Adli Bilimler ve Suç Araştırmaları Dergisi

ISSN: 2687-3397 **E-ISSN:** 2791-8696
Cilt: 8, **Sayı:** 2026 **Makale Türü:** Araştırma
Makalenin Geliş Tarihi: 25.04.2025 **Makalenin Kabul Tarihi:** 07.04.2026

Siber Suçların Rutin Aktiviteler Teorisi ile Açıklanabilirliği Üzerine Değerlendirme

Zeynep Rüveyda Gökmen[*], *Vedat Yılmaz*[**]

Öz: Dijitalleşmenin hız kazandığı çağdaş toplumlarda, suçun doğası ve mekânsal gerçekleşme biçimleri radikal bir dönüşüme uğramıştır. Fiziksel dünyada gerçekleşen geleneksel suç türlerinin yanı sıra, siber uzayda meydana gelen yeni nesil suç biçimleri, kriminolojik teori ve uygulamaların yeniden değerlendirilmesini gerekli kılmaktadır. Bu çalışma, Rutin Aktiviteler Teorisi'nin (RAT) siber suçları açıklama potansiyelini kuramsal düzeyde değerlendirmeyi amaçlamaktadır. Geleneksel suçlara yönelik olarak geliştirilen RAT, suçun meydana gelmesini motive olmuş failin varlığı, uygun hedefin bulunması ve yeterli koruyucuların yokluğu unsurlarıyla açıklar. Çalışmada, bu üç unsurun siber suç bağlamında nasıl kavramsallaştırılabileceği ve dijital ortamdaki karşılıklarının neler olduğu incelenmiştir. Bulgular, RAT'in siber suçların analizinde belirli bir açıklama gücüne sahip olduğunu ancak dijital ortamın anonimliği, mekânsızlığı ve bireysel dijital alışkanlıkların rolü gibi özgün unsurlar karşısında yetersiz kalabildiğini göstermektedir. Bu bağlamda RAT'in dijital ortama tamamen uyarlanabilmesi için bireysel davranış örüntülerini de içeren daha geniş kapsamlı kuramsal yaklaşımlara ihtiyaç duyulduğu sonucuna varılmıştır.

Anahtar Kelimeler: Siber Suç, Rutin Aktiviteler Teorisi, Dijital Güvenlik, Kriminoloji, Suç Teorileri

[*] Zeynep Rüveyda GÖKMEN, Yüksek Lisans, Jandarma ve Sahil Güvenlik Akademisi, Adli Bilimler Enstitüsü, zeynepgokmen99@gmail.com, ORCID: 0009-0004-9579-4997
[**] Vedat YILMAZ, Dr., Jandarma ve Sahil Güvenlik Akademisi, Adli Bilimler Enstitüsü, vedat.yilmaz@jsga.edu.tr, ORCID: 0000-0002-3112-9371

Turkish Journal of Forensic Science and Crime Studies

ISSN: 2687-3397 **E-ISSN:** 2791-8696
Volume: 8, **Issue:** 2026 **Article Type:** Research
Received Date: 25.04.2025 **Accepted Date:** 07.04.2026

Evaluation of the Explanability of Cyber Crimes with Routine Activities Theory

Zeynep Rüveyda Gökmen[*], *Vedat Yılmaz*[**]

Abstract: In contemporary societies where digitalization is accelerating, the nature of crime and its spatial occurrence have undergone a radical transformation. In addition to traditional crime types that occur in the physical world, new generation crime types that occur in cyberspace necessitate the re-evaluation of criminological theory and practices. This study aims to evaluate the explanatory potential of the Routine Activity Theory (RAT) in the context of cybercrime from a theoretical perspective. Originally developed for analyzing conventional crimes, RAT explains criminal events through three key elements: the presence of a motivated offender, the availability of a suitable target, and the absence of capable guardians. This paper examines how these components can be conceptualized in digital environments and identifies their cyber equivalents. Findings indicate that while RAT provides a certain explanatory value in analyzing cybercrime, it falls short in addressing the unique characteristics of digital environments, such as anonymity, spatial detachment, and the role of individual online behaviors. Accordingly, the study concludes that fully adapting RAT to the cyber realm requires the integration of broader theoretical frameworks that incorporate behavioral and lifestyle factors.

Keywords: Cyber Crime, Routine Activities Theory, Digital Security, Criminology, Crime Theories

[*] Zeynep Rüveyda GÖKMEN, M.S., Gendarmerie and Coast Guard Academy, Forensic Sciences Institute, zeynepgokmen99@gmail.com, ORCID: 0009-0004-9579-4997
[**] Vedat YILMAZ, Ph.D, Gendarmerie and Coast Guard Academy, Forensic Sciences Institute, vedat.yilmaz@jsga.edu.tr, ORCID: 0000-0002-3112-9371

Giriş

Günümüzde suç olgusunun sınırları önemli ölçüde değişim göstermektedir. Suçun geleneksel olarak fiziksel ortamlarda gerçekleşmesi yerini, dijital platformlarda işlenen yeni suç biçimlerinin aldığı bir yapıya bırakması, çağdaş kriminoloji literatüründe önemli bir kırılma noktası oluşturmaktadır. Siber suçlar olarak tanımlanan bu suç türleri, bilgi ve iletişim teknolojilerinin hızlı gelişimi ve yaygınlaşmasıyla birlikte giderek daha karmaşık, teknik uzmanlık gerektiren ve sınır ötesi özellikler taşıyan eylemler biçiminde ortaya çıkmaktadır (Gordon & Ford, 2006; Başar, 2015). Bu suçlar, faillerin kimliklerini gizleyebilmeleri ve eylemlerini coğrafi sınırlamalara bağlı kalmadan gerçekleştirebilmeleri sayesinde geleneksel suç kategorilerinden önemli ölçüde ayrışmaktadır.

Siber suçlar yalnızca bireysel mağduriyetleri değil, aynı zamanda kurumsal güvenliği, kamu düzenini ve ulusal güvenliği de tehdit eden çok boyutlu bir risk alanı yaratmaktadır. Bilgi hırsızlığı, kimlik avı (phishing), kötü amaçlı yazılımlar, veri ihlalleri, fidye yazılımları, finansal dolandırıcılık, çevrim içi taciz, çocukların dijital ortamda istismarı gibi farklı formlarda karşımıza çıkan bu suç türleri hem mikro düzeyde bireysel kullanıcıları hem de makro düzeyde devlet kurumlarını ve uluslararası ilişkileri etkileyebilmektedir. Bu bağlamda siber suçlar; ekonomik kayıplara, gizliliğin ihlaline, hizmet kesintilerine, itibari zararlara ve hukuki yaptırımlara neden olabilmekte ayrıca ulusal güvenliğin zedelenmesine yol açacak sonuçlar doğurabilmektedir.

Söz konusu suç ortamının bu denli geniş ve etkili bir yapıya bürünmesi, kolluk kuvvetlerinin ve adli makamların suçla mücadele stratejilerini yeniden yapılandırmalarını zorunlu kılmaktadır. Bu bağlamda, siber suç fenomeninin doğasının çok yönlü olarak anlaşılması, etkili önleme ve müdahale mekanizmalarının oluşturulması açısından kritik bir öneme sahiptir. Kriminolojik perspektiften değerlendirildiğinde, dijital suçların analizi, yalnızca teknik önlemlerle sınırlı kalmayıp suç davranışının arkasında yatan yapısal ve çevresel etkenlerin anlaşılmasını da içermelidir.

Öte yandan, bilgi ve iletişim teknolojilerinde yaşanan hızlı artış, yalnızca bireysel çıkarları tehdit eden değil aynı zamanda siyasal ve kamusal alanlara yönelik ulusötesi suç biçimlerinin ortaya çıkmasına da imkân tanımıştır. Dijital ortamda üretilen suçlar artık yalnızca bireyler arası ilişkiler bağlamında değil, devletlerarası güvenlik ve diplomatik ilişkiler çerçevesinde de değerlendirilmek zorundadır (Ron vd., 2018). İnternetin küresel ölçekte erişilebilir hale gelmesi, çevrim içi işlemlerin artması ve bireylerin dijital sistemlerle olan ilişkilerinin yoğunlaşması, siber suçları çağdaş güvenlik sorunlarından biri haline getirmiştir (Gordon & Ford, 2006). Günümüzde bireyler sadece fiziksel varlıklarıyla değil, dijital kimlikleri, verileri ve çevrim içi faaliyetleri aracılığıyla da suç mağduru olabilmektedir.

Siber suçların artış göstermesi ve taşıdığı özelliklerin klasik suç formlarından belirgin biçimde ayrılması, geleneksel kriminolojik teorilerin bu suç türlerini açıklamada ne ölçüde yeterli olduğunu sorgulayan yeni bir kuramsal arayışları beraberinde getirmiştir. Uzun vadeli suç davranışlarını açıklamaya yönelik geliştirilen klasik teorilerin, dijital ortamlarda gerçekleşen suçları ne derece kapsayabildiği yeniden değerlendirilmelidir. Bu nedenle, siber suçlara dair kriminolojik yaklaşımların güncellenmesi ve teorik zeminlerinin çağın gereklilikleri doğrultusunda yeniden yapılandırılması gerekmektedir (Weulen Kranenbarg vd., 2021).

Klasik kriminolojik kuramlar, dijital teknolojilerin ve internetin yaşamın merkezine yerleşmesinden çok önce, bireylerin fiziksel ortamda suç davranışı sergilemesini açıklamaya yönelik teorik çerçeveler sunmuştur. Bu kuramlar, uzun yıllar boyunca çeşitli ampirik araştırmalarla desteklenmiş ve suç olgusunun birey temelli açıklamalarına önemli katkılar sağlamıştır. Bununla birlikte dijitalleşmenin hız kazandığı günümüzde, siber suçların giderek artan önemi, geleneksel kriminolojik yaklaşımların bireylerin sanal ortamda gerçekleştirdiği suçları açıklamada ne ölçüde yeterli olduğunu sorgulayan yeni bir araştırma alanını doğurmuştur (Stalans & Donner, 2018, s. 25).

Bu yeni suç ortamı, klasik kriminolojik teorilerin geçerliliğini ve uygulanabilirliğini yeniden tartışmaya açmıştır. Özellikle çevresel ve fırsat temelli yaklaşımlar, dijital suç alanında da kullanıma uygun açıklamalar sunabilmektedir. Bu teorilerden biri olan Rutin Aktiviteler Teorisi (Routine Activity Theory- RAT), suçun yalnızca bireysel motivasyonla değil, aynı zamanda sosyal çevrede oluşan fırsatlarla birlikte gerçekleştiğini öne sürmektedir. Rutin Aktiviteler Teorisi, başlangıçta geleneksel suç türlerini açıklamak üzere geliştirilmiş olsa da dijital çağın getirdiği yeni suç biçimleriyle birlikte yeniden yorumlanmaktadır. Bu çalışmada, RAT'nin dijital ortamdaki geçerliliği ve siber suçlara uygulanabilirliği değerlendirilecek ve teorinin temel kavramları dijital bağlamda ele alınarak tartışılacaktır.

Siber Suçlar

Bilgisayar ve internet teknolojilerinin gelişimi, yalnızca teknik bir ilerleme değil aynı zamanda insanlık tarihindeki toplumsal dönüşüm süreçlerini yeniden tanımlayan çok katmanlı bir değişim dalgası olarak değerlendirilmektedir. Bu teknolojiler, bireysel yaşam pratiklerinden küresel ekonomi ve sosyal örgütlenmelere kadar pek çok alanda radikal etkiler yaratarak, modern toplumun yapısal dinamiklerini dönüştürmüştür. Dijitalleşmenin gündelik yaşamın ayrılmaz bir parçasına dönüşmesiyle birlikte internetin yaygın kullanımı ve karmaşıklaşan yapısı, kötüye kullanım risklerini artırmış ve dijital mecralarda işlenen yeni suç türlerinin ortaya çıkmasına zemin hazırlamıştır. Bu bağlamda siber suçlar, dijital teknolojilerin öngörülen işlevlerinin dışında, yasa dışı amaçlarla kullanılması sonucu gelişen ve çağdaş toplumlarda ciddi güvenlik tehditleri oluşturan bir olgu olarak

literatürde yerini almıştır. Dijital ortmada işlenilen suçlar farklı terminolojik çerçevelerle tanımlansa da bu tür suçlar büyük ölçüde "siber suçlar" kavramı altında ele alınmaktadır (Kökkaya, 2022).

Dolayısıyla, bilgisayar ve internetin tarihsel gelişim süreci yalnızca teknolojik evrimi izlemek açısından değil, aynı zamanda siber suçlarla mücadeleye yönelik kuramsal ve pratik yaklaşımların kökenlerini anlamak açısından da önem arz etmektedir. Günümüzde tartışma konusu olan siber suç ve siber güvenlik kavramlarının doğru biçimde kavranabilmesi internetin doğasını ve işleyişini anlamakla başlamalıdır. Zira internet olmaksızın siber suçların varlığından söz etmek mümkün değildir.

İnternet, yalnızca siber suçların işlendiği dijital bir zemin sağlamakla sınırlı bir araç olarak değerlendirilmemelidir. Teknik bir altyapı ya da bireylerden bağımsız işleyen nötr bir platform olmanın ötesinde internet, çok boyutlu sosyal etkileşimlerin ve dijital uygulamaların gerçekleştiği dinamik bir ortam olarak ele alınmalıdır. Bu nedenle, bireylerin interneti hangi amaçlarla ve nasıl kullandığı, suç davranışlarını anlamada temel bir analiz kategorisi olarak kabul edilmelidir. İnternetin kullanım biçimleri, dijital alanın toplumsal işlevlerini doğrudan etkilemekte ve bu da belirli suç türlerinin ortaya çıkışına olanak tanımaktadır. Örneğin, çevrimiçi ticaretin gelişmesiyle birlikte, kullanıcıların finansal bilgilerini hedef alan kredi kartı dolandırıcılığı gibi suç türlerinin dijital ortamda meydana gelmesi mümkün hale gelmiştir (Yar & Steinmetz, 2019, s. 30). Bu çerçevede, internet ve onunla bağlantılı iletişim teknolojilerinin evrimi, yalnızca teknik değil, aynı zamanda toplumsal güvenlik, kamu düzeni, ekonomik istikrar ve bireysel hak ve özgürlükler açısından da çok boyutlu zorlukları beraberinde getirmiştir. Teknolojinin bu yönü, dijitalleşmenin suç ve kontrol mekanizmaları üzerindeki etkilerini anlamada merkezi bir öneme sahiptir (Yar & Steinmetz, 2019, s. 25-26).

İnternetin tarihsel kökeni, 1950'li yıllarda Amerika Birleşik Devletleri tarafından geliştirilen "Semi-Automatic Ground Environment" (SAGE) adlı sisteme dayanmaktadır. Bu sistem, özellikle II. Dünya Savaşı'nın ardından ortaya çıkan güvenlik tehditlerine karşı, düşman bombardıman uçaklarına yönelik erken uyarı ve müdahale mekanizması geliştirmek amacıyla tasarlanmıştır. 1962 yılına gelindiğinde ise, Massachusetts Institute of Technology (MIT) bünyesinde görev yapan J. C. R. Licklider tarafından ortaya atılan "Galaktik Ağ" (Galactic Network) kavramı, geniş çaplı bilgisayar ağlarının geliştirilmesine ilişkin teorik zemin oluşturmaya başlamıştır. Licklider, aynı yıl içinde ABD Savunma Bakanlığı'na bağlı olarak faaliyet gösteren ve stratejik araştırmaları destekleyen Advanced Research Projects Agency (ARPA) adlı kurumun başına getirilmiştir. Bu kurum daha sonra, güvenlik odaklı misyonunun vurgulanması amacıyla "Defense" (savunma) ifadesiyle yeniden adlandırılmış ve Defense Advanced Research Projects Agency (DARPA) adını almıştır (Kökkaya, 2022).

İnternetin bugünkü formuna evrilmesinde kritik bir kırılma noktası, 1990 yılında Amerika Birleşik Devletleri'nin ARPANET sistemini sivil kullanıma açmasıyla gerçekleşmiştir. Aynı dönemde, İsviçre'de faaliyet gösteren Avrupa Nükleer Araştırma Merkezi (CERN) bünyesindeki araştırmacılar, esasen bilgi paylaşımını kolaylaştırma amacıyla geliştirilen ilk web tarayıcısını oluşturmuştur. "World Wide Web (www)" olarak adlandırılan bu yazılım, kısa sürede çeşitli yazılımcıların katkılarıyla daha gelişmiş sürümlere evrilmiş ve yalnızca metinsel içerik değil, görsellerin de aktarılabildiği çok yönlü bir dijital iletişim aracı haline gelmiştir. Böylelikle internet, başlangıçta akademik ve askeri çevrelerle sınırlı bir yapıya sahipken, giderek geniş kitlelerin erişimine açılmış ve küresel ölçekte etkileşim ve bilgi paylaşımının önünü açan evrensel bir iletişim altyapısına dönüşmüştür (Yar & Steinmetz, 2019, s. 31–32; Kökkaya, 2022).

1990'lı yılların ortalarında internetin ticarileşmesi, küresel ölçekte hızlı ve kapsamlı bir büyüme sürecini tetiklemiştir (Neumüller, 2017). Bu dönemde, internete erişimi olan ülke sayısı 1994 yılında 83 iken, 1999 yılına gelindiğinde bu sayı 226'ya ulaşmıştır. Bu artış, dijital erişimin yalnızca belirli coğrafyalarla sınırlı kalmadığını, aksine dünya genelinde hızlı bir yaygınlaşma eğilimi sergilediğini göstermektedir. Aralık 1995 itibarıyla internet kullanıcılarının sayısı yaklaşık 16 milyon olarak tahmin edilirken, bu rakam 2002 yılının Mayıs ayında 580 milyonu aşmış ve dünya nüfusunun yaklaşık %10'una tekabül etmiştir. İnternetin benimsenme oranı sonraki yıllarda da istikrarlı bir artış göstermiş; Haziran 2017 itibarıyla toplam kullanıcı sayısı 3,89 milyara ulaşarak küresel nüfusun %51,7'sini kapsamıştır (Yar & Steinmetz, 2019, s. 32).

Bu ivme günümüzde de devam etmektedir. 2024 yılı verilerine göre, dünya genelinde internet kullanan birey sayısının yaklaşık 5,5 milyara ulaştığı tahmin edilmektedir. Bu rakam, bir önceki yılın 5,3 milyarlık kullanıcı sayısıyla karşılaştırıldığında artış eğiliminin sürdüğünü ve bu oranın küresel nüfusun %68'ine karşılık geldiğini ortaya koymaktadır. Bu istatistikler, internetin yaygınlaşma hızını ve dijital erişimin artık küresel ölçekte temel bir gerçeklik haline geldiğini açık biçimde yansıtmaktadır (Statista, 2024).

Bu hızlı yayılma ve dijitalleşme süreci, kriminoloji disiplininde yeni tartışma alanlarının oluşmasına neden olmuştur. Özellikle internetin sunduğu avantajlarla birlikte gelen olası kötüye kullanım biçimleri, güvenlik, mahremiyet ve toplumsal riskler açısından çok yönlü değerlendirmeleri gerekli kılmaktadır. Bu bağlamda, siber suçlar yalnızca teknik değil, aynı zamanda sosyolojik, psikolojik, hukuki ve normatif boyutlarıyla ele alınması gereken kompleks bir olgu olarak öne çıkmakta ve kriminolojik literatürde giderek daha fazla önem arz etmektedir.

Siber suçlar, ortaya çıktıkları ilk dönemlerde oldukça sınırlı ve basit yapılarla karakterize edilmekteydi. Bu dönemde suçlar, genellikle bilgisayar sistemlerine izinsiz erişim, veri sabotajı ya da yazılım manipülasyonu gibi teknik bilgiye dayalı ancak dar kapsamlı eylemlerle sınırlıydı. Ancak zaman içerisinde dijital teknolojilerin hızlı gelişimiyle birlikte, bu suç türleri yalnızca daha karmaşık hale

gelmekle kalmamış, aynı zamanda küresel ölçekte yaygınlaşan, süreklilik arz eden, ekonomik açıdan büyük maliyetler doğuran ve toplumsal güvenliği tehdit eden çok boyutlu bir olgular dizisine dönüşmüştür (Birceviz, 2019; Caravelli & Jones, 2019, s. 35).

Bilişim teknolojilerinin dinamik ve sürekli değişen doğası göz önüne alındığında, "siber suç" kavramına ilişkin açık, kesin ve evrensel bir tanım geliştirmek oldukça güçtür. Bu belirsizlik hem suç türlerinin çeşitliliğinden hem de dijital ortamlara yönelik saldırı yöntemlerinin sürekli değişim göstermesinden kaynaklanmaktadır. Siber suçların teorik olarak sınıflandırılmasına ilişkin çeşitli yaklaşımlar mevcut olmakla birlikte, literatürde en yaygın kabul gören ayrım, bu suçların siber bağımlı (cyber-dependent crimes) ve siber destekli (cyber-enabled crimes) olmak üzere iki temel kategoriye ayrılmasıdır. Siber bağımlı suçlar, yalnızca bilgisayar sistemleri, dijital ağlar veya bilgi ve iletişim teknolojileri kullanılarak işlenebilen, fiziksel dünyada bir karşılığı bulunmayan suçlardır. Siber destekli suçlar ise büyük ölçüde bilgi teknolojilerinin sunduğu imkânlara dayalı olarak ortaya çıkmış olup, teknolojik gelişmelere paralel şekilde sürekli olarak evrim geçirmektedir (Kranenbarg ve Leukfeld, 2021, s. 176). Bununla birlikte, bu çalışmada siber suçlara ilişkin değerlendirme dijital suç tipolojisinin günümüzde ulaştığı çeşitlilik dikkate alınarak, yalnızca iki ana kategoriyle sınırlandırılmamıştır.

Rutin Aktiviteler Teorisi

Rutin Aktiviteler Teorisi (Routine Activities Theory - RAT), suçun meydana gelmesini mümkün kılan yapısal ve çevresel koşullara odaklanan önemli bir çevresel kriminoloji yaklaşımıdır. Bu teori, özellikle modern ve kentleşmiş toplumlarda suçun mekânsal ve zamansal örüntülerini anlamlandırmak açısından güçlü bir analitik araç sunmaktadır.

20. yüzyılın ortalarına kadar kriminolojik yaklaşımlar genellikle birey merkezli olup, suç davranışını ya kalıtsal eğilimler ya da metafizik inanışlar ve bireysel rasyonalite çerçevesinde değerlendirmekteydi. Ancak İkinci Dünya Savaşı sonrasında yaşanan küresel sosyoekonomik dönüşümler ve bu sürece eşlik eden suç oranlarındaki artış, bu tür bireyselci açıklamaların sınırlılıklarını gün yüzüne çıkarmıştır. Bu gelişmeler, suçu açıklamada daha sistematik ve yapısal etkenleri dikkate alan bütüncül teorik yaklaşımlara olan gereksinimi ortaya koymuştur (Birceviz, 2019).

Bu bağlamda, Lawrence E. Cohen ve Marcus Felson tarafından 1979 yılında kaleme alınan "Social Change and Crime Rate Trends: A Routine Activity Approach" başlıklı makale, RAT'nin teorik temelini oluşturmaktadır. Yazarlar, İkinci Dünya Savaşı sonrasındaki dönemde meydana gelen önemli toplumsal değişimlerin –örneğin iş gücüne katılım oranlarının yükselmesi, kent dışı yerleşimlerin (banliyölerin) yaygınlaşması ve tüketim toplumunun gelişimi– bireylerin günlük

yaşam rutinlerini değiştirdiğini ve bu değişimlerin suç işleme fırsatlarını artırdığını ileri sürmüşlerdir (Hagan, 2017, s. 222–225; Schmalleger, 2017, s. 262; Siegel, 2019, s. 82).

Rutin Aktiviteler Teorisi'ne göre, bireylerin günlük yaşam kalıpları ile mağduriyet riski arasında doğrudan bir bağ bulunmaktadır. İnsan davranışları büyük ölçüde tekrar eden örüntülerden oluşur ve bu düzenlilik, bireylerin hangi zaman ve mekânda bulunabileceklerinin öngörülmesini mümkün kılar. Bireyler, yaşamlarını kolaylaştırmak adına belirli rutinler geliştirir, örneğin işe giderken sabit bir güzergâh kullanmak ya da eve dönerken aynı alışveriş noktasında durmak gibi. Bu rutinler bir yandan kolaylık sağlarken, öte yandan öngörülebilirlik düzeyini artırarak mağduriyet riskini de beraberinde getirebilir (Delice, 2021).

Benzer şekilde, suç işlemeye eğilimli bireyler de çevrelerindeki dinamikleri tanıdıkça, potansiyel hedefleri daha kolay belirleyebilmekte ve eylem sonrasında kaçış planlarını daha etkili şekilde organize edebilmektedirler. Bu bağlamda, RAT suçu bireylerden çok, bireylerin içinde bulundukları sosyal yapı ve mekânsal bağlam üzerinden anlamlandıran bir perspektif sunmaktadır (Delice, 2021).

Rutin Aktiviteler Teorisi'nin temel varsayımı, bir suçun gerçekleşmesi için üç unsurun aynı anda ve aynı mekânda bir araya gelmesi gerektiğidir: (1) suç işlemeye motive olmuş bir fail, (2) uygun bir hedef ve (3) caydırıcı unsurların eksikliği (Birceviz, 2019). Teorinin temel bileşenleri aşağıda ayrıntılı biçimde ele alınmıştır:

> Motive Olmuş Bir Fail: RAT, faillerin neden suç işlediğini açıklamak yerine, potansiyel suç faillerinin her zaman toplumda mevcut olduğunu ve önemli olanın bu bireylerin suç işlemesine olanak tanıyan ortamlar olduğunu varsayar (Siegel, 2019, s. 82–84; Lanier & Henry, 2009, s. 80–82).
>
> Uygun Bir Hedef: Hedefler bir birey, bir nesne ya da dijital bir varlık olabilir. Uygunluk derecesi ise hedefin maddi ya da sembolik değeri, taşınabilirliği, görünürlüğü ve kolay erişilebilirliği gibi özelliklere bağlıdır. Örneğin, küçük, taşınabilir ve değerli bir nesne olan cep telefonları, büyük ve sabit bir televizyona kıyasla daha cazip hedeflerdir (Schmalleger, 2017, s. 262–265).
>
> Caydırıcı Unsurların Eksikliği: Suçun gerçekleşmesini engelleyebilecek unsurlar arasında bireyler (örneğin polis, komşular) ya da teknolojik araçlar (örneğin güvenlik kameraları, alarm sistemleri) yer alır. Bu unsurların varlığı suç üzerinde caydırıcı bir etki yaratırken, yoklukları suç ihtimalini artırmaktadır (Hagan, 2017, s. 222–225).

Teoriye göre, bu üç unsurun aynı anda varlık göstermesi suçun meydana gelme ihtimalini artırırken, herhangi birinin eksikliği, suçu engelleyici bir rol oy-

namaktadır (Hagan, 2017; Schmalleger, 2017; Siegel, 2019). Bununla birlikte, hedeflerin suç açısından ne derece elverişli olduğu; onların değer düzeyi, fiziksel olarak görünür olup olmaması, ulaşılabilirlik derecesi ve hukuka aykırı müdahalelere karşı direnç düzeyi gibi çeşitli değişkenlere bağlıdır. Öte yandan caydırıcı unsurlar yalnızca kurumsal güvenlik önlemlerini değil, aynı zamanda toplumsal alanın doğal gözetim mekanizmalarını da kapsamaktadır. Bu üç unsurun belirli bir zaman ve mekânda kesişimi, bireylerin tekrar eden rutin faaliyetlerinin oluşturduğu yapısal suç fırsatları ile doğrudan ilişkilidir.

Nitekim potansiyel mağdurların suça eğilimli bireylerle daha sık kesişmesi ya da hedeflerin görünürlüğünün artması gibi toplumsal düzeydeki değişkenler, suç fırsatlarının çoğalmasında etkili olmaktadır. Buna karşılık, koruyucu önlemlerin zayıf olduğu sosyal çevrelerde suçun gerçekleşme olasılığı da artış göstermektedir. Bu nedenle, RAT'ye dayalı ampirik çalışmalar çoğunlukla coğrafi bilgi sistemleri ve suç haritalama teknikleri kullanarak, suçun yüksek yoğunlukta meydana geldiği "sıcak noktaları" belirlemeyi hedefler. Bu teknikler, suçun mekânsal örüntüsünü analiz etmek açısından önemli bir analitik katkı sunmaktadır (Lanier & Henry, 2009, s. 82; Schmalleger, 2017, s. 262–265).

RAT aynı zamanda, durumsal suç önleme stratejilerinin teorik temelini oluşturan güçlü bir yaklaşımdır (Akdemir & Yenal, 2020). Kamusal alanların daha iyi aydınlatılması, gözetim sistemlerinin kurulması ya da mahalle dayanışmasının teşvik edilmesi gibi stratejiler, suç fırsatlarını azaltmayı amaçlayan uygulamalar arasında yer almaktadır (Hagan, 2017, s. 222–225). Bu bağlamda RAT, yalnızca suçun nedenlerini anlamakla kalmaz, aynı zamanda etkili suç önleme politikalarının geliştirilmesine de katkı sunar.

Tüm bu yönleriyle RAT, suçun oluşumuna zemin hazırlayan çevresel ve fırsat temelli koşulları açıklamada önemli katkılar sunmaktadır. Nitekim dijital ortamda da bireylerin günlük rutinlerinin değişmesi, hedeflerin somut nesneler yerine veri ve sistem gibi soyut varlıklara dönüşmesi ve geleneksel koruyucuların yerini teknolojik önlemlerin alması gibi dinamikler, RAT'in temel unsurlarının dijital bağlama kısmen uyarlanabileceğini göstermektedir. Ancak bu uyarlanabilirlik, teoriye sınırsız bir geçerlilik atfetmek anlamına gelmemektedir. Zira siber suç ortamlarında zaman, mekân ve gözlemlenebilirlik gibi geleneksel suç ortamlarının belirleyici değişkenleri büyük ölçüde anlamını yitirmekte ve faillerin anonimliği, hedeflerin soyutlaşması ve koruyucu unsurların teknikleşmesi gibi etkenler, suçun doğasını temelden dönüştürmektedir. Bu nedenle RAT, siber suçlara uygulanabilirliğini korusa da açıklayıcılık gücünün sınırlandığı durumlar göz önünde bulundurulmalıdır. Bu bağlamda çalışmanın devamında, RAT'nin dijital ortama ne ölçüde uyarlanabileceği sorusu, teori bileşenleri ekseninde değerlendirilerek tartışılacaktır.

RAT'nin Siber Ortama Uyarlanabilirliği

Rutin Aktiviteler Teorisi, geleneksel suç türlerinin -örneğin hırsızlık, cinayet, otomobil hırsızlığı ve aile içi şiddet- analizinde uzun süredir kullanılan, kuramsal olarak sağlam ve uygulamada etkili bir çerçeve sunmaktadır. Teorinin sunduğu sistematik yaklaşım, suçun meydana gelme koşullarını açıklamakla kalmaz, aynı zamanda suçun önlenmesine yönelik stratejik politika üretimini de mümkün kılar. RAT temelli durumsal suç önleme yaklaşımları, bireylerin gündelik yaşam rutinlerindeki güvenlik açıklarını hedef alarak suç fırsatlarını en aza indirmeyi amaçlamaktadır.

Günümüzde RAT'nin dijital çağ bağlamında geçerliliğini sürdürüp sürdüremeyeceği yönündeki tartışmalar, özellikle siber suçlar özelinde önemli bir akademik ilgi alanına dönüşmüştür. Bu doğrultuda, erken dönem çalışmalar RAT'nin sanal ortama ne ölçüde uyarlanabileceğini sorgulamış, fiziksel ve dijital ortamlar arasındaki yapısal farklılıklar ile benzerlikler analiz edilmiştir (Leukfeldt & Yar, 2016).

Fiziksel mekâna dayalı geleneksel suç kuramlarında merkezi önemde olan "mekânsal yakınlık" kavramı, dijital ortamlarda ağ bağlantıları üzerinden yeniden tanımlanmakta, suçun gerçekleştiği zaman ve yerin kavramsal sınırları, sanal mekânın maddi olmayan ve dağınık doğası nedeniyle dönüşüme uğramaktadır. Bu dönüşüm, RAT'nin temel bileşenleri olan motive olmuş bir fail, uygun hedef ve etkin koruyucunun yokluğu unsurlarının dijital ortamda yeniden kavramsallaştırılmasını zorunlu kılmaktadır.

Siber suçların doğası gereği, fail ve mağdurun aynı fiziksel mekânda bulunması gerekmemektedir. Aksine, dijital iletişim teknolojileri ve çevrimiçi ağlar sayesinde bu etkileşim uzaktan ve zaman farkı olmaksızın gerçekleşebilir hale gelmiştir. Dahası, yeterli düzeyde siber koruma önlemleri –örneğin güvenlik duvarları, çok faktörlü kimlik doğrulama, antivirüs yazılımları veya kötü amaçlı yazılımların tespit sistemleri– bulunmadığında, faillerin hedeflerine ulaşma olasılığı önemli ölçüde artmaktadır (Stalans & Donner, 2018, s. 29).

Yar (2005), RAT'nin üç temel unsurunun dijital bağlamda nasıl işleve kavuştuğunu açıklayarak, teorinin siber suçlara ne ölçüde uyarlanabileceğini sistematik biçimde ortaya koymuştur (Yar, 2005). Fiziksel dünyada suçun önlenmesinde güvenlik görevlileri, polis ya da mahalle gözetimi gibi aktörler rol oynarken; dijital dünyada bu rolü sistem yöneticileri, içerik denetleyicileri, platformların uyguladığı güvenlik politikaları ve teknolojik altyapılar üstlenmektedir. Özellikle çok faktörlü kimlik doğrulama, şifreleme sistemleri, yapay zekâ destekli tehdit tespit araçları ve düzenli olarak güncellenen yazılım yamaları, siber uzaydaki koruyucu unsurlar arasında yer almaktadır.

Bu çalışma özelinde RAT'nin siber suçlara uygulanabilirliği değerlendirildiğinde, teorinin üç temel unsurunun dijital ortama teorik olarak aktarılabilse de bu unsurların siber çerçevedeki karşılıklarının kavramsal ve pratik düzeyde çeşitli

sınırlılıkları olduğu görülmektedir (Siegel, 2019; Lanier & Henry, 2009; Hagan, 2017; Schmalleger, 2017) :

Motive Olmuş Fail: RAT, suçu açıklarken failin varlığını başlangıç koşulu olarak kabul eder. Ancak failin neden suç işlediğine dair açıklamalar sunmaz. Siber suçlarda failin motivasyonları oldukça çeşitlidir. Finansal kazanç elde etme arzusu, politik ya da ideolojik hedefler doğrultusunda hacktivist faaliyetler yürütme, teknik becerilerini kanıtlama isteği ya da dijital anonimlik üzerinden güç kazanma gibi motivasyonlar ön plana çıkmaktadır. Ayrıca, kripto paraların takibinin zorlaşması, dark web pazarlarının gelişmesi gibi yapısal dinamikler, faillerin eyleme geçmesini teşvik eden önemli unsurlar arasında yer almaktadır. Bu çeşitlilik, RAT'nin sabit fail tanımının ötesine geçilmesi gerektiğini ve siber faillerin psikososyal arka planlarını açıklayabilecek daha kapsamlı yaklaşımlara ihtiyaç duyulduğunu göstermektedir.

Uygun Hedef: Siber ortamlarda hedefler, fiziksel suçlara kıyasla çok daha çeşitlidir ve daha kolay tespit edilebilir durumdadır. Kişisel veriler, banka bilgileri, sistem açıklıkları, kamuya açık ağlar veya zayıf şifreleme sistemlerine sahip cihazlar potansiyel hedefler arasında yer almaktadır. Fakat fiziksel suçlarda gözlemlenebilir ve nesnel niteliklere sahip olan hedefler, dijital ortamda daha soyut bir yapı kazanmakta ve sürekli değişen niteliği deolayısıyla RAT'nin hedef uygunluğu kavramı, bu değişken dinamikleri açıklamakta sınırlı kalabilmektedir.

Caydırıcı Unsurların Eksikliği: RAT'nin üçüncü unsuru olan caydırıcı unsurların eksikliği, suçun gerçekleşme olasılığını doğrudan etkileyen faktörlerden biridir. Fiziksel çevrede bu unsurlar güvenlik kameraları, polis devriyeleri ve toplumsal gözetim iken, siber dünyada karşılığı dijital güvenlik teknolojileri olabilmektedir. Etkili dijital caydırıcılar arasında çok faktörlü kimlik doğrulama, saldırı tespit sistemleri, şifreleme teknolojileri, kullanıcı güvenlik eğitimi ve düzenli yazılım güncellemeleri sayılabilir. Bu önlemlerin yetersizliğinin yalnızca var olması değil, aynı zamanda saldırgan tarafından fark edilip kullanılabilir bulunması da suçun gerçekleşme olasılığını artırmaktadır. RAT, caydırıcı unsurların eksikliğinin suçun oluşumuna zemin hazırladığını öngörmektedir ancak bu eksikliklerin saldırgan tarafından keşfedilmesi süreci, RAT'ın doğrudan açıklama kapasitesini aşabilen bir boyut taşımaktadır. Zira, RAT daha çok suçun gerçekleştiği bağlamda koruyucu unsurların mevcudiyetini veya yokluğunu açıklamaya odaklanırken, siber suç bağlamında saldırganın güvenlik

açıklarını tespit etme ve değerlendirme süreci, teorinin kapsamını zorlayan ek bir aşama olarak ortaya çıkmaktadır. Bu nedenle, dijital ortamda caydırıcı önlemlerin zayıflığı RAT çerçevesinde kısmen açıklanabilirken, söz konusu zafiyetlerin saldırgan tarafından keşfedilmesi, teorinin açıklama gücünü sınırlandıran bir durum oluşturmaktadır.

Bu değerlendirmeler doğrultusunda, RAT'nin dijital suç ortamına belirli ölçüde uyarlanabilir olduğu ancak siber suçların karmaşık yapısı ve değişken doğası göz önünde bulundurulduğunda, teoriye bazı kuramsal ve pratik sınırlamaların eşlik ettiği açıkça görülmektedir. Bu nedenle, RAT'nin siber suç bağlamındaki açıklayıcılığı belirli alanlarda değerli olmakla birlikte, siber suçların kapsamlı analizinde destekleyici teorilerle tamamlanması ya da dijital ortama özgü yeni teorik yaklaşımların geliştirilmesi gerekmektedir.

Sonuç ve Değerlendirme

Dijital teknolojilerin toplumsal yaşamın her alanına nüfuz etmesiyle birlikte suçun doğası, mahiyeti ve gerçekleşme biçimleri köklü bir dönüşüme uğramıştır. Suçun mekânsal ve zamansal sınırları yeniden tanımlanmış; fiziksel ortama özgü eylemler, yerini siber uzayda gerçekleşen, görünmez, sınırsız ve çok katmanlı suç biçimlerine bırakmıştır. Bu yeni gerçeklik, klasik kriminolojik teorilerin geçerliliğini sorgulayan ve yeniden değerlendiren eleştirel bir literatürün oluşmasına zemin hazırlamıştır. Bu bağlamda, mevcut çalışma Rutin Aktiviteler Teorisi'nin siber suçları açıklamada ne oranda yeterli olduğunu değerlendirmektedir.

Rutin Aktiviteler Teorisi, suçun meydana gelmesini bireysel motivasyon ya da psikolojik eğilimlerden ziyade çevresel fırsat yapıları ve sosyal bağlamın sunduğu koşullarla açıklamayı amaçlayan çevresel bir yaklaşımdır (Cohen & Felson, 1979). Geleneksel suçlarda bu modelin üç temel unsuru suçun ortaya çıkmasında belirleyici etkenler olarak kabul edilmektedir. Bu yapı, fiziksel mekânın ve sosyal etkileşimin ön planda olduğu suç türlerinin analizinde yüksek derecede açıklayıcılık sağlamaktadır. Ancak dijital teknolojilerin suç ortamına girmesiyle birlikte, RAT'in klasik öncüllerinin bu yeni ortama ne ölçüde uyarlanabileceği sorusu gündeme gelmiştir.

Nitekim siber suçlar, mekândan ve zamandan bağımsız olarak, anonim kimlikler aracılığıyla ve çoğu zaman fiziksel temas olmaksızın işlenmektedir. Bu durum, RAT'in dayandığı mekânsal yakınlık, doğrudan gözlem ve fiziksel etkileşim gibi kavramların dijital ortamlarda karşılık bulmasını zorlaştırmaktadır. Failler, coğrafi olarak uzak mesafelerden çevrim içi sistemlere erişebilmekte, mağdurlar ise hedef haline gelmek için belirli bir fiziksel ortamda bulunmak zorunda kalmamaktadır. Dolayısıyla, RAT'in geleneksel suçlara uygulandığı biçimiyle doğrudan dijital ortama aktarılması, açıklayıcılık gücünü sınırlandırmaktadır (Yar & Steinmetz, 2019).

Öte yandan, RAT'in temel bileşenlerinin dijital suç ortamında kısmen de olsa karşılık bulduğu bazı dinamikler mevcuttur. Örneğin, "uygun hedef" kavramı, dijital bağlamda kişisel veriler, finansal bilgiler, sistem şifreleri, sosyal medya hesapları gibi soyut ancak yüksek değere sahip dijital varlıklar üzerinden yeniden tanımlanabilmektedir. Bu tür dijital hedeflerin erişilebilirliği, görünürlüğü ve korunma düzeyi, tıpkı fiziksel varlıklar gibi faillerin tercihlerini etkilemektedir (Holt & Bossler, 2015). Benzer şekilde, "yeterli koruyucuların eksikliği" unsuru da dijital ortamda antivirüs yazılımları, güvenlik duvarları, iki faktörlü kimlik doğrulama sistemleri ve bireysel dijital farkındalık gibi önlemlerle temsil edilmektedir. Ancak bu tür teknolojik koruyucular, fiziksel ortamdaki bekçi veya kamera gibi somut caydırıcılarla karşılaştırıldığında hem görünürlük hem de etkileşim bakımından daha soyut kalmaktadır (Ngo & Paternoster, 2011).

Bu noktada, RAT'in dijital ortama uyarlanmasında esas sorun yalnızca yapısal değil, aynı zamanda kuramsaldır. Zira RAT, bireylerin çevrim içi yaşam tarzları, dijital alışkanlıkları ve sosyal medya etkileşimleri gibi bireysel davranış kalıplarını yeterince analiz etmemektedir. Oysa siber suçların birçoğu, mağdurun çevrim içi görünürlüğü, dijital güvenlik bilgi düzeyi ve maruz kaldığı sosyal ağlar gibi değişkenlere doğrudan bağlıdır. Bu nedenle RAT, dijital suçları açıklamada belirli ölçüde katkı sunsa da bireysel düzeydeki davranışsal faktörleri dışarıda bırakması nedeniyle kavramsal olarak eksik kalabilmektedir (Vakhitova vd., 2019).

Bu bağlamda RAT'in dijital suçlara uygulanabilirliği yalnızca teorinin potansiyelini değil, aynı zamanda sınırlılıklarını da içeren çok boyutlu bir değerlendirmeyi gerekli kılmaktadır. Dijital ortamdaki suç biçimleri RAT'in klasik yapısıyla tam olarak örtüşmese de teoriye yapılacak kavramsal uyarlamalarla çevresel koşullar ve suç fırsatları arasındaki ilişki belirli ölçülerde açıklanabilir hâle gelebileceği düşünülmektedir. Ancak bu noktada, RAT'in siber suçların özgün yapısını anlamada ne ölçüde yetersiz kaldığını ve bu boşluğun hangi yeni kuramsal yaklaşımlarla giderilebileceğini irdeleyen daha kapsamlı teorik çerçevelerin geliştirilmesi önemli bir gereklilik olarak ortaya çıkmaktadır.

Sonuç olarak, Rutin Aktiviteler Teorisi geleneksel suçların analizinde uzun yıllardır etkili biçimde kullanılan bir çerçeve sunmaktadır. Ancak dijital teknolojilerin suç yapısını köklü biçimde dönüştürmesi, bu teorinin siber suçlara ne ölçüde uyarlanabileceğini tartışmalı hâle getirmiştir. Dijital ortamda suçun mekânı, zamanı, faili ve hedefi geleneksel suçlardan oldukça farklıdır. Bu da RAT'in temel unsurlarının dijital bağlamda sınırlı bir açıklama gücüne sahip olmasına neden olmaktadır. Teorinin bazı bileşenleri dijital ortama uyarlanabilse de bireylerin çevrim içi davranışları, dijital alışkanlıkları ve maruz kalma biçimleri gibi önemli faktörler yeterince dikkate alınmamaktadır. Bu nedenle, RAT siber suçların açıklanmasında belli ölçüde katkı sunsa da dijital suçların özgün yönlerini anlayabilmek için yeni veya tamamlayıcı kuramsal yaklaşımlara ihtiyaç duyulmaktadır. Bu çalışma, RAT'in siber suçlara uygulanabilirliğini değerlendirerek, bu alanda daha kapsayıcı teorik çerçevelerin geliştirilmesi gerektiğine işaret etmektedir.

Kaynakça

Akdemir, N., & Yenal, S. (2021). How phishers exploit the coronavirus pandemic: A content analysis of COVID-19 themed phishing emails. *SAGE Open, 11*(3). https://doi.org/10.1177/21582440211031879

Altun, A. (2022). Siber suçların kriminolojik analizi. *Journal of Social, Humanities and Administrative Sciences*, 8(48), 91–99. https://doi.org/10.31589/JOSHAS.884

Başar, Y. (2015). *Siber suç soruşturmalarında adli bilişim incelemeleri* [Yüksek lisans tezi, Afyon Kocatepe Üniversitesi]. Ulusal Tez Merkezi.

Birceviz, F. (2019). *Rutin aktiviteler teorisi bağlamında siber suç mağduriyetinin incelenmesi* [Yüksek lisans tezi, Milli Savunma Üniversitesi]. Ulusal Tez Merkezi.

Caravelli, J., & Jones, N. (2019). *Cyber security: Threats and responses for government and business*. Praeger.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588-608. http://dx.doi.org/10.2307/2094589

Delice, M. (2021). Evden hırsızlık suçuna etki eden faktörlerin rutin aktiviteler teorisi perspektifinden incelenmesi. *Academic Social Resources Journal*, 6(25), 896–909. https://doi.org/10.31569/ASRJOURNAL.228

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hagan, F. E. (2017). *Introduction to criminology: Theories, methods, and criminal behavior* (9th ed.). SAGE Publications.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensics: An introduction* (2nd ed.). Routledge.

Jahankhani, H. (Ed.). (2018). *Cyber criminology*. Springer.

Kökkaya, F. (2022). *Siber suçlarla mücadelede Türkiye-Avrupa Birliği arasındaki işbirliği* [Yüksek lisans tezi, Fırat Üniversitesi]. Ulusal Tez Merkezi.

Lanier, M. M., & Henry, S. (2009). *Essential criminology* (3rd ed.). Westview Press.

Leukfeldt, R., & Yar, M. (2015). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Neumüller, A. S. (2017). *Cybercrime centres: Analysis and recommendations based on research and case study of police cybercrime centres in Ireland and Austria* [Yüksek lisans tezi, University College Dublin].

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

Ron, M., Fuertes, W., Bonilla, M., Toulkeridis, T., & Díaz, J. (2018). Cybercrime in Ecuador, an exploration, which allows to define national cybersecurity policies. *Proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS 2018*), 27–40.

Schmalleger, F. (2017). *Criminology today: An integrative introduction* (8th ed.). Pearson.

Shaw, C. R., & McKay, H. D. (1969). *Juvenile delinquency and urban areas*. University of Chicago Press.

Siegel, L. J. (2019). *Criminology: The core* (7th ed.). Cengage Learning.

Statista. (2024). *Internet usage worldwide- statistics & facts*. https://www.statista.com/topics/1145/internet-usage-worldwide/

Stalans, L. J., & Donner, C. M. (2018). Explaining why cybercrime occurs: Criminological and psychological theories. In H. Jahankhani (Ed.), *Cyber criminology: Advanced sciences and technologies for security applications* (pp. 25–45).

Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M. K., & Webster, J. L. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior*, 101, 225–237. https://doi.org/10.1016/j.chb.2019.07.012

Weulen Kranenbarg, M., & Leukfeldt, R. (Eds.). (2021). *Cybercrime in context: The human factor in victimization, offending, and policing*. Springer.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427. https://doi.org/10.1177%2F147737080556056

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications.