadır (Rebovich ve Corbo 2021: 416-419).

Siber güvenliğe çocuklar açısından çok dikkat edilmektedir. Buna karşın, İnternet üzerinden yaşlıların olası dolandırıcılık ve mali, fiziksel ve duygusal istismarına çok daha az ilgi gösterilmektedir (Saariluoma, 2016: 63). Yaşlılar, İnternet kullanımları her geçen gün artan grupta yer aldıkları için siber suçlular tarafından algılanan güvenlik açıkları nedeniyle her zaman İnternet dolandırıcılığı için birincil hedef olmaktadır (Eric, 2018). Bu çerçevede her yıl, siber suçlular Amerika Birleşik Devletleri’ndeki savunmasız yaşlı bireylerden yaklaşık 40 milyar dolar çalmaktadır (Munanga, 2019). Age UK yardım kuruluşu tarafından alınan verilere göre, siber suçlular 2018-2019 mali yılında Birleşik Krallık’taki yaşlı bireylerden 4 milyon eurodan fazla para çalmıştır. 55 yaş üstü grubundakiler, bu dönemde rapor edilen siber suç mağdurlarının toplamının %19’unu temsil etmektedir (Coker, 2020).

Bazı bilim insanları yaşlıların, özellikle de en yaşlı kesimin, “dijital uçurumun” dezavantajlarını yaşama olasılığının daha yüksek olduğunu ve bunun yeni izolasyon biçimleriyle sonuçlanabileceğini öne sürmektedirler (Mierzwa, 2020: 2). Pek çok bilim insanı iyi bir yaşam kalitesinin aktif sosyal katılım ve destekleyici sosyal ağlar ile pozitif bir şekilde ilişkili olduğunu ifade etmektedir. Burada yaşanacak problemler sonuç olarak fiziksel, sosyal ve psikolojik iyilik halinin bozulmasına yol açabilir. Yaşam kalitelerini artırmak için birçok ülkede yaşlılar, bilgisayar becerilerini öğrenmeye ve günlük pratiklerinde İnternet’i kullanmaya teşvik edilmektedir (Zhang, 2016: 2-4).

3. YAŞLI BİREYLERİN SİBER GÜVENLİK SWOT ANALİZİ

En genel ifadeyle SWOT analizi, ortamındaki dahili güçlü ve zayıf yanları ve dış fırsatları ve tehditleri değerlendirmektedir (Sammur vd., 2014). SWOT analizi firmalara, kurumlara, sektörlere uygulanabildiği gibi, iç ve dış çevresini analiz edebilmesi, buna uygun stratejiler geliştirebilmesi açısından farklı durumlara da uygulanabilir. Böylelikle ele alınan konunun güçlü-zayıf yönlerine, karşı karşıya olunacak fırsatlar/tehditlere ve stratejilere göre bir yol haritası belirlenebilir (Başlıgil ve Özdemir, 2011). Bu çerçevede yaşlıların siber güvenliğine ilişkin yapılan çalışmalar sistematik olarak taranmış ve uzman görüşleri alınmak suretiyle aşağıda yer alan SWOT analizi yapılmıştır. Çalışmanın yapılması esnasında karşılaşılan en önemli zorluklardan biri, konu üzerine olan literatürün oldukça sınırlı olmasıdır.

Tablo 3: Yaşlı Bireylerin Siber Güvenlik SWOT Analizi

Güçlü Yönler	Zayıf Yönler
<ul style="list-style-type: none"> Geronteoloji biliminin hızlı gelişimi. Büyük veri kavramının ortaya çıkması. Yaşlı bireylerin, siber uzayda deneyimlerine ve genellikle artan örgütsel ve sosyal becerilerine dayanarak daha iyi performans gösterebilir hale gelmesi. Yaşlı bireylerde yaşam boyu öğrenme kavramının gelişmesi ve dijital okuryazarlığın arttırması. 	<ul style="list-style-type: none"> Yaşlı bireylerin, kendini devlet memuru olarak tanıtan siber dolandırıcılara inanmaları. Yaşlılığa bağlı engeller; görme bozukluğu, el becerisi ve hareketliliğine ilişkin sorunlar, anlama ve kavrama zorlukları. Dijital teknolojinin tehlikeli, çok pahalı, karmaşık ve öğrenmesi çok zor olduğuna dair oluşan algı.

<ul style="list-style-type: none"> Yaşlı bireylerde bağımsız karar verme, sistem bilgisi ve süreç anlayışı, sosyallik ve takım çalışması, disiplinler arası düşünme, sorun çözme ve koordinasyon becerilerinin gelişmesi. Kamu spotu vb. uygulamalar ile siber suçlara karşı farkındalık artışı sağlamaya yönelik çabaların varlığı. E-devlet kullanımının artmasıyla yaşlıların siber uzaya entegre olması. 	<ul style="list-style-type: none"> Yaşlı bireylere yönelik siber eğitime erişimin önündeki ekonomik ve sosyal engeller. Gelirin yetersiz olması nedeniyle teknolojik ürünlere ulaşamama. Yaşlı bireylerin özellikle internet bankacılığında kullanıcı şifrelerini unutması. E-devlet'in güvenlik sorunları. Yaşlı bireylerde dijital okuryazarlığının düşük olması. Mobil uygulamaların sesli bilgilendirme konusundaki yetersizliği. Yaşlı bireylerde siber güvenlik kaygıları. Yaşlı bireylerin inovasyona katılımının düşük düzeyde olması. Yaşlıların teknolojik cihazları kullanma konularında güven eksiklikleri.
<p style="text-align: center;">Fırsatlar</p> <ul style="list-style-type: none"> Siber güvenlik teknolojilerinde yaşanan gelişmeler. Siber uzay ve güvenliğin yeni sektörleri ortaya çıkarması. Siber uzayın yaşlıları sosyal katılımlı hale getirmesi. Yaşam kalitesini iyileştirmesi. Güvenli internet alışverişinin gelişmesi. Dijital teknolojinin gelişmesinin tıbbi bakımı kolaylaştırması. Yapay zeka uygulamalarının siber uzayda yaşlı bireylerin güvenliğini sağlaması. Yaşlı bireylere yönelik özelleştirilmiş ürünlerin üretilmesine yönelik taleplerin artması. Akademik ve girişimsel anlamda konuya ilginin artması. 	<p style="text-align: center;">Tehditler</p> <ul style="list-style-type: none"> Güvenlik konusundaki açıkların yavaş kapanması. Firmaların yaşlı bireylerin siber güvenlik önceliklerine geç tepki vermeleri. Ülkelerin dijitalleşme tutkusunun olumsuz yansımaları. Dünyada ve Türkiye'de internet kullanmayan yaşlı nüfusun fazla olması. İnternet bankacılığının yaygınlaşmasının getireceği güvenlik sorunları. Değişen sosyal dinamikler bağlamında yaşlıların artık daha çok oranda yalnız yaşamaları. Evde ve online çalışmak isteyen yaşlı bireyleri hedef alan dolandırıcılık faaliyetleri. Mobil uygulamaların kimlik, bilgi ve para hırsızlığı için kullanılması. Truva atı, virüs, klavye dinleme, casus yazılımlar, önemsiz e-posta gibi kötücül yazılımların artması.

Kaynak: Şahin ve Yıldırım, 2019; Tekedere ve Arpacı, 2016; Baran vd., 2017; Tuna Uysal, 2020; Atakişi ve Orhan, 2020; Çiçek vd., 2021; Küçük ve Koçak, 2019; Al-Mayahi ve Mansoor, 2012; Goud, 2021.

4. YAŞLILARA YÖNELİK SİBER GÜVENLİK ÇÖZÜM ÖNERİLERİ

Siber uzayda giderek daha fazla yaşlı birey vakit geçirmektedir. Veriler, Amerika Birleşik Devletleri'ndeki yaşlı bireylerin rekor düzeyde İnternet'te çevrimiçi olduğunu ve sosyal medya hesapları açtığını göstermektedir (Federal Bureau of Investigation, 2018). Boz-Karataş (2015: 184-186)'e göre; yaşlılar için siber uzayda güvenli bir ortam sağlanırsa onların yaşamlarında aşağıdaki olumlu değişimler yaşanabilir:

- ✓ Aile üyeleri ve arkadaşlarıyla iletişim kurarak yalnızlık kaynaklı depresyondan korunur.
- ✓ Fiziksel olarak hiç tanışmadıkları kişilerle kurdukları iletişim ile sosyal izolasyondan kaçınılır.
- ✓ Modern dünyaya açılma ve bu dünya ile bütünleşme sağlanır.
- ✓ Sağlık, hobiler ve tüketim malları vb. hakkında yararlı bilgilere erişebilir ve bilgilendirici açıdan sosyal destek sağlanır.
- ✓ Çevrimiçi topluluklara katılarak kurulan sosyal ilişkiler, stres düzeyini düşürür ve sosyal refahı artırır.
- ✓ İnternet'in sağladığı kişisel gelişim, bilişsel yetkinlik, verimlilik ve uyarlanabilirlik, haysiyet düzeyi, algılanan bağımsızlık, sosyal yeterlilik, kontrol, özerklik, öz-yeterlik ve iyimserlik yaşam kalitesini artırır.

Bilgisayar okuryazarı yaşlı bireyler, çeşitli bilgi kaynaklarını okuyabilme ve farklı dijital platformlar aracılığıyla arkadaşları ve aileleriyle bağlantı kurabilme gibi birçok avantajdan yararlanmaktadır. Siber uzaydayken, siber suçluların ve zorbaların bir sonraki kurbanlarına saldırmayı beklemeleri talihsiz bir durumdur. İnternet etkinliği, tüm büyük arama motorlarına değerli bilgiler sağlamaktadır. Bu bilgi hedefli pazarlama ve diğer veri analizlerinde kullanılmakta, ancak suçluların elindeyken bilişsel eksiklikleri olan savunmasız yaşlı bireylere karşı siber suçları işlemek için kullanılmaktadır (Hildreth vd., 2009: 588).

Hastalık ve yaşın neden olduğu bilişsel gerileme, yaşlı bireylerin mali durumlarını yönetme yeteneklerini etkilemektedir (Karlavish, 2017). Bu değişiklikler, ek gözetim için banka hesabında ikinci bir kişinin olması ve ayrıca bankanın herhangi bir düzensiz finansal faaliyeti rapor etmesini sağlamak gibi önlemlerin dikkate

alınmasını gerektirmektedir. Yaşlı bir bireyin siber dolandırıcılık veya tele-pazarlama dolandırıcılığının kurbanı olduğundan şüpheleniliyorsa, polise ihbar edilmelidir (Munanga, 2019: 4).

Siber suçlar bağlamında ilk adım eğitimidir; bir sonraki adım ise bu suçları meydana geldiklerinde bildirmektir. Böylece kolluk kuvvetleri konuyu ele alabilir. Siber suçların neden olduğu mali kayıpların yanı sıra, siber suç mağdurları psikolojik sıkıntı ve bunun sonucunda teknolojiyi kullanma korkusu yaşayabilir. Psikolojik etkiyi ele almak ve hafifletici önlemleri belirlemek, sağlık profesyonellerinin odak noktasının bir parçası olmalıdır (Geriatric Nursing, 2018).

Federal Bureau of Investigation (2018)'e göre, yaşlı bireylerin siber suçların başlıca adayları olmasında çeşitli faktörler rol oynamaktadır. Kredi geçmişleri ve genellikle güvenen ve yardımcı olan bir neslin parçası oldukları gerçeği, bu tür suçları artırmaktadır. Ayrıca yaşlı bireylerin siber suçları kolluk kuvvetlerine siber suçları bildirme olasılığının da düşük olduğu belirtilmektedir. Siber suçlular tarafından hedef alınan yaşlı bireylerin korunması noktasında aşağıda yer alan hususlar yardımcı olabilir (Federal Bureau of Investigation, 2018; Eric, 2018; Home Instead Senior Care, 2017; Blackwood-Brown, 2018; ConnectSafely, 2018).

- ✓ **Parolalar oluşturmak ve onları güçlendirmek:** Bilgisayar, tablet ve akıllı telefon dahil tüm cihazlarınızı güvenli parolalarla (en az 12 karakter uzunluğunda) kilitlemek önemlidir.
- ✓ **Harekete geçmeden önce düşünmek:** Banka hesabı veya vergilerinizle ilgili bir sorun gibi aciliyet duygusu yaratan e-posta, telefon ve İnternet yoluyla iletişime geçilmesi muhtemelen bir aldatmaca olarak düşünülmeli ve dikkat edilmelidir.
- ✓ **Şüpheli duyulduğunda çöpe atmak:** E-postalardaki bağlantılara tıklamak, dolandırıcıların kişisel bilgilere erişime şeklidir. Bir e-posta alışılmadık görünüyorsa, gönderen kişiyi tanımayan olsa bile en iyi seçenek e-postayı silmektir. Dolandırıcılar, arkadaşlarımızın e-posta adreslerine el koyabilir ve onlar gibi görünen mesajlar gönderebilir. Şüpheli mesajları filtrelemeye yardımcı olması için e-posta hesabı için spam filtreleri açılmalıdır.
- ✓ **Uygulamalardan çıkış yapmak:** Kullanımınız bittiğinde uygulamalardan ve web sitelerinden çıkış yapmak unutulmamalıdır. Bunları bilgisayar ekranınızda açık bırakmak sizi güvenlik ve gizlilik risklerine açık hale getirebilir.
- ✓ **Hesaplarınıza güvenli erişim sağlamak:** Parolalar çalınabildiğinden, hesaplara iki aşamalı kimlik doğrulama eklemek ikinci bir koruma katmanı sağlanmalıdır.
- ✓ **Dikkatli paylaşım yapmak:** Facebook vb. sosyal paylaşım sitelerinde herkese açık olarak neler paylaştığınızı farkında olmak önemlidir. Bilgileri kimlerin görebileceğini sınırlamak için gizlilik ayarları yapılmalı ve konum bilgileri paylaşılmamalıdır.
- ✓ **Güvenlik yazılımı kullanımı:** Güvenilir bir kaynaktan cihazlara güvenlik yazılımı yüklenmeli ve güncel tutulmalıdır. Reklamlardan veya e-postalardan gelen güvenlik güncellemelerine karşı dikkatli olunmalıdır.
- ✓ **Güvenlik duvarı güvenliği korumasının kullanımı:** İşletim sistemi büyük olasılıkla, ayarlamaya gerek kalmadan bilgisayarınızı koruyacak varsayılan güvenlik duvarı ayarlarına sahiptir. Bunu aktive etmek önemlidir.
- ✓ **Tarayıcı güvenliği ayarlarının aktive edilmesi:** Firefox, Google Chrome, İnternet Explorer ve Safari gibi tarayıcılar içine optimum güvenlik belirlemek üzere bu tarayıcıların her birinde ayarlar yapılmalıdır. Hassas verilerin izini bırakmamak için oturumun sonunda göz atma geçmişi temizlenebilir.
- ✓ **Bilgisayar ve İnternet'ten anlayan yetişkin aile üyelerinden yardım alınması:** Siber güvenlik önlemleri her yaşlı tarafından kolay anlaşılabilir ve uygulanabilir olmayabilir. Böyle bir durumda yetişkin bir aile üyesine danışmak ve yardım almak gereklidir.
- ✓ **Eğitim:** Bilgisayar ve İnternet güvenliğinin temelleri, çevrimiçi güvenli olmayan web sitelerinden alışveriş yapmaktan kaçınmak, e-posta, telefon veya İnternet üzerinden mali bilgileri vermemek, arayan kimliğine sahip telefonları kullanmak ve yalnızca bilinen kişilerle konuşmak, telefonla yardım amaçlı katkılarda bulunmaktan kaçınmak gibi konularda yaşlılara eğitim verilmelidir. Yaşlılar bu eğitime açık olmaları ve kendilerini siber suçlara karşı korumaları önemlidir.

5. SONUÇ

Siber güvenlik sorunları, bireyler, kurumlar ve ülkeler için büyük maddi ve manevi kayıplara yol açmaktadır. İnternet’i evlerinde kişisel bilgisayar, tablet, cep telefonu vb. ile kullanan ev kullanıcıları, yeterli güvenlik önlemlerini almadıklarından siber suçlara karşı savunmasız durumda olan büyük bir gruptur. Özellikle yaşlılar, İnternet ve teknolojilerle ilgili diğer yaş gruplarına göre daha az bilgiye sahiptirler. Aktif olarak yaşamın içerisinde yer aldıkları eğitim ve çalışma süreçlerinde İnternet ve teknolojiye yeterince maruz kalmadıklarından sahip oldukları siber dünya bilgisi de sınırlı kalmaktadır. Yaşlılık çalışmalarının henüz dikkat çeken bir alan olmasına paralel olarak, yeni iletişim araçlarının yaş faktörü bazında incelenmesine ilişkin yapılan çalışmaların daha çok genç nesil üzerinde yoğunlaştığı görülmektedir. Bu açıdan bakıldığında yaşlı bireylere yönelik çalışmaların sınırlı olduğu mevcut çalışmaların da daha çok teknik ve psikolojik perspektiflerden beslendikleri görülmektedir.

Toplumun daha genç ve siber uzayı anlayan grupları da yaşlı bireyler gibi siber suçlara maruz kalmaktadır. Çocukların “siber uzay”ın yarattığı olumsuzluklardan korunması için gösterilen özenin yaşlı bireylere de uygulanması gerekmektedir. Bilgi eksikliğinin yarattığı güvenlik açıklarının yanında siber suçlular, manevi manipülasyonlar açısından da zayıf olmaları sebebiyle yaşlıları daha fazla hedef almaktadırlar.

Dünya nüfusunun gün geçtikçe yaşlandığı ve yaşlıları sosyal yaşamdan izole etmemek gerektiği göz önüne alınarak yaşlılara, İnternet ve İnternet’e erişimi sağlayan teknolojiler konusunda eğitim verilmesi gereklidir. Dijital ortamdaki muhtemel tehditler ve tehlikeleri bilen yaşlılar böylelikle daha dikkatli olacak, siber suça maruz kaldıklarında bunu bildirecek, siber güvenlik önlemlerini uygulayacak ve gerektiği yerlerde aile üyelerine/uzmanlara danışacaklardır.

Yaşlıların güvenli bir siber uzayda hayatlarını sürdürebilmeleri için gerekli bilgilerle donatılması oldukça önemlidir. Siber uzay, yalnızca siber suçları barındıran karamsar bir dünya değildir. Yaşlı bireyler, İnternet’e ve siber güvenliğe ilişkin bilgi düzeylerini geliştirebildikleri takdirde siber uzayın onlara sunduğu ve yaşam kalitelerini yükseltebilecek potansiyelleri sunan birçok avantajdan da yararlanabilirler.

KAYNAKÇA

- Al-Mayahi, I. & Mansoor, S.P. (2012). “UAE E-Government: SWOT Analysis and TOWS Matrix”, 2012 Tenth International Conference on ICT and Knowledge Engineering, 21-23 November 2012, IEEE, 201-204. DOI: 10.1109/ICTKE.2012.6408556.
- Arfi, N. & Agarwal, S. (2013a). “Assessment of Types of Cyber Crime Faced By Elderly Across Residence”, The International Journal of Engineering & Science 2(6):1-3.
- Arfi, N. & Agarwal, S. (2013b). “Assessment of knowledge of Cybercrime among Elderly across Residence”, International Journal of Innovative Research & Studies, 2(6):643-650.
- Arfi, N. & Agarwal, S. (2014). “Knowledge of Cyber Crime Among Elderly Across Gender”, International Journal for Advance Research in Engineering and Technology, 2(2):7-9.
- Atakişi, B. & Orhan, F.Ş. (2020). “Orta Yaş ve Üstü Yetişkinlerin Günlük Yaşamda İnternet Kullanma Durumlarının İncelenmesi”, YILDIZ Journal of Educational Research, 5(1):1-26.
- Avcıoğlu, G.Ş. (2017). “Emek, Sibernetik ve Toplum”, Selçuk Üniversitesi Edebiyat Fakültesi Dergisi, (37):515-518 . DOI: 10.21497/sefad.328649.
- Baran, A.G.; Kurt, Ş.K. & Tekeli, E.S. (2017). “Yaşlıların Dijital Teknolojileri Kullanım Düzeyleri Üzerine Bir Araştırma”, İletişim Kuram ve Araştırma Dergisi, (45):1-24.
- Başlıgil, H. & Özdemir, Y. (2011). “Arama “Swot Analizi” Çalışması İle Durum Tespiti ve Senaryo Uygulaması İle Geleceğe Ait Öneriler”, Uluslararası Yükseköğretim Kongresi: Yeni Yönelişler ve Sorunlar, 27-29 Mayıs 2011, UYK-2011, İstanbul.
- Blackwood-Brown, C.G. (2018). “An Empirical Assessment of Senior Citizens’ Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills”, Doctoral Dissertation, Nova Southeastern University, Florida, USA.
- Boz, H. & Karataş, S.E. (2015). “A Review on Internet Use and Quality of Life of the Elderly”, Cypriot Journal of Educational Sciences, 10(3):182-191.
- Chang, L.Y.C. & Grabosky, P. (2014). “Cybercrime and Establishing a Secure Cyberworld”, (Ed. Gill M.) The Handbook of Security, ss. 321-339, Palgrave Macmillan, London.

- Commonwealth of Australia, (2013). *Cybersafety for Seniors: A Worthwhile Journey*, Second Interim Report Joint Select Committee on Cyber-Safety, ISBN 978-1-74366-008-9, https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=jsc/senior_australians/report.htm Erişim 24.02.2021.
- Coker, J. (2020). *Elderly People in the UK Lost Over £4m to Cybercrime Last Year*, Infosecurity Magazine, [https://www.infosecurity-magazine.com/news/elderly-online-uk-lose-four/#:~:text=A%20freedom%20of%20information%20\(FOI,over%20%C2%A34m%20was%20recorded](https://www.infosecurity-magazine.com/news/elderly-online-uk-lose-four/#:~:text=A%20freedom%20of%20information%20(FOI,over%20%C2%A34m%20was%20recorded) Erişim 23.02.2021.
- Connectsafely, (2018). *Senior's Guide for Online Safety*, <https://cyberinsureone.com/online-safety-seniors/> Erişim 24.02.2021.
- Çiçek, B.; Şahin, H. & Erkal, S. (2021). "Yaşlıların Aktif Yaşlanma Tecrübeleri: Nitel Bir Çalışma", *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 17(33):369-397. DOI: 10.26466/opus.773745.
- De Groot, J. (2020). *What is Cyber Security? Definition, Best Practices and More*, <https://digitalguardian.com/blog/what-cyber-security>, Erişim 16.02.2021.
- Eric, C. (2018). "The Ultimate Internet Safety Guide for Seniors", <https://www.safetymagazine.com/blog/the-ultimate-internet-safety-guide-for-seniors/> Erişim 17.02.2021.
- Federal Bureau of Investigation, (2018). *Elder Fraud*, <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud>, Erişim 23.02.2021.
- Fourie, L.; Sarrafzadeh, A.; Pang, S.; Kingston, T.; Hettema, H. & Watters, P. (2014). "The Global Cyber Security Workforce: An Ongoing Human Capital Crisis", *Global Business and Technology Association*, 173-184.
- Geriatric Nursing, (2018). *Psychological Care of the Elderly*, <https://geriatricnursing.org/psychological-care-of-the-elderly/> Erişim 23.02.2021.
- Goud, N. (2021). *How to protect elderly from Cyber Attacks?*, <https://www.cybersecurity-insiders.com/how-to-protect-elderly-from-cyber-attacks/> Erişim 26.03.2021.
- Gratian, M.; Bandi, S.; Cukier, M.; Dykstra, J. & Ginther, A. (2018). "Correlating Human Traits and Cyber Security Behavior Intentions", *Computers & Security*, (73):345-358.
- Grimes, G.A.; Hough, M.G.; Mazur, E. & Signorella, M.L. (2010). "Older Adults' Knowledge of Internet Hazards", *Educational Gerontology*, 36(3):173-192. DOI: 10.1080/03601270903183065
- Grose, M. (2011). *Keeping Kids Safe in a Cyber World*, <https://eas.sa.edu.au/wp-content/uploads/2019/07/Insights-Keeping-kids-safe-in-a-cyber-world.pdf> Erişim 23.02.2021.
- Hekim, H. & Başbüyük, O. (2013). "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2):135-158.
- Hildreth, C.J.; Burke, A.E. & Glass, R.M. (2009). "Elder Abuse", *JAMA*, 302(5):588. DOI: 10.1001/jama.302.5.588.
- Home Instead Senior Care, (2017). *10 Cybersecurity Best Practices for Older Adults*, <https://www.protectseniorsonline.com/resources/cybersecurity-best-practices/> Erişim 24.02.2021.
- Humayun, M.; Niazi, M.; Alshayeb, M. & Mahmood, S. (2020). "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study", *Arabian Journal for Science and Engineering*, 45(4):3171-3189.
- Karlawish, J. (2017). *Whealthcare: Or How We Can Assure Older Adults, Cognitive and Financial Well-Being*, <http://www.whealthcare.org> Erişim 23.02.2021.
- Kurnaz, İ. (2016). "Siber Güvenlik ve İntiltil Kavramsal Çerçeve", *Cyberpolitik Journal*, 1(1):56-77.
- Küçük, O. & Koçak, M.C. (2019). "İleri Yaş Grubu Kişilerin İnternet Kullanım Alışkanlıkları: Trabzon Örneği", *Journal of International Social Research*, 12(65):1162-1168.
- Lehto, M. (2015). "Phenomena in the Cyber World", (Ed. Lehto, M. & Neittaanmaki, P.), *Intelligent Systems, Control and Automation: Science and Engineering*, In *Cyber Security: Analytics, Cyber Security: Analytics, Technology and Automation*, Volume 78, ss.3-29, Finland. DOI: 10.1007/978-3-319-18302-2_1.

- Mbanaso, U. & Dandaura, E. (2015). "The Cyberspace: Redefining A New World", *Journal of Computer Engineering (IOSR-JCE)*, 17(3):17-24. DOI: 10.9790/0661-17361724.
- Mierzwa, S. (2020). Doing More to Support Those Residing in Assisted-Living or Eldercare Facilities with Cybersecurity and Cybercrime Prevention, *Cybersecurity Magazine*, <https://www.researchgate.net/publication/339587518> Erişim 23.02.2021.
- Morrison, B.; Coventry, L. & Briggs, P. (2020). "Corrigendum: Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults", *Frontiers in Psychology*, (11):1306.
- Mulka, L. (2014). *Cyber Literacy for the Digital Age: A Comprehensive Cyber and Digital Literacy Textbook*, B.E. Publishing, 1st Edition, ISBN 978-1-74366-008-9.
- Munanga, A. (2019). "Cybercrime: A New and Growing Problem for Older Adults", *Journal of Gerontological Nursing*, 45(2):3-5.
- Oluga, S.O.; Ahmad, A.; Alnagrat, A. & Sulyman, S.H. (2014). "An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats", *International Journal of Computer Science and Information Security (IJCSIS)*, 12(3):62-100.
- Pool, P. (2013). "War of the Cyber World: The Law of Cyber Warfare", *The International Lawyer*, (47):299-323.
- Rebovich, D. & Corbo, L. (2021). "The Distillation of National Crime Data into A Plan for Elderly Fraud Prevention: A Quantitative and Qualitative Analysis of U.S. Postal Inspection Service Cases of Fraud against the Elderly", *Victims & Offenders*, 16(3):407-430. DOI: 10.1080/15564886.2020.1865225.
- Saariluoma, P. (2016). "Cybersecurity for Old People", *Gerontechnology*, 14(2):63.
- Sammot-Bonnici, T. & Galea, D. (2014). "SWOT Analysis", (Ed. John Wiley & Sons, Ltd), *Wiley Encyclopedia of Management*, Volume 12, ss. 1-8.
- Solms, R.V. & Niekerk, J.V. (2013). "From Information Security to Cyber Security", *Computers & Security*, (38):97-102.
- Sum, S.; Mathews, R.M. & Hughes M. (2009). "Participation of Older Adults in Cyberspace: How Australian Older Adults Use The Internet", *Australas Journal on Ageing*, 28(4):189-193. DOI: 10.1111/j.1741-6612.2009.00374.x. PMID: 19951340.
- Şahin, B. & Yıldırım, A. (2019). "Yaşlı Bireylerde İnternet Kullanımı ile Yaşam Doyumu, Algılanan Sosyal Destek ve Umutsuzluk Düzeyleri Arasındaki İlişkinin İncelenmesi", *Yaşlı Sorunları Araştırma Dergisi (YSAD)*, 12(2):97-106.
- Tekedere H. & Arpacı F. (2016). "Orta Yaş ve Yaşlı Bireylerin İnternet ve Sosyal Medyaya Yönelik Görüşleri", *Türkiye Sosyal Araştırmalar Dergisi*, 20(2):377-392.
- Tuna Uysal, M. (2020). "Yaşlı Bireylerin Sosyalleşmesinde Dijital Teknolojinin Rolü: Dijital Yaşlılar Üzerine Bir Çalışma", *Süleyman Demirel Üniversitesi Fen-Edebiyat Fakültesi Sosyal Bilimler Dergisi*, (50):43-59.
- Zhang, J. (2016). "Aging in Cyberspace: Internet Use and Quality of Life of Older Chinese Migrants", *The Journal of Chinese Sociology*, (3):26. DOI: 10.1186/s40711-016-0045-y.
- Zhang, F. & Kaufman, D. (2015). "Social and Emotional Impacts of Internet Use on Older Adults", *European Scientific Journal*, 11(17):1-15.
- Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, L.; Çetin, F. & Basim, H.M. (2020). "Cyber Security Awareness, Knowledge And Behavior: A Comparative Study", *Journal of Computer Information Systems*, 1-16.