Bilgi | *Journal of Social Sciences*
Sosyal Bilimler Dergisi
ISSN 1302-1761 E-ISSN 2645-9051

Bilgi, 2024, 26 (1): 1-22

ARAŞTIRMA MAKALESİ

Siber Suçlarla Mücadelede Sosyal Hizmet[1]

Mehmethan Uysal[2] Muhammet Ali Köroğlu[3]

MAKALE BİLGİSİ

Başvuru: 05.12.2023
Kabul: 27.12.2023
Online Yayım: 29.05.2024

Anahtar Kelimeler:

Siber Suç
Sosyal Hizmet
Siber Mağduriyet
Dijitalleşme

Kaynak Gösterimi
Uysal, M. &. Köroğlu, M.A. (2024). Siber Suçlarla Mücadelede Sosyal Hizmet. Bilgi Sosyal Bilimler Dergisi, 26 (1), 1-22. doi.org/ 10.54838/ bilgisosyal.1400824

Özet

Amaç- Bu çalışma; siber suçlarla mücadelede sosyal hizmetin rolünü ve etkisini incelemek, önemini vurgulamak, etkili bir şekilde kullanılmasını hedeflemektedir. Buna ek olarak çalışma; toplumun güvenliğinin arttırılması, mağdurlara yardım sağlanması, siber suç faillerinin rehabilitasyonu ve siber suçların önlenmesi gibi alanlarda sosyal hizmetin nasıl katkıda bulunabileceğini ortaya koymayı amaçlamaktadır.

Yöntem/Metodoloji/Dizayn- Çalışmada; İçişleri Bakanlığı, FBI ve ITU gibi kaynaklardan elde edilen veriler kullanılmıştır. Siber suçların tanımı, türleri, etkileri, önlenmesi ve ıslah edilmesi gibi konular ele alınmıştır. Sosyal hizmetin siber suçlarla ilgili görev, sorumluluk ve uygulamaları da incelenmiştir.

Sonuçlar- Çalışmanın sonuçları; siber suçlarla mücadelede sadece hukuki ve teknik önlemlerin yeterli olmadığını, sosyal hizmet gibi insan odaklı ve bütüncül bir yaklaşıma da ihtiyaç duyulduğunu göstermektedir. Sosyal hizmet; siber suçların nedenlerini, etkilerini ve sonuçlarını anlamak, siber suçlara karşı farkındalık ve bilinç oluşturmak, siber suç mağdurlarına psikososyal destek sağlamak, siber suç faillerine eğitim ve danışmanlık vermek, siber suçların önlenmesi için politika ve programlar geliştirmek gibi görevler üstlenmelidir.

Katkı/Farklılıklar- Bu çalışma, siber suçlarla ilgili sosyal hizmet alanında bilimsel birikime katkı sunmayı amaçlamaktadır. Buna ek olarak bu çalışma, siber suçlarla ilgili sosyal hizmet disiplininin güçlü ve zayıf yönlerini, metodolojik ve etik sorunlarını, araştırma boşluklarını ve gelecek çalışmalar için önerilerini ortaya koymaktadır. Ayrıca bu çalışma, siber suçlarla mücadelede multidisipliner bir bakış açısı koyarak sosyal çalışmacılar, araştırmacılar, politika yapıcılar ve ilgili diğer paydaşlar arasında iş birliği ve koordinasyonu teşvik etmektedir.

[1] Bu çalışma, Dr. Öğr. Üyesi Muhammet Ali Köroğlu'nun danışmanlığında yürütülen "Siber Suçlarla Mücadelede Sosyal Hizmet" başlıklı Mehmethan Uysal'ın yüksek lisans tezinden üretilmiştir.

[2] **Sorumlu Yazar**: Yüksek Lisans Öğrencisi, Uşak Üniversitesi, Lisansüstü Eğitim Enstitüsü, Sosyal Hizmet Yönetimi A.B.D., Bir Eylül Kampüsü, Uşak ✉ mehmethanuysal@gmail.com, **ORCID**: 0000-0002-5248-4663

[3] Dr. Öğr. Üyesi, Uşak Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Sosyal Hizmet Bölümü, Bir Eylül Kampüsü, Uşak. ✉ muhammet.koroglu@usak.edu.tr, **ORCID**: 0000-0001-8593-6139

Bilgi | *Journal of Social Sciences*
Sosyal Bilimler Dergisi
ISSN 1302-1761 E-ISSN 2645-9051

Bilgi, 2024, 26 (1): 1-22

RESEARCH ARTICLE

Social Work in the Fighting Cybercrimes

Mehmethan Uysal[1] Muhammet Ali Köroğlu[2]

ARTICLE INFO

Submitted: 5.12.2023
Accepted: 27.12.2023
Published Online: 6.5.2024

Keywords:

Cybercrime
Social Work
Cyber Victimization
Digitalization

To cite this article
Uysal, M. &. Köroğlu, M.A. (2024). Social Work in the Fighting Cybercrimes. Bilgi Journal of Social Sciences, 26 (1), 1-22. doi.org/10.54838/bilgisosyal.1400824

Abstract

Purpose - This study aims to examine the role and impact of social work in fighting cybercrime, to emphasize its importance, and to target its effective use. In addition, the study aims to reveal how social work can contribute to the areas such as increasing the security of the society, providing assistance to the victims, rehabilitating the cybercrime perpetrators, and preventing cybercrimes.

Methodology/Approach/Design - In the study; data obtained from sources such as the Ministry of Interior, FBI and ITU were used. Issues such as the definition, types, effects, prevention, and rehabilitation of cybercrimes are discussed. The duties, responsibilities and practices of social work related to cybercrimes are also examined.

Findings - The results of the study show that legal and technical measures alone are not sufficient in fighting cybercrime, and that there is a need for a human-centered and holistic approach such as social work. Social work should undertake tasks such as understanding the causes, effects, and consequences of cybercrime, creating awareness and consciousness against cybercrime, providing psychosocial support to cybercrime victims, providing education, and counselling to cybercrime perpetrators, and developing policies and programs for preventing cybercrime.

Originality/Value - This study aims to contribute to the scientific accumulation in the field of social work related to cybercrime. In addition, this study reveals the strengths and weaknesses of the social work discipline related to cybercrime, the methodological and ethical problems, the research gaps, and the suggestions for future studies. Furthermore, this study promotes collaboration and coordination among social workers, researchers, policy makers, and other relevant stakeholders by putting a multidisciplinary perspective in fighting cybercrime.

[1] **Corresponding Author**: Graduate student, Uşak University, Graduate Education Institute, Social Service Management., ✉ mehmethanuysal@gmail.com, **ORCID**: 0000-0002-5248-4663
[2] Asst. Prof, Uşak University, Faculty of Economics and Administrative Sciences, Department of social work. ✉ muhammet.koroglu@usak.edu.tr, **ORCID**: 0000-0001-8593-6139

Giriş

Siber suç, dijital ortamda işlenen ve çeşitli zararlar doğuran bir suç türüdür. Siber suçun tanımı farklı kaynaklarda benzer şekilde verilmektedir (Çalıcı, 2011: 18-19). En kapsamlı ifadeyle siber suç; bilgisayar, ağlar ve diğer dijital araçları kullanarak bilişim sistemlerine ve dijital altyapılara zarar vermek, hukuka aykırı yollarla gelir veya menfaat sağlamak, kişisel bilgileri çalmak veya manipüle etmek gibi amaçlarla işlenen suçlardır (McQuade III, 2008: 43-44).

Siber suçlar, günümüzde dijitalleşmenin ve teknolojik gelişmelerin getirdiği fırsatlarla birlikte insanlık için büyük bir tehdit oluşturmaktadır (Bahar, 2018: 3). İnternetin yaygınlaşması, mobil cihazların kullanımının artması ve sosyal medya platformlarının popülerleşmesi gibi etkenler, siber suçluların saldırılarını kolaylaştırmakta ve yayılma alanlarını genişletmektedir (Güngör, 2015: 28-35). We Are Social (2023)'ın yayımladığı rapora göre 2017 ile 2022 yılları arasında küresel bazda internet kullanıcı sayısı %28,36; mobil cihaz kullanıcı sayısı %6,4; sosyal medya kullanıcı sayısı ise %49,22 oranında artmıştır. Siber suçların en yaygın türlerinden olan fidye yazılımı saldırıları da bu yıllarda %168,6 oranında artış göstermiştir (Connolly ve Wall, 2019: 2; SonicWall, 2023).

Ayrıca nesnelerin interneti gibi yeni teknolojiler, siber suçluların hedef alabileceği daha fazla cihaz ve sistem ortaya çıkarmıştır (Yıldırım, 2019: 88). Nesnelerin interneti, fiziksel nesnelerin internete bağlanarak veri alışverişi yapmasını sağlayan bir kavramdır (Gündüz ve Daş, 2018: 328). Bu sayede akıllı evler, akıllı şehirler, akıllı sağlık, akıllı ulaşım gibi alanlarda yeni uygulamalar geliştirilebilmektedir. Ancak nesnelerin interneti, aynı zamanda siber güvenlik açısından birçok risk ve zorluğu da beraberinde getirmektedir. Nesnelerin interneti cihazları; genellikle düşük maliyetli, düşük güç tüketimi ve düşük işlem kapasitesine sahip olmaları nedeniyle, güvenlik önlemleri açısından yetersiz kalmaktadır (Akince, 2021: 72). Bu da siber suçluların bu cihazları ele geçirerek kötü amaçlı yazılımlar yaymak, veri çalmak, hizmeti engellemek, fidye istemek gibi saldırılar gerçekleştirmesine

olanak sağlamaktadır. Dolayısıyla nesnelerin interneti teknolojisinin yaygınlaşmasıyla beraber siber suçlar daha da karmaşık ve tehlikeli bir hâl almaktadır (Yanarışık, 2020: 322).

Siber suçlar, internet ve bilişim teknolojilerinin kullanıldığı her alanda işlenebilen ve mağdurların hayatlarını olumsuz yönde etkileyebilen suçlardır (Sandilaç, 2022: 154-156). Siber suç mağdurları, sadece maddi değil, aynı zamanda manevi, psikolojik, hukuki ve etik zararlar da görebilmektedir (Küçükay, 2019). Bu nedenle, mağdurların yaşadıkları travmaları atlatmaları, haklarını savunmaları ve topluma yeniden uyum sağlamaları için profesyonel yardıma ihtiyaç duymaktadırlar (Güdek, 2016: 55-62).

Sosyal çalışmacılar, siber suç mağdurlarına yönelik önemli bir rol üstlenmektedir. Sosyal çalışmacılar, mağdurlara psikososyal destek, hak koruma, adalet arayışı ve toplumsal farkındalık gibi çeşitli hizmetler sunmaktadır (Albayrak, 2021: 384-386). Bu hizmetler, mağdurlara çeşitli yönlerden destek olmaktadır. Öncelikle, mağdurların duygu ve düşüncelerini anlamak, empati kurmak, güven ve destek ortamı oluşturmak, stresle başa çıkma yöntemleri öğretmek, özgüven ve özsaygılarını artırmak, sosyal ilişkilerini geliştirmek ve yaşam kalitelerini yükseltmek gibi psikososyal hizmetler sunmaktadır (Özbay, 2017: 59-62).

Bu psikososyal hizmetlerin yanı sıra, mağdurların haklarını bilmesine, ihlal edilen haklarını tespit etmesine, hak arama sürecinde gerekli mercilere başvurmasına, hukuki süreçleri takip etmesine, hukuki danışmanlık almasına ve mağduriyetlerinin giderilmesi için gerekli maddi, sosyal ve hukuki destekleri sağlamasına yardımcı olmaktadır. Son olarak, mağdurların ve suçluların tespit edilmesi, yakalanması, yargılanması ve cezalandırılması için gerekli adli süreçlere katılmasına, delil toplamasına, tanıklık yapmasına, ifade vermesine, mağdur haklarını kullanmasına, siber suçların önlenmesi, siber güvenliğin sağlanması ve siber suç mağdurlarının desteklenmesi için toplumsal farkındalık oluşturmasına katkıda bulunmaktadır (Adli Destek ve Mağdur Hizmetleri Dairesi Başkanlığı, 2021; Öztürk, Kayadibi ve Taşdemir, 2021).

Sosyal çalışmacılar, siber suç mağdurlarına yönelik bu hizmetleri sunarken siber suçlarla ilgili güncel bilgi ve becerilere sahip olmak, siber suç mağdurlarının ihtiyaç ve beklentilerini doğru analiz etmek, etik ilke ve değerlere uygun davranmak, iş birliği ve koordinasyon içinde çalışmak, sürekli kendini geliştirmek ve mesleki denetim almak gibi hususlara dikkat etmelidir. Bu sayede, siber suç mağdurlarının yaşadıkları sorunlarla başa çıkmalarına, haklarını savunmalarına ve topluma yeniden uyum sağlamalarına katkıda bulunmaktadır (Şamar, 2018).

Bu çalışmanın amacı siber suçlarla mücadelede sosyal hizmetin yeri ve önemini incelemektir. Dört bölümden oluşan çalışmada teknolojik dönüşümler ve siber suçlar hakkında bilgi verilmekte, ikinci olarak siber suç ve sosyal hizmet ilişkisi incelenmekte, üçüncü olarak Dünyadaki siber suçlarla mücadelede sosyal hizmet uygulama örnekleri verilmekte, son olarak ise siber suçlar istatistikleri sosyal hizmet perspektifinden tartışılmaktadır.

1. Teknolojik Dönüşümler ve Siber Suçlar

Teknoloji, insanların belirli amaçlar için kullanabilecekleri araçlar, sistemler, teknikler ve becerilerin toplamıdır (Layton, 1974). İnsanların doğal çevrelerini değiştirmelerine, ihtiyaçlarını karşılamalarına ve sorunlarını çözmelerine yardımcı olur. Bilim, mühendislik, sanat ve matematik gibi birçok disiplinle ilişkilidir. Teknoloji, tarihsel olarak insan toplumlarının gelişiminde önemli bir rol oynamıştır (Şenel ve Gençoğlu, 2003: 56-59). Teknolojinin ilerlemesi, son yıllarda büyük bir ivme kazanmıştır. Bilgisayarlar, internet, cep telefonları ve diğer dijital teknolojiler, hayatımızın her alanında önemli bir etkiye sahip olmuştur. Yapay zekâ ve makine öğrenimi teknolojilerinin geliştirilmesi de birçok sektörde büyük bir devrim gerçekleştirmiştir.

Teknoloji sayesinde insanlar kıtaların ötesindeki türdeşleriyle etkileşim kurabilme olanağı elde etmiştir (Çelik, 2012: 61). Geçmiş toplumlarda da görüldüğü gibi etkileşim içerisinde olan bireyler mutlaka kültürel alışverişte bulunurlar (Yıldırım, 2014: 2-4). Sürekli bir sosyal etkileşim içerisinde

olan bireyler küreselleşme sürecinin başlamasına sebep olmuşlardır (Kaya ve Aydemir, 2011: 16). Küreselleşmeyle birlikte çeşitli sorunlar ortaya çıkmıştır. Bunlar arasından en önemlilerden biri de kuşkusuz siber güvenlik sorunudur. Küreselleşmeden önce suçluların yaşadıkları alanlarının ötesine geçmeleri oldukça zordu (Kıvılcım, 2013: 222-223). Bundan dolayı genel olarak işlenen suçlar belirli ortam içerisinde gerçekleşmiştir. Fakat teknolojinin gelişmesiyle gerek ulaşımın kolay olması gerek sanal ortamların tüm dünyaya kolaylıkla açılması sebebiyle suç kavramı da yeniden değerlendirilmeye başlanmıştır (Yılmaz, 2017: 27).

Siber suç, üzerinde tam olarak uzlaşıya varılamayan kavramlardan biridir. Oxford Dictionary'e göre siber suç, bilgisayar korsanlarının çeşitli ağlara ve sistemlere zarar verme ya da yok etme girişimidir. Loader ve Thomas (2013)'e göre ise bilgisayar ve küresel ağlar aracılığıyla işlenen yasa dışı faaliyetlerdir. Bu iki tanımda da görüldüğü üzere kavramsal farklılıklar söz konusu olsa da anlamsal olarak belirtilmeye çalışılan ifade aynıdır. Yani kısacası siber suç, elektronik cihazlarla ya da bu aygıtlara bağlı ağlar aracılığıyla işlenen suçların tümüdür.

Günümüzde, siber suç teknolojik gelişmelerle birlikte artan bir sorun haline gelmiştir. İnternet, insanların günlük hayatlarının vazgeçilmez bir parçası olmasının yanı sıra, kötü niyetli insanların da istismar ettiği bir alan olmuştur. Siber suçlar; bireylerin, kurumların ve devletlerin maddi veya manevi zararlara uğramasına ve kişisel bilgilerin ifşa edilmesine neden olabilmektedir (Altunok ve Vural, 2011: 332).

Siber suçları önlemek ve cezalandırmak için birçok ülke yasal çerçeveler oluşturmuştur. Buna rağmen siber suçlarla mücadele etmek her zaman zor bir süreç olmuştur. Çünkü siber çete üyeleri genellikle farklı ülkelerde yaşamakta ve bu ülkelerin yasal sistemleri arasında farklılıklar olabilmektedir (Holt ve Bossler, 2015). Ayrıca siber suçluların kullandığı teknolojiler sürekli olarak gelişmekte ve siber güvenlik yazılımları bu değişikliklere ayak uydurmak zorunda kalmaktadır. Siber suçlarla mücadele etmenin sadece teknik ve yasal yönleri yoktur, aynı zamanda toplumsal ve insani yönleri de

vardır (Çakır ve Taşer, 2023: 364). Siber suçların mağdurları ve faili olan kişilerin psikolojik, sosyal ve ekonomik durumları da dikkate alınmalıdır. Bu nedenle, siber suçlarla ilgili çalışmalar, sadece siber güvenlik uzmanları ve hukukçular tarafından değil, aynı zamanda toplumun refahını ve bireylerin ihtiyaçlarını karşılamayı amaçlayan meslek grupları tarafından da yürütülmelidir (Broadhurst, 2006: 13-15).

2. Siber Suç ve Sosyal Hizmet İlişkisi

Sosyal hizmet, insanların yaşam kalitesini artırmak ve insan haklarını korumak amacıyla birey, grup ve toplum düzeyinde hizmet veren bir meslektir. Sosyal hizmet, insanların karşılaştığı sosyal sorunlara çözüm bulmak için bilimsel yöntemler, mesleki değerler ve etik ilkeler çerçevesinde çalışır (Nicholas, Rautenbach ve Maistry, 2010).

Sosyal hizmet, günümüzün en önemli sosyal sorunlarından biri olan siber suçlarla mücadele etmek için gerekli bilgi, beceri ve tutuma sahiptir. Sosyal çalışmacılar, bu alandaki zorluklarla başa çıkmak için çok yönlü bir rol üstlenirler ve siber suç mağdurlarına yardım etmek, haklarını savunmak ve yasal süreçlerde destek olmak, onların travmatik deneyimlerini anlamalarına yardımcı olur (Jebaseelan ve Fonceca, 2021). Ayrıca, siber suç faillerine psikoterapi sunarak onların davranışlarını değiştirmeye çalışırlar.

Siber suçlar, toplumun her kesimini etkileyebilir, ancak bazı gruplar daha fazla risk altındadır. Bunların başında dezavantajlı gruplar gelmektedir. Dezavantajlı gruplar; sosyal, ekonomik, biyolojik veya kültürel nedenlerle toplumda eşit olmayan bir konuma sahip gruplardır. Dezavantajlı gruplar arasında yaşlılar, engelliler, yoksullar, kadınlar ve çocuklar sayılabilir (Arkan ve İrez, 2021: 15-16). Bu gruplar, siber suçlara karşı daha savunmasızdır. Nitekim genellikle dijital okuryazarlık düzeyleri düşüktür ve siber suçlara karşı korunma yollarını tam olarak bilmezler. Ayrıca bu gruplar siber suç mağduru olduklarında daha fazla zarar görebilirler çünkü maddi kaynakları kısıtlıdır, sosyal destekten yoksundurlar veya yasal haklarını savunacak güce sahip değildirler (Das ve Nayak, 2013: 147).

Siber suçlar ve dijital güvenlik konusunda toplumsal farkındalığı arttırmak için sosyal çalışmacılar önemli bir rol oynar. Danışmanlık oturumları, seminerler ve atölye çalışmaları gibi etkinliklerle bireyleri ve toplulukları siber suçların tehditleri, önemli güvenlik önlemleri ve kişisel mahremiyetin korunması hakkında bilgilendirebilirler (Zengin ve Çalış, 2017: 64). Sosyal çalışmacılar, bireylerin ve ailelerin dijital güvenlik tehlikelerini değerlendire bilir ve etkili önlemler almasına yardımcı olabilir. Siber zorbalık, çevrimiçi dolandırıcılık ve siber saldırılar gibi konularla ilgili bireysel ve aile bazlı risk faktörlerini belirleyerek uygun güvenlik önlemlerinin alınmasına rehberlik edebilirler (Çaycı ve Çaycı, 2017: 167-168).

Siber suçlara maruz kalan kişiler ve aileler, ciddi psikolojik ve sosyal sonuçlarla karşı karşıya kalabilir. Sosyal çalışmacılar, travma sonrası stres, güvensizlik ve diğer sorunlarla başa çıkmalarına yardımcı olabilirler. Aynı zamanda, siber suçlarla ilgili hukuki süreçleri yönlendirerek mağdurların haklarını koruyabilirler. Sosyal çalışmacılar, polis, savcılık, sivil toplum kuruluşları ve diğer ilgili paydaşlarla iş birliği yaparak siber suçlarla mücadelede etkili bir ağ oluşturabilirler (Tropina, Callanan ve Tropina, 2015: 46). Bu birliktelik sayesinde, siber suçların önlenmesi ve soruşturulması için daha iyi stratejiler geliştirilebilir ve mağdurlara daha iyi hizmet sağlanabilir.

Siber suç failleri, genellikle farklı motivasyonlarla bu suçları işlemektedirler. Bu motivasyonlar arasında maddi kazanç, siyasi nüfuz, ideolojik inanç, kişisel tatmin, intikam veya eğlence gibi faktörler sayılabilir (Harmancı, Gözübenli ve Zengin, 2015: 105). Ancak bu suçluların yakalanması ve cezalandırılmasının ötesinde, onların topluma yeniden entegre edilmeleri ve rehabilitasyonları da önemli bir sorundur (Derin ve Öztürk, 2021: 242). Siber suç faillerinin rehabilitasyonu, toplumlar için önemli bir sosyal hizmet ihtiyacını ortaya koymaktadır. Sosyal çalışmacılar, siber suç faillerinin rehabilitasyonunda çeşitli zorluklarla karşı karşıyadır. Siber suçlar genellikle karmaşık ve teknik bilgi gerektiren suçlar olduğu için, bu suçları işleyen kişilerin rehabilitasyonu da özel bir uzmanlık gerektirir. Bu konuda özel uz-

manlığı olmayan kişilerin müdahalesi siber suç faillerinin topluma entegrasyonunu zorlaştırabilir (Lim ve Thing, 2022: 7-8).

3. Dünyadaki Siber Suçlarla Mücadelede Sosyal Hizmet Uygulamaları

Sosyal hizmet, siber suçlarla mücadele için dünyanın çeşitli yerlerinde farklı kurum ve kuruluşların yürüttüğü çeşitli projeler, programlar, hizmetler ve faaliyetlerle örnek oluşturmaktadır. Bu alanda önde gelen ülkeler arasında Avustralya, ABD ve İngiltere bulunmaktadır.

Avustralya, siber suç mağdurlarına yönelik kapsamlı ve öncü bir hizmet sunan bir ülkedir. 2015 yılında, siber suç mağdurlarına destek sağlamak amacıyla "eSafety Commissioner" adlı bir kurum oluşturmuştur. Bu kurum, siber zorbalık, siber taciz, siber şiddet, siber istismar gibi konularda mağdurlara danışmanlık, eğitim, rehberlik, şikâyet, raporlama gibi hizmetler sunmaktadır (Morgan ve diğerleri, 2016: 35-45). Ayrıca, siber suç mağdurlarının haklarını savunmak, siber suçluları cezalandırmak ve siber suçları önlemek için yasal, teknik ve toplumsal düzeyde çalışmalar yürütmektedir.

eSafety Commissioner, siber suç mağdurlarının ihtiyaçlarına göre bireysel, grup ve toplum odaklı hizmetler vermektedir (UNICEF, 2022: 91). Bireysel düzeyde, mağdurlara psikolojik destek, hukuki yardım, güvenlik tedbirleri, zarar tazmini gibi hizmetler sağlamaktadır. Grup düzeyinde, mağdurların birbirleriyle iletişim kurmalarını, dayanışma göstermelerini, deneyimlerini paylaşmalarını ve birlikte çözüm üretmelerini sağlayan platformlar oluşturmaktadır. Toplum düzeyinde, siber suç mağdurlarına karşı farkındalık yaratmak, siber suçlara karşı bilinçlendirmek, siber güvenlik kültürünü geliştirmek, siber suçla mücadelede iş birliği yapmak gibi hizmetler sunmaktadır. Ayrıca sosyal hizmet öğrencilerine ücretsiz çevrimiçi seminerler vermektedir (Harris ve diğerleri, 2022: 19-22).

ABD'de Cybercrime Support Network (CSN) adlı bir kurum, siber suçlulara yönelik sosyal hizmet uygulamaları gerçekleştirmektedir. CSN, siber suçluların ıslahı ve topluma kazandırılması amacıyla kurulmuş, kâr amacı gütmeyen bir sivil toplum kuruluşudur. CSN; siber suçlulara, bilişim tekno-

lojilerinin olumlu amaçlar için kullanılmasını öğreten, mesleki ve sosyal becerilerini geliştiren, topluma uyumlarını sağlayan bir program yürütmektedir (Cobb, 2019: 626). Bu program, siber suçluların bireysel, ailesel, eğitsel, mesleki ve toplumsal durumlarını değerlendiren, onlara bireysel ve grup danışmanlığı, meslek edindirme, mentorluk, gönüllülük, burs, staj gibi hizmetler sunan, onların siber suçluluktan uzak durmalarını ve topluma faydalı bireyler olmalarını teşvik eden bir programdır. CSN, bu programı, siber suçluların ihtiyaçlarına, ilgi alanlarına ve yeteneklerine göre kişiselleştirmekte ve onlara birebir destek vermektedir (Atay, Sweetland ve Carr, 2020: 21-28).

CSN'nin yürüttüğü program, siber suçlulara sosyal hizmet sunmanın örneklerinden biridir. Bu program, siber suçluların topluma kazandırılmasına katkı sağlamakta, onların bilişim teknolojilerini olumlu amaçlar için kullanmalarına imkân tanımakta ve onların yaşam kalitesini artırmaktadır. Bu program, aynı zamanda, siber suçlulukla mücadele etmenin, sadece cezai yaptırımlarla değil, aynı zamanda sosyal hizmet yaklaşımlarıyla da mümkün olduğunu göstermektedir. Bu program, siber suçlulara sosyal hizmet sunmanın önemini, gerekliliğini ve faydalarını ortaya koymaktadır (Force, 2021: 37-45)

İngiltere'de ise siber suç mağdurlarına yönelik sosyal hizmet uygulamalarından biri, Cyber Helpline adlı bir kuruluştur. Cyber Helpline, siber suç mağdurlarına ücretsiz, gizli ve uzman yardım sunan bir çevrimiçi platformdur. Bu platform, siber suç mağdurlarının sorunlarını anlamak, çözüm yolları sunmak ve gerekli kurumlarla iletişime geçmek gibi hizmetler vermektedir. Cyber Helpline, siber suç mağdurlarının ihtiyaçlarına göre bireyselleştirilmiş bir destek planı oluşturmaktadır. Bu plan, siber suç mağdurlarının siber saldırıdan kurtulmalarına, zararlarını en aza indirmelerine ve gelecekteki riskleri azaltmalarına yardımcı olmaktadır (Pina, Storey, Duggan ve Franqueira, 2021: 34-36).

4. Tartışma

İnternet, günümüzde hayatımızın vazgeçilmez bir parçası haline gelmiştir. İnternet sayesinde, bilgiye erişim, iletişim, eğitim, eğlence, ticaret, sağlık gibi pek çok alanda kolaylık ve fayda sağlanmaktadır (Akkaya, 2021: 2023-2024). Ancak internetin sunduğu bu imkanlar, aynı zamanda bazı riskler ve sorunlar da doğurmaktadır. Bunların başında, siber suçlar gelmektedir. Siber suçlar, bilişim teknolojilerinin kötüye kullanılması sonucu ortaya çıkan ve toplumun huzur, güvenlik ve refahını tehdit eden suçlardır (Doğan ve Abacı, 2021).

Tablo 1. İnternet Kullanıcı Sayısı ve Oranı

Yıl	Dünya nüfusu (milyar)	İnternet kullanıcıları (milyar)	İnternet kullanım oranı (%)
2018	7.6	3.9	51,2
2019	7.7	4.1	53,6
2020	7.8	4.6	58,7
2021	7.9	4.9	62,7
2022	8.0	5.3	66,3

Kaynak: (ITU, 2023)

Tablo 1, internet kullanıcı sayısı ve oranının son beş yılda dünya çapında arttığını göstermektedir. Bu artış, internetin sunduğu fırsatlar, kolaylıklar ve imkanlar nedeniyledir. Ancak, internetin yaygınlaşması, aynı zamanda siber suçların da artmasına neden olmaktadır. Çünkü, internet, siber suçlulara anonimlik, erişim kolaylığı, düşük maliyet, yüksek kazanç, küresel etki, cezai yaptırımlardan kaçınma gibi avantajlar sağlamaktadır (Dokgöz, 2023). Bu durum, siber suçların önlenmesi ve cezalandırılması için daha etkin ve işbirlikçi stratejiler geliştirilmesini gerektirmektedir. Ayrıca, internet kullanıcılarının siber güvenlik bilincini artırmak, siber suçlara karşı korunma yöntemlerini öğrenmek ve siber suçlara maruz kaldıklarında nereye başvuracaklarını bilmek de önemlidir (Bacıoğlu, 2022: 30-34). Sosyal hiz-

met, bu konularda toplumu bilgilendirmek, eğitmek ve yönlendirmek için çalışabilir.

İçişleri Bakanlığı tarafından Haziran 2020'de 30 büyük şehri kapsayacak şekilde 18 yaş üstü 649 kişi ile, 2021 yılında ise Şubat ve Mart aylarında 31 şehri kapsayacak şekilde 18 yaş üstü 650 kişi ile toplamda iki adet çalışma yapılmıştır.

Tablo 2. Türlere Göre Siber Suç Mağduriyet Oranı

Suç Türü / Ay-Yıl	Haziran 2020	Şubat 2021	Mart 2021
Bilgisayar Korsanlığı	%0,8	%8,4	%24,2
Kişilere Karşı Siber Suçlar	%1,8	%7,1	%25,8
Siber Ekonomik Suçlar	%2,3	%15,8	%12,9
Zararlı Yazılım Bulaşması	%5,1	%15,2	%52,1
En Az 1 Siber Suç Mağduriyeti	%7,1	%38,8	%36,9

Kaynak: (İçişleri Bakanlığı, 2021: 95-96)

İçişleri Bakanlığı tarafından 2021 yılında yayımlanan bir rapora göre, Türkiye'de siber suç mağduriyet oranları önemli ölçüde artmıştır. Tabloya göre, en yaygın siber suç türü zararlı yazılım bulaşmasıdır. Bu suç türünde mağduriyet oranı Haziran 2020'de %5,1 iken Mart 2021'de %52,1'e yükselmiştir.

En az bir siber suç mağduriyeti yaşayanların oranı da önemli ölçüde artmıştır. Haziran 2020'de %7,1 olan bu oran, Şubat 2021'de %38,8'e, Mart 2021'de ise %36,9'a yükselmiştir. Bu, yaklaşık 5 katlık bir artıştır. Bu veriler ışığında Türkiye'de siber suçların arttığı açıkça gözlemlenmektedir. Bu artışın önüne geçmenin bir yolu, sosyal hizmetin siber suçlara karşı farkındalık, önleme ve müdahale çalışmalarını güçlendirmesidir. Sosyal hizmet, siber suçların nedenlerini, etkilerini ve çözümlerini bireysel, ailevi, toplumsal ve politik düzeylerde ele alabilir. Sosyal hizmet, siber suç mağdurlarına psikososyal destek sağlayabilir, siber suç faillerine rehabilitasyon hizmetleri sunabilir, siber suç riski altındaki gruplara koruyucu eğitimler verebilir

ve siber suçla mücadele için yasal ve etik normları savunabilir. Böylece sosyal hizmet, siber suçların önlenmesi ve azaltılması için etkili bir araç olabilir.

Tablo 3. Siber Suç Mağduriyetinin Etkileri

Siber Suçun Mağdura Etkisi	**Oranı**
Kişisel Bilgilerimin Çalınmasından Korkuyorum	%75,1
İnterneti Kullanırken Daha Dikkatli Davranıyorum	%74,2
İtibarımın Zedelenmesinden Korkuyorum	%69,2
Siber Farkındalığım Arttı	%67,1
Finansal Bilgilerimin Çalınmasından Korkuyorum	%66,9
Siber Suçlarla İlgili Endişelerim Arttı	%63,3
Online Alışkanlıklarım Değişti	%54,2
Stres ve Kaygı Sorunları Yaşadım	%36,3
Psikolojik Sorunlar Yaşadım	%21,7

Kaynak: (İçişleri Bakanlığı, 2021: 109-110)

Tablo 3'ü yorumlarken siber suçların sadece bireylerin değil, toplumun da güvenliğini ve refahını tehdit eden bir sorun olduğunu göz önünde bulundurmak gerekir. Siber suçlar, bireylerin özel hayatlarını, kişisel verilerini, finansal durumlarını, itibarlarını ve psikolojik sağlıklarını olumsuz yönde etkileyebilmektedir. Dolayısıyla siber suçlarla mücadele etmek, siber suçlara karşı korunmak ve siber suç mağdurlarına destek olmak, sosyal hizmetin önemli bir alanıdır. Sosyal hizmet, siber suçlarla ilgili toplumda farkındalık oluşturmak, siber suç mağdurlarına psikososyal yardım sağlamak, siber suçlara karşı önleyici ve koruyucu tedbirler almak, siber suçlara dair hukuki düzenlemelerin yapılmasını teşvik etmek gibi görevler üstlenebilir. Bundan dolayı sosyal hizmet, siber suçların bireysel ve toplumsal etkilerini azaltmak için multidisipliner bir yaklaşımla çalışmalıdır. Sosyal hizmet, siber suçlarla ilgili olarak hem kurumsal hem de bireysel düzeyde müdahale edebilen bir meslek grubudur.

Tablo 4. Son Beş Yılda Şikayetler ve Kayıplar

Yıl	Şikâyet Sayısı	Toplam Zarar (Milyar $)
2018	351.937	2.7
2019	467.361	3.5
2020	791.790	4.2
2021	847.376	6.9
2022	800.944	10.3
Toplam	**3.259.408**	**27.6**

Kaynak: (IC3, 2023)

FBI'nın İnternet Suç Şikâyet Merkezi (IC3) tarafından yayımlanan 2022 yılı siber suç raporuna göre son beş yılda IC3, yaklaşık 3.26 milyon adet siber suç şikâyeti almıştır. Bu, bir önceki beş yıla göre %129,4'lük bir artış anlamına gelmektedir (IC3, 2018). Bu şikâyetlerin toplam zararı ise son beş yılda yaklaşık 27.4 milyar dolardır.

Tablo 4'e göre, son beş yılda çevrimiçi suçlardan kaynaklanan şikâyet sayısı ve toplam zarar artmıştır. Bu artışın başlıca nedenleri, COVID-19 pandemisi, çevrimiçi ortamda daha fazla zaman geçirme, aşı dağıtımı ile ilgili dolandırıcılık yöntemleri ve çevrimiçi suçluların saldırı tekniklerinin gelişmesidir. 2022 yılında, şikâyet sayısı 2021 yılına göre %5,5 azalsa da, toplam zarar %49,3 artarak 10.3 milyar dolara ulaşmıştır. Her bir şikâyetten kaynaklanan ortalama zarar ise 12.857 dolardır.

Çevrimiçi suçlara maruz kalan veya tanık olan insanların, ilgili kurumlara başvurması ve sosyal hizmetlerden destek alması gerekmektedir. Sosyal hizmet mesleği, çevrimiçi suçların önlenmesi, mağdurların korunması ve rehabilite edilmesi konusunda önemli bir rol oynamaktadır. Sosyal hizmet mesleği, çevrimiçi suçlara karşı insan hakları, sosyal adalet, profesyonel etik ve kanıta dayalı uygulama ilkelerini temel almaktadır. Sosyal hizmet mesleği, çevrimiçi suçlara karşı bütüncül, eleştirel ve yaratıcı bir yaklaşım sergilemektedir.

Sonuç ve Değerlendirme

Siber suçlar, günümüzde giderek artan ve toplumun her kesimini etkileyen bir sorundur. Siber suçlar; bireylerin, kurumların ve devletlerin güvenliğini, haklarını ve özgürlüklerini tehdit etmektedir. Siber suçlarla mücadele, sadece teknik ve yasal önlemlerle değil, aynı zamanda sosyal ve psikolojik boyutlarıyla da ele alınması gereken bir konudur.

Sosyal hizmet, siber suçlarla mücadelede önemli bir rol oynamaktadır. Sosyal hizmet, siber suç mağdurlarına, faillerine ve risk altındaki gruplara yönelik koruyucu, önleyici, iyileştirici ve rehabilite edici hizmetler sunmaktadır. Sosyal hizmet, siber suçların nedenlerini, etkilerini ve çözüm yollarını bireysel, ailevi, toplumsal ve kültürel bağlamlarda değerlendirmektedir. Sosyal hizmet, siber suçlarla ilgili farkındalık, eğitim, danışmanlık, destek, savunuculuk ve iş birliği gibi faaliyetler yürütmektedir.

Ancak, sosyal hizmetin siber suçlarla mücadelede karşılaştığı bazı sorunlar da vardır. Bu sorunlar, siber suçların uluslararası ve çok boyutlu niteliği, siber suçların hızlı ve sürekli değişimi, siber suçlarla ilgili yasal ve etik düzenlemelerin yetersizliği, siber suçlarla ilgili bilgi ve beceri eksikliği, siber suçlarla ilgili araştırma ve yayınların azlığı, siber suçlarla ilgili kurumsal ve sektörel iş birliğinin zayıflığı, siber suç mağdurlarının, faillerinin ve risk altındaki grupların tanımlanması, ulaşılması ve hizmet verilmesindeki güçlükler olarak sıralanabilir.

Siber suçlarla ilgili yasal ve etik düzenlemeler, siber suçların niteliğine, kapsamına ve etkilerine uygun olarak güncellenmeli, uygulanmalı ve denetlenmelidir. Bu düzenlemeler, siber suçların önlenmesi, mağdurların korunması ve faillerle müdahale edilmesi gibi konularda etkili olmalıdır. Ayrıca, bu düzenlemeler, sosyal çalışmacılar gibi siber suçlarla ilgilenen meslek gruplarının görüş ve önerilerini de dikkate almalıdır. Böylece, siber suçlarla mücadelede daha kapsamlı ve bütüncül bir yaklaşım benimsenmiş olacaktır.

Siber suçlar, bireylerin, kurumların ve toplumun güvenliğini, mahremiyetini, haklarını ve refahını tehdit edebilir. Bu nedenle, sosyal çalışmacıların,

siber suçlarla ilgili bilgi ve beceri düzeyini artırmaları gerekmektedir. Siber suçlarla ilgili bilgi ve beceri düzeyi, sosyal hizmet eğitiminde, mesleki gelişimde ve hizmet sunumunda artırılmalıdır. Sosyal hizmet eğitiminde, siber suçların tanımı, türleri, nedenleri, sonuçları ve önlenmesi gibi konulara yer verilmelidir. Sosyal hizmet öğrencileri, siber suçlara maruz kalan veya siber suç işleyen bireylerle nasıl çalışacaklarını öğrenmelidir. Sosyal hizmet öğrencileri, aynı zamanda siber güvenlik, siber etik, siber vatandaşlık gibi kavramlarla da tanıştırılmalıdır.

Kaynakça

Adli Destek ve Mağdur Hizmetleri Dairesi Başkanlığı. (2021). Mağdura Yaklaşım Kılavuzu. Ankara

Akince, Bora (2021). Nesnelerin İnterneti, Güvenlik ve Gizlilik, İnsan Hakları Bağlamında Bir Değerlendirme. **International Journal of Social Inquiry**. 14(1), 53-80.

Akkaya, Mehmet Ali (2021). Bilgi Kaynağı ve Bilgiye Erişim Aracı Olarak İnternet Algısı: Kuşaklararası Yaklaşım Farklılığının Karşılaştırılması. **Bilgi Yönetimi**. 4(2), 222-239.

Albayrak, Hande (2021). Eleştirel Sosyal Hizmet Teorisi ve Uygulaması. **Toplum ve Sosyal Hizmet**. 32(1), 383-401.

Altunok, Ebru ve Ali Fatih **Vural** (2011). Bilişim Suçları. **Denetişim.** (8), 74-84.

Arkan, Zeynep ve Serhat **İrez** (2021). Türkiye'de ve Dünyada Dezavantajlılık Sosyal İçerme Eğitim Programı. Ankara

Bacıoğlu, Seda Donat (2022). 21. Yüzyılda Çocukları ve Gençleri Bekleyen Siber Riskler. **Psikiyatride Güncel Yaklaşımlar**. 14(1), 29-37.

Bahar, Atalay (2018). Bilişim Suçları, İletişim ve Sosyal Medya. **İstanbul Aydın Üniversitesi Dergisi**. 10(3), 1-36.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. **Policing: An International Journal of Police Strategies & Management**. 29(3), 408-433.

Cobb, S. (2019). Advancing accurate and objective cybercrime metrics. **J. Nat'l Sec. L. & Pol'y**. 10, 605.

Connolly, L. Y. ve D. S. **Wall** (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. **Computers & Security**, 87, 101568.

Çakır, Hüseyin ve Murat **Taşer** (2023). Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi. **Gazi University Journal of Science Part C: Design and Technology**. 1-1.

Çalıcı, Can (2011). Sosyal ağlarda suç farkındalığı: Facebook örneği **(Yayımlanmamış Yüksek Lisans Tezi),** İstanbul Üniversitesi Sosyal Bilimler Anabilim Dalı.

Çaycı, Ayşegül Elif ve Berk **Çaycı** (2017). Dijital İletişim Çağında Teknolojinin Açığa Çıkardıkları: Gözetim ve Mahremiyet. **Turkish Online Journal of Design, Art & Communication. 7**(1).

Çelik, Mehmet Yunus (2012). Boyutları ve Farklı Algılarıyla Küreselleşme. **Dumlupınar Üniversitesi Sosyal Bilimler Dergisi.** (32).

Das, S. ve T. **Nayak** (2013). Impact of cybercrime: Issues and challenges. **International Journal of Engineering Sciences & Emerging Technologies**. 6(2), 142-153.

Derin, Görkem ve Erdinç **Öztürk** (2021). Klinik Adli Psikoloji: Klinik Psikoloji Temelli Adli Psikolojik Değerlendirme. **VII. TURKCESS Uluslararası Eğitim ve Sosyal Bilimler Kongresi**. 240-246

Doğan, Ahmet ve Furkan **Abacı** (2021). Türkiye'de Siber Terörizme Karşı Bilişim Teknolojilerinin Kullanımı. **OPUS International Journal of Society Researches**. 18(42), 5968-5998.

Dokgöz, Halis (2023), Siber Suçlar, Ankara:**Akademisyen Kitabevi**.

Force, R. T. (2021). Combating ransomware. Intel Security Group.

Güdek, Kemal (2016), Suçluluk ve suç davranışı adli sosyal çalışma, Ankara:**Nobel Tıp Kitabevi**.

Gündüz, Muhammed Zekeriya ve Resul **Daş** (2018). Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları. **Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi**. 24(2), 327-335.

Güngör, Murat (2015). Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapilanma. **TC Kalkınma Bakanlığı Bilgi Toplumu Daire Başkanlığı**. Yayın(2919).

Harris, Anita ve diğerleri (2022). Social Cohesion and Participation in a Digital Age for Diverse Young Australians. **Centre for Resilient and Inclusive Societies**. Deakin University.

Harmancı, Fatih M., **Gözübenli**, Murat ve Cevdet **Zengin** (2015). Güvenlik Sektöründe Temel Stratejiler, **Nobel Yayınevi**.

Holt, T. J. ve A. M. **Bossler** (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. **Taylor & Francis**.

IC3. (2018). FBI Internet Crime Report 2017.

IC3. (2023). FBI Internet Crime Report 2022.

ITU. (2023). Measuring digital development: Facts and Figures 2022.

Jebaseelan, U. S., ve **Fonceca**, C. M. (2021). Transdisciplinary Research: A social work perspective. **Int. J. of Aquatic Scienc**e, 12(2), 549-557.

Kaya, Mehmet ve Cahit **Aydemir** (2011). Küreselleşmenin Tarihsel Gelişimi. **Dicle Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi**. 1(1), 14-36.

Kıvılcım, Fulya (2013). Küreselleşme Kavramı ve Küreselleşme Sürecinin Gelişmekte Olan Ülke Türkiye Açısından Değerlendirilmesi. **Sosyal ve Beşeri Bilimler Dergisi**. 5(1), 219-230.

Küçükay, Alper (2019). Suç önleme stratejileri ve güvenlik politikalarına psikolojik bir bakış. **Türkiye Adalet Akademisi Dergisi**(38), 343-392.

Layton, E. T. (1974). Technology as knowledge. **Technology and culture**, 31-41.

Lim, J. W. ve V. L. **Thing** (2022). Towards Effective Cybercrime Intervention. **Cyber Security Strategic Technology Centre, ST Engineering.**

Loader, B. D. ve D. **Thomas**, (2013). Cybercrime: Law enforcement, security and surveillance in the information age. **Routledge**.

McQuade III, Samuel C. (2008). Encyclopedia of cybercrime, London: **Greenwood Press**.

Morgan, A. ve diğerleri (2016). Evaluation of the Australian cybercrime online reporting network.

Nicholas, L., **Rautenbach**, J. ve M. **Maistry** (2010). Introduction to social work. **Juta and Company Ltd**.

Özbay, Ahmet (2017). Sanal zorbalığa maruz kalan ergenlerin çözüm odaklı kısa süreli terapi yönelimli psikoeğitim programının psikolojik belirtiler ve sanal mağduriyete etkisi. Sakarya Üniversitesi Eğitim Bilimleri Anabilim Dalı.

Öztürk, Aslıhan Burcu, **Kayadibi**, Büşra ve Zeynep Dilruba **Taşdemir** (2021). Adli Destek ve Mağdur Hizmetleri Müdürlüğü Kapsamında Gerçekleştirilen Uygulamalara Yönelik Bir Değerlendirme. **Sosyal Hizmet "Social Work"**, 95.

Pina, A., **Storey**, J. E., **Duggan,** M. ve V. N. **Franqueira** (2021). Technology-Facilitated Intimate Partner Violence: A multidisciplinary examination of prevalence, methods used by perpetrators and the impact of COVID-19.

Sandilaç, Nurullah (2022). Siber Suç, Siber Terör ve Siber Savaş Üçgeninde Siber Dünya. **Bilişim Hukuku Dergisi**. 4(1), 81-140.

SonicWall. (2023). Cyber Threat Report.

Şamar, Berhudan (2018). Mağduriyet bağlamında adli sosyal hizmet ve adli görüşme odaları. **Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü**.

Şenel, Ahmet ve Serhat **Gençoğlu** (2003). Küreselleşen Dünyada Teknoloji Eğitimi. **Gazi Üniversitesi Endüstriyel Sanatlar Eğitim Fakültesi Dergisi**. 11(12), 45-65.

T.C. İçişleri Bakanlığı İç Güvenlik Stratejileri Dairesi Başkanlığı. (2020). Covid-19 Pandemisi Döneminde Siber Suç Riskleri ve Güvenliği Etkileri.

T.C. İçişleri Bakanlığı İç Güvenlik Stratejileri Dairesi Başkanlığı. (2021). Türkiye'de Siber Suçların Boyutu ve Güvenliğe Etkileri. Has Matbaacılık.

Tropina, T., **Callanan**, C. ve T. **Tropina** (2015). Public–private collaboration: Cybercrime, cybersecurity and national security. **Self-and co-regulation in Cybercrime, cybersecurity and national security**, 1-41.

UNICEF. (2022). Legislating For The Digital Age.

We Are Social. (2018). Digital 2017: Global Overview Report.

We Are Social. (2023). Digital 2022: Global Overview Report.

Yanarışık, Oğuzhan (2020), İç Güvenlik ve Siber Güvenlik, İç Güvenlik Yönetimi ve Polislik, (pp.303-327), Ankara:**Polis Akademisi Yayınları**.

Yıldırım, Arzu (2014). Sosyo-kültürel Yapı ve Suç Olgusu Arasındaki İlişki: Malatya İli Örneği. **Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi**. 2014(3), 1-7.

Yıldırım, Hüseyin (2019). Dördüncü Sanayi Devrimi'Nin Ulusal Güvenliğe Etkisinin Karşılaştırmalı Analizi. **Bursa Uludag University (Turkey)**.

Yılmaz, Onur (2017). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik**. Cyberpolitik Journal**. 2(4), 22-43.

Zengin, Oğuzhan ve Nurullah **Çalış** (2017). Sosyal Hizmet Uzmanlarinin Mesleki Uygulamalari ve Çalışma Koşulları. **Toplum ve Sosyal Hizmet**. 28(1), 47-68.

‖Beyan ve Açıklamalar/Disclosure Statements ‖

1. Bu çalışmanın yazarı, **Bilgi Dergisi**'nce beyan edilen araştırma ve yayın etiği ilkelerine uyduğunu beyan etmektedir (The author confirms that his work complies with the principles of research and publication ethics announced by **Bilgi**).
2. Yazar tarafından herhangi bir çıkar çatışması beyan edilmemiştir ve araştırmadan herhangi bir üçüncü şahıs/kurumun etkilenebileceğine dair bildirim bulunmamaktadır (No potential conflict of interest and the research's effects on any person/institution was reported by the author).
3. Makalenin tamamının Mehmet **Uysal** ve Muhammet Ali **Köroğlu** tarafından kaleme alınmış olduğu bildirilmiş ve ilave bir teşekkür konusu belirtilmemiştir (It was reported that the article was written by Mehmet Uysal and Muhammet Ali Köroğlu, as no additional ack-nowledgement has been made).

Extended Abstract

Social Work in the Fighting Cybercrimes

Mehmet Uysal & Muhammet Ali Köroğlu

Cybercrime is a growing threat to the global economy, security and human rights. It affects individuals, businesses, governments and society as a whole. Cybercrime can take many forms, such as online exploitation and abuse of children, darknet markets for illicit drugs and firearms, ransomware attacks, human trafficking using social media, identity theft, fraud, cyberterrorism and cyberwarfare. Cybercriminals often operate across borders, using sophisticated techniques and tools to evade detection and prosecution. The challenges posed by cybercrime require a comprehensive and coordinated response from various actors, including law enforcement, policymakers, civil society, academia and the private sector.
Social work is a profession that aims to promote social justice, human dignity and well-being. Social workers can play a viral role in the fighting cy-

bercrime, by providing support and protection to victims, raising awareness and education, advocating for policy and legal reforms, and collaborating with other stakeholders. Social workers can also help prevent cybercrime, by addressing the root causes and risk factors, such as poverty, inequality, marginalization, social exclusion, mental health issues, substance abuse and lack of digital literacy. Social workers can use their skills and values, such as empathy, respect, empowerment, critical thinking and ethical decision-making, to engage with diverse and vulnerable populations in cyberspace.

This article aims to explore the potential and challenges of social work in the fighting cybercrime. It will review the existing literature and evidence on the nature and impact of cybercrime, the current responses and gaps, and the role and contribution of social work. It will also propose a conceptual framework and a set of recommendations for enhancing the involvement and effectiveness of social work in this emerging field. The article will conclude by highlighting the need for further research, education and practice development on social work and cybercrime.