Ekonomi, İşletme ve Bilişim Dergisi
Journal of Economics, Business and Information

ISSN: 3062-2425 Cilt/Vol. 3, Sayı/No. 1, 1-20, 2026.

Türkiye'de Bilgi Güvenliği Ekosisteminin Dönüşümü: 2015–2025 Döneminde Öne Çıkan Siber Tehditler ve Alınan Önlemler

Sinan Yeğen[1], Erdal Özdoğan[2], Mehmet Cıranoğlu[3]

Makale Hakkında

Gönderim Tarihi
6 Mayıs 2026
Kabul Tarihi
29 Haziran 2026
Makale Türü

Tarama Makalesi

Özet

Dijital teknolojilerin yaygınlaşmasıyla birlikte bilgi güvenliği, teknik bir süreç olmaktan çıkıp hem kurumların hem de devletlerin sürdürülebilirliği için stratejik bir unsur haline gelmiştir. 2015–2025 yılları arasında Türkiye'deki bilgi güvenliği alanında yaşanan dönüşümü ele alan bu çalışma, bilgi güvenliği kapsamında ortaya çıkan tehditlerin nasıl gelişim gösterdiğini ve bu tehditlere karşı geliştirilen önlemleri analiz etmektedir. Nitel araştırma yöntemlerinden literatür taraması tekniği kullanılarak yapılan analizde süreç, "Farkındalık ve Kurumsal Yapılanma", "Kritik Altyapı Güvenliği" ve "Dirençlilik ve Denetim" olmak üzere üç ana kırılma dönemi altında değerlendirilmiştir. Bulgular, fidye yazılımları ve DDoS saldırılarının yıllara göre artış göstererek hibrit tehditlere dönüştüğünü, buna karşılık savunma mekanizmalarının sadece teknik yatırımlarla sınırlı kalamayacağını ortaya koymaktadır. Çalışma sonucunda, tepkisel savunma anlayışının yerine, Sıfır Güven mimarisi, zorunlu siber güvenlik denetimleri ve insan faktörünün eğitimini merkeze alan önleyici ve bütüncül bir yönetim modeline geçişin zorunlu olduğu tespit edilmiştir.

Anahtar Kelimeler: Bilgi Güvenliği, Siber Güvenlik, Kritik Altyapılar, Siber Tehditler, Siber Dirençlilik, Sıfır Güven

Transformation of the Information Security Ecosystem in Türkiye: Prominent Cyber Threats and Measures Taken During the 2015-2025 Period

Article Info

Received
May 06, 2026
Accepted
June 29, 2026
Article Type
Review Article

Abstract

With the widespread adoption of digital technologies, information security has evolved from a purely technical process into a strategic element for the sustainability of both institutions and governments. This study, which examines the transformation in information security in Turkey between 2015 and 2025, analyzes how threats within the scope of information security have evolved and the measures developed against these threats. Using a qualitative research method, specifically a literature review, the analysis evaluates the process under three main turning points: "Awareness and Institutional Structuring," "Critical Infrastructure Security," and "Resilience and Control." The findings reveal that ransomware and DDoS attacks have increased over the years, transforming into hybrid threats; however, defense mechanisms cannot be limited solely to technical investments. The study concludes that a shift from a reactive defense approach to a proactive and holistic management model centered on Zero Trust architecture, mandatory cybersecurity audits, and human factor training is essential.

Keywords: Information security, cyber security, critical infrastructures, cyber threats, cyber resilience, zero-trust

1 Şef, Bursa Uludağ Üniversitesi, İnegöl İşletme Fakültesi sinanyegen@uludag.edu.tr. (Sorumlu Yazar)
2 Doçent Doktor, Bursa Uludağ Üniversitesi, İnegöl İşletme Fakültesi, Yönetim Bilişim Sistemleri Bölümü, erdalozdogan@uludag.edu.tr https://orcid.org/ 0000-0002-3339-0493
3 Doçent Doktor, Bursa Uludağ Üniversitesi, İnegöl İşletme Fakültesi, İşletme Bölümü ciranoglu@uludag.edu.tr https://orcid.org/ 0000-0002-7798-7099

Atıf: Yeğen, A., Özdoğan, E., ve Cıranoğlu, M. (2026). Türkiye'de Bilgi Güvenliği Ekosisteminin Dönüşümü: 2015–2025 Döneminde Öne Çıkan Siber Tehditler ve Alınan Önlemler. *Ekonomi, İşletme ve Bilişim Dergisi*, *3*(1), 1-20.

1. Giriş

Bilgi, çağımızda hem bireylerin günlük yaşamını sürdürebilmesi hem de kurumların işleyişi için vazgeçilmez bir stratejik kaynak haline gelmiştir. Dijital teknolojilerin hızla gelişmesiyle birlikte bankacılık, sağlık ve kamu hizmetleri gibi kritik altyapıların sanal ortama geçişi, toplumsal yapıyı kökten değiştirerek bilgiye olan bağımlılığı artırmıştır. Bu dönüşüm süreci, bilgiyi sadece destekleyici bir araç olmaktan çıkarıp günlük hayatın ve sosyo-ekonomik işleyişin merkezine yerleştirmiştir (Aldemir ve Kaya, 2020). Dijitalleşme süreci, günlük hayatımıza ve kurumsal işleyişe büyük kolaylıklar sağlarken, diğer taraftan bilgi güvenliğini sağlamayı bir teknik detay olmaktan çıkarıp doğrudan bir zorunluluk haline getirmektedir. Ancak dijitalleşmenin getirdiği bu kolaylıklar, aynı zamanda bilginin kötüye kullanılması gibi ciddi güvenlik risklerini de beraberinde getirmektedir. Bilgi varlıklarını yönetemeyen veya koruyamayan kurumlar için bu süreç ekonomik ve idari problemler yaratırken, siber güvenlik konusu ulusal güvenliğin en öncelikli meselelerinden biri haline gelmiştir. Dijitalleşme, bilginin küresel ölçekte saniyeler içinde dolaşımına imkân tanısa da, bu durum verileri geçmişe göre daha savunmasız bırakmaktadır. Bu nedenle siber güvenlik kavramı, bilginin korunması, muhtemel kayıpların önüne geçilmesi ve ilgili önlemlerin alınması yönünde hem birey hem de kurum bazında dikkatle incelenmesi gereken stratejik bir konudur. Siber güvenliğin taşıdığı bu stratejik husus, onu sıradan bir bilgi işlem faaliyeti olmaktan çıkararak; kurumların piyasadaki varlığını, itibarını ve ekonomik ömrünü güvence altına alan en temel yönetim stratejilerinden biri haline getirmektedir. Özellikle finansal veriler, kişisel bilgiler ve ticari sırlar siber saldırıların öncelikli hedefleri arasındadır. Bu hassas bilgilerin korunması ve erişimin kontrol altında tutulması zorunluluğu, bilgi güvenliği kavramını öne çıkarmaktadır. Özellikle günümüzde sistemlerin birbirine entegre çalışması, tek bir güvenlik açığının bile zincirleme hasarlara yol açma riskini artırmaktadır (Solmaz, 2023).

Dijitalleşme süreciyle birlikte genişleyen risk ortamı değerlendirildiğinde, verilerin korunmasının artık göz ardı edilemeyecek kadar kritik bir boyuta ulaştığı anlaşılmaktadır. Bu noktada karşımıza çıkan bilgi güvenliği; en temel tanımıyla bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin güvence altına alınmasıdır (Efe, 2019). Söz konusu üç temel ilkenin, yetkisiz erişimlerin önlenmesi ve veri içeriğinin bozulmadan ihtiyaç anında kullanıma sunulması süreçlerine dayandığı görülmektedir. Tüm bu gereklilikler göz önüne alındığında, günümüzde bilgi güvenliği kavramını sadece yazılımsal veya donanımsal bir teknik önlem olarak yorumlamanın eksik bir yaklaşım olabileceği düşünülmektedir. Dolayısıyla bu durumun, idari süreçlerin, kurumsal politikaların ve hukuki yükümlülüklerin uyum içinde yürütüldüğü bütüncül ve stratejik bir yönetim felsefesini gerekli kıldığı değerlendirilmektedir. Nitekim Türkiye'de yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) mevzuatı gibi yasal düzenlemeler, bu bütüncül yaklaşımı desteklemekte ve verilerin güvenli bir şekilde yönetilmesini kurumlar için kesin bir hukuki yükümlülük haline getirmektedir (Erdem ve Süzen, 2025). Bireylerden devletlere kadar kritik bir öneme sahip olan bilgi güvenliği, günümüzde kurumların devamlılığının ve iş sürekliliğinin sağlanması adına bir gereksinim haline gelmiştir (Akseki, Meydaneri ve Taşdemir, 2023). Finansal veriler veya stratejik planlar gibi bilgi varlıklarının zarar görmesinin, kurumlar açısından ciddi maddi ve manevi kayıplara zemin hazırlayabileceği öngörülmektedir. Mevcut yüksek risk potansiyeli göz önüne alındığında; bilgi güvenliğini yalnızca teknik birimlerin yerine getirmesi gereken bir görev olarak değerlendirmenin eksik bir yaklaşım olabileceği düşünülmektedir. Dolayısıyla, bu sürecin üst yönetimden tüm çalışanlara kadar yayılan ortak ve bütüncül bir sorumluluk alanı olarak ele alınmasının, kurumların devamlılığı açısından daha güvenli bir zemin sunacağı ifade edilebilir.

Bilgi ve iletişim teknolojilerinin son on yılda yaşadığı hızlı dönüşüm, toplumsal ve ekonomik süreçleri dijital bir zemine taşırken, siber uzayı da modern devletlerin en kritik cephelerinden biri haline getirmiştir. Türkiye özelinde 2015-2025 dönemi, kamu hizmetlerinin e-devlet üzerinden merkezileştiği,

finansal teknolojilerin tabana yayıldığı ve sanayiye entegre olduğu bir süreci kapsamaktadır (Damar, 2022). Bu gelişmeler ülkemiz açısından sektörün güçlü yönü olarak görülmektedir (Aydın, 2012). Nitekim ülkemizde önceleri dışa bağımlı olarak sürdürülen bilişim sektörü, uygulayıcı rolünden çıkarak kendi değerlerini üretme çabasına girmiştir (Aydınbaş,2023). Ancak bu teknolojik genişleme, beraberinde saldırı yüzeyi olarak tanımlanan alanın da kontrolsüz bir şekilde büyümesine neden olmuş; siber tehditleri bireysel boyuttan, ulusal güvenliği tehdit eden organize bir yapıya dönüştürmüştür. Geçmişte daha çok sistemleri işlevsiz bırakmaya yönelik olan DDoS gibi basit zararlı yazılım saldırıları artarak devam etmekte (Aydın, 2023), diğer taraftan veri sızıntıları, karmaşık fidye yazılımları ve yapay zekâ destekli oltalama faaliyetleri gibi yeni saldırılar veya yöntemler ortaya çıkmaktadır. Nitekim gelecekteki saldırıların artık sadece veri hırsızlığıyla sınırlı kalmayıp, kritik altyapılar gibi ulusal güvenliği ve toplumsal düzeni doğrudan hedef alacağı tahmin edilmektedir (Hur vd., 2017).

Mevcut literatür, teknik açıkların kapatılmasının tek başına yeterli olmadığını, zafiyetlerin büyük bir kısmının idari boşluklar veya kullanıcı farkındalığındaki eksikliklerden kaynaklandığını göstermektedir. Bu nedenle, geçmiş on yılı güvenlik çerçevesinde analiz etmek, yalnızca kronolojik bir döküm sunmak değil, aynı zamanda savunma mekanizmalarımızın hangi noktalarda kırıldığını anlamak adına hayati bir önem taşımaktadır. Diğer taraftan, Türkiye'nin siber güvenlik ekosistemi sadece teknik bir gelişim değil, yoğun bir hukuki ve idari yapılanma süreci de geçirmiştir. Ancak mevzuatın dinamik teknolojik değişimlere adaptasyon hızı, akademik bir perspektifle incelenmeye muhtaçtır. Bu araştırma, teknik zafiyetler, yönetsel stratejiler ve hukuki düzenlemeler arasındaki eşgüdümü sorgulayarak, Türkiye'nin dijital geleceği için daha dirençli ve sürdürülebilir bir güvenlik politikası oluşturulmasına bilimsel bir temel sunmayı hedeflemektedir.

Çalışma, 2015–2025 döneminde Türkiye'de bilgi güvenliği alanında ortaya çıkan başlıca problemleri ve güvenlik zafiyetlerini incelemektir. Söz konusu dönemde öne çıkan siber saldırı türlerinin dönemsel olarak nasıl evrildiğini ve bu saldırılara karşı geliştirilen teknik, idari ve hukuki önlemleri analiz etmeyi amaçlamaktadır. Bu kapsamda Türkiyedeki son yıldaki bilgi güvenliği ve siber güvenlik alanında yapılan çalışmaların evriminin nasıl olduğu araştırma sorusu olarak dikkate alınmıştır.

Makalenin diğer kısımları şöyle organize edilmiştir: İkinci Bölümde kavramsal çerçeve ele alınmış, Üçüncü bölümde ise çalışmanın metodolojisi yer almaktadır. Bölümde bulgular doğrultusunda Dönemsel kırılımlar ele alınmıştır. Son bölümde çalışma özetlenmiştir.

2. Kavramsal Çerçeve

2.1. Bilgi Güvenliği

Bilgi güvenliği, bir kurumun sahip olduğu her türlü bilginin yetkisiz kişilerin eline geçmesini, izinsiz olarak değiştirilmesini veya yok edilmesini engellemeye yönelik teknik ve yönetsel faaliyetlerin tümünü ifade eder. Bu kapsamda sadece bilgisayar sistemlerinde tutulan dijital veriler değil, kâğıt üzerindeki kayıtlar ve sözlü paylaşımlar da korunması gereken bilgi varlığı olarak kabul edilir (Akseki, Meydaneri ve Taşdemir, 2023). Hangi formatta olursa olsun, bilginin taşıdığı bu stratejik değer günümüzde eşi görülmemiş bir seviyeye ulaşmıştır. Nitekim bilgi toplumunda bilginin temel üretim faktörü hâline gelmesiyle birlikte, bilgi güvenliği de bilgiye erişim kadar önemli bir ihtiyaç olarak ortaya çıkmıştır(Özdemirci ve Torunlar, 2018).

Günümüzde bilgi güvenliği, iş sürekliliğini sağlama, maddi ve itibari kayıpları önleme ve hukuki yükümlülükleri yerine getirme açısından kurumsal düzeyde stratejik bir yönetim alanı olarak görülmektedir(Kestane, 2025). Bu nedenle konu, yalnızca bilgi işlem birimlerinin değil, üst yönetimden en alt kademedeki çalışanlara kadar tüm personelin sorumluluk alanına giren kurumsal bir süreç olarak ele alınmalıdır. Bu çerçevede bilgi güvenliği, kurumların yalnızca teknik altyapı yatırımı değil, aynı

zamanda risk yönetimi ve kurumsal yönetişim anlayışlarını da yeniden gözden geçirmesini gerektiren bir alan hâline gelmektedir (Yeniman Yıldırım, 2018). Kurumların söz konusu risk ve yönetişim süreçlerini başarıyla yürütebilmesi, bilginin korunmasına yönelik temel ilkelerin kurumsal mimariye eksiksiz bir şekilde entegre edilmesine bağlıdır. Bilgi güvenliği, genel kabul gören ve birbirinden ayrılmaz üç temel bileşen üzerinden inşa edilmektedir. Bu evrensel yapı, gizlilik, bütünlük ve erişilebilirlik ilkelerinden oluşmaktadır.

2.1.1. Bilgi Güvenliğinin Temel İlkeleri

Bilgi güvenliği literatüründe en çok kabul gören yaklaşım, kavramı üç temel ilke üzerinden açıklar: gizlilik, bütünlük ve erişilebilirlik. Bu üçlü yapı, hem teorik tartışmalarda hem de kurumların güvenlik politikalarında bilgi güvenliğinin omurgasını oluşturur.

Gizlilik ilkesi, bilginin sadece yetkili kişi, sistem ve süreçler tarafından görülebilmesini ve yetkisiz erişimlerin engellenmesini ifade eder (Akseki, Meydaneri ve Taşdemir, 2023). Kurumların müşteri kayıtları, finansal verileri veya personel bilgileri gibi hassas verilerin üçüncü kişilerce ele geçirilmesi, gizlilik ilkesinin ihlali anlamına gelir.

Veri sızıntıları, zayıf parolalar, oltalama, zararlı yazılımlar ve fidye yazılımları, gizliliği hedef alan başlıca tehdit unsurlarıdır(Aslay, 2017; Yeniman Yıldırım, 2018; Solmaz; Erdem ve Süzen, 2025). Bu ilkenin korunması için kimlik doğrulama, erişim yetkilendirme ve şifreleme gibi yöntemler kullanılmaktadır. Özellikle çok sayıda kullanıcıya açık sistemlerde, gizlilik ilkesinin ihlali doğrudan itibar kaybı ve hukuki yaptırımlarla sonuçlanabilmektedir.

Bütünlük ilkesi, bilginin yetkisiz ya da hatalı biçimde değiştirilmemesini, kaynaktan hedefe giderken içeriğinin bozulmadan korunmasını amaçlar (Aldemir ve Kaya, 2020). Bir veritabanındaki kayıtların izinsiz silinmesi, değiştirilmesi veya sisteme sahte veri eklenmesi, bilgi bütünlüğünü zedeleyen örneklerdir. Zararlı yazılımlar ve yetkisiz müdahaleler bütünlük ilkesini tehdit eder; bu nedenle özet değerleri, dijital imzalar ve değişiklik kayıtları gibi mekanizmalardan yararlanılır.

Finansal işlemler ve kritik kayıt sistemlerinde bütünlük ihlallerinin tespiti çoğu zaman zor olduğundan, bu ilkenin korunması yalnızca teknik değil, denetimsel kontrolleri de gerektirmektedir(Kestane, 2025).

Erişilebilirlik ilkesi ise yetkili kullanıcıların bilgiye ihtiyaç duydukları anda, kabul edilebilir süre ve performans düzeyinde erişebilmesini ifade eder(Akseki, Meydaneri ve Taşdemir, 2023). Erişilebilirlik ilkesinin ihlali, temel olarak Dağıtık Hizmet Dışı Bırakma (DDoS) saldırıları ya da kritik altyapılarda meydana gelen teknik arızalar sonucunda ortaya çıkmaktadır. Kesintisiz çalışması gereken hayati altyapılarda erişilebilirliğin sekteye uğraması, sadece ciddi ekonomik zararlar doğurmakla kalmayıp aynı zamanda toplumsal işleyişte geniş çaplı aksamalara da sebebiyet verebilmektedir (Can, 2022; Genco, 2020).

Bu üç temel ilkenin yanında güvenilirlik, kimlik doğrulama, inkâr edememe ve kayıt tutma gibi yardımcı ilkeler de bilgi güvenliği yönetimini tamamlayan unsurlar olarak değerlendirilmektedir. Böylece bilgi güvenliği, tek tek teknolojilerden ibaret değil; bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini birlikte gözeten bütüncül bir çerçeve hâline gelmektedir.

2.2. Siber Güvenlik

Gelişen teknoloji ve internetin gündelik hayatın ayrılmaz bir parçası hâline gelmesiyle birlikte yönetim, hizmet ve iletişim süreçleri tamamen dijital ortama taşınmıştır. Bu dönüşüm, kara, deniz, hava ve uzay gibi fiziksel boyutlardan bağımsız, kendine has sanal bir ekosistem olan siber uzay (siber ortam, siber alan) kavramını ortaya çıkarmıştır. İlk olarak 1980'lerde literatürde görünürlük kazanan bu kavram; günümüzde yalnızca internete bağlı ağları değil, iletişim temelli cep telefonlarından telsiz sistemlerine,

uçaklardan insansız hava araçlarına kadar bilgi teknolojilerini kullanan tüm kapalı ve açık ağları kapsamaktadır. Dijital imkânların devlet, kurum ve bireyler tarafından her alanda kullanılması, bilginin barındığı tüm bu sanal ortamları açık birer hedef hâline getirmiştir. Bu bağlamda, siber uzaydaki bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkeleri çerçevesinde korunması amacıyla alınan tüm önlemler ve olgular bütünü, modern siber güvenlik kavramını ortaya çıkarmıştır (Aldemir ve Kaya, 2020).

Bilgi güvenliği kavramı doğrudan bilginin kendisini korumaya odaklanırken; siber güvenlik, bu bilginin barındığı, işlendiği ve iletildiği ağların, sunucuların, mobil cihazların ve elektronik sistemlerin bütünüyle korunmasını kapsayan çok daha geniş ve eylemsel bir çerçeve sunar (Karayel ve Akbıyık, 2023). Başka bir deyişle siber güvenlik; kurumların, devletlerin ve bireylerin dijital varlıklarını kötü amaçlı saldırılara karşı korumak amacıyla teknoloji, süreç, risk yönetimi ve eğitim gibi araçların entegre bir şekilde kullanılmasıdır (Karayel ve Akbıyık, 2023).

Teknolojinin ve internetin hızla yaygınlaşmasıyla birlikte siber tehditlerin boyutu, yalnızca bireysel veri hırsızlığı olmaktan çıkmış; kurumların iş sürekliliğini, kritik altyapılarını ve devletlerin ulusal güvenliğini hedef alan çok boyutlu bir tehdit halini almıştır(Aslay, 2017). Dolayısıyla modern anlamda siber güvenlik; sadece ağları ve sistemleri pasif bir şekilde korumanın ötesinde, oluşabilecek siber saldırıları önceden tespit etmeyi, saldırı anında teknik destek ve savunma mekanizmalarını devreye sokmayı ve olası bir hasar durumunda sistemleri hızla eski ve güvenli hâline döndürmeyi amaçlayan stratejik bir yönetişim sürecidir(Aslay, 2017).

2.3. Kritik Altyapı

Modern toplumların işleyişi ve refahı, kesintisiz hizmet sunması beklenen bazı temel yapılara doğrudan bağlıdır. Bu bağlamda AFAD tarafından hazırlanan Açıklamalı Afet Yönetimi Terimleri Sözlüğü' nde kritik altyapı; "işlevlerini kısmen veya tamamen yerine getir(e)mediğinde toplumsal düzenin sürdürülebilirliğinin veya kamu hizmetlerinin sunumunun olumsuz etkileneceği, ulaşım, haberleşme, enerji, su, finans gibi sektörleri kapsayan ağ, varlık, sistem ve yapılar bütünü" olarak tanımlanmaktadır(AFAD, 2014). Modern toplumların temelini oluşturan bu yapılar; telekomünikasyon, su ve enerji kaynakları, ulaştırma ve finans sistemleri gibi devletin ve toplumun can damarı olan unsurları kapsamaktadır.

Türkiye özelinde bu kavramın sınırları ve stratejik öncelikleri resmi kararlarla netleştirilmiştir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'na göre Türkiye'deki kritik altyapı sektörleri; haberleşme, enerji, su kaynakları, sağlık, ulaşım ve finansal hizmetler olmak üzere temel başlıklar altında belirlenmiştir(Resmî Gazete, 2013). Bu sektörlerin herhangi birinde yaşanacak bir kesintinin, sistemlerin birbirine bağımlı yapısı nedeniyle diğer sektörleri de etkileyerek ulusal çapta bir krize (ekonomik ve toplumsal refah kaybına) dönüşme potansiyeli bulunmaktadır(Can, 2022).

Kritik altyapıların günümüzde siber güvenliğin en temel inceleme alanlarından biri hâline gelmesinin ana nedeni ise bu sistemlerin hızla dijitalleşmesidir. Geniş coğrafi alanlara yayılmış olan bu devasa altyapıların kurulumu ve kesintisiz işletilmesi, genellikle SCADA (Merkezi Denetim ve Veri Toplama) adı verilen endüstriyel kontrol sistemleri aracılığıyla tek bir merkezden yönetilmektedir (USOM, 2014). Bu sistemlerin uzaktan kontrol edilebilmesi için internet hatlarına ve dijital ağlara bağlı olması, onları siber saldırganlar için cazip ve açık birer hedef hâline getirmektedir. Dolayısıyla kritik altyapılara yönelik başarılı bir siber saldırı, yalnızca sanal ortamdaki bir veri ihlali veya hırsızlığı olarak kalmamakta; elektriklerin kesilmesi, ulaşımın durması, hastanelerin çalışamaz hâle gelmesi ve finansal sistemin çökmesi gibi doğrudan ulusal güvenliği tehdit eden yıkıcı fiziksel felaketlere dönüşebilmektedir (Özker, 2022).

2.4 Sıfır GÜVEN

Siber güvenlik literatüründe Sıfır Güven kavramına yönelik çok çeşitli tanımlamalar bulunur bu çalışmada, Kindervag (2010) tarafından geliştirilen tanımlar dikkate alınmıştır. Sıfır Güven, bilgi güvenliğindeki geleneksel "iç ağ güvenilirdir, dış ağ güvenilmezdir" fikrini tamamen ortadan kaldıran yeni bir kavramsal modeldir (Kindervag, 2010). Bu modelin özünde yatan temel felsefe oldukça basittir: Güvenlik uzmanları, ağ üzerinden geçen veri paketlerine tıpkı insanlarmış gibi peşinen güvenme alışkanlığını derhal bırakmalıdır. Sıfır Güven mantığında, trafiğin kaynağına veya konumuna bakılmaksızın tüm ağ trafiği istisnasız bir şekilde "güvenilmez" olarak kabul edilir.

Bu felsefi dönüşüm üç temel ilkeye dayanmaktadır:

1.Konumdan bağımsız olarak tüm kaynaklara güvenli erişimin sağlanması.

2."En az ayrıcalık" kuralının kesin bir biçimde uygulanması ve erişim kontrollerinin sıkı tutulması. 3.Ağdaki tüm trafiğin sürekli olarak denetlenip kaydedilmesi (Kindervag, 2010).

Bu sayede güvenlik, yalnızca ağın dış sınırlarını koruyan pasif bir kalkan olmaktan çıkıp, tüm iç ve dış hareketleri sürekli sorgulayan önleyici bir yapıya bürünmektedir.

Özellikle kritik altyapılara yönelik siber saldırıların etkisini minimuma indirmede bu önleyici yapı stratejik bir önem taşımaktadır. Güncel veriler, sistemlerini Sıfır Güven düzenine göre yapılandıran kritik altyapı kuruluşlarının, olası bir siber ihlal durumunda bu modele sahip olmayan kurumlara kıyasla ortalama 1.17 milyon ABD Doları daha az finansal zarara uğradığını göstermektedir (Özker, 2022). Ayrıca, olası siber zararların yalnızca dış saldırganlardan değil, ağın tam merkezindeki iç kaynaklardan da gelebileceği gerçeği göz önüne alındığında Sıfır Güven anlayışının kurumlara eklenecek sıradan bir teknik tavsiye olmaktan çıkarak, hayati bir güvenlik zorunluluğu hâline geldiği değerlendirilmektedir. (Aldemir ve Kaya, 2020).

John Kindervag tarafından 2010 yılında ortaya konulan Sıfır Güven ağ mimarisi, güvenliği sonradan eklenen bağımsız bir katman olmaktan çıkarıp doğrudan ağın temel yapısına yerleştirmek amacıyla üç ana bileşen üzerinden şekillendirilmiştir (Kindervag, 2010).

Bölümlendirme Ağ Geçidi: Geleneksel ağ tasarımlarında sistemi korumak amacıyla güvenlik duvarı, izinsiz giriş önleme sistemleri, web uygulama güvenlik duvarı, ağ erişim kontrolü ve sanal özel ağ gibi birbirinden bağımsız çalışan birçok cihaz kullanılmaktadır. Bölümlendirme ağ geçidi, bu dağınık güvenlik ürünlerinin işlevlerini merkezi bir paket yönlendirme motorunda bütünleştiren entegre bir donanımdır. Söz konusu bileşen, ağın dış sınırları yerine doğrudan merkezine konumlandırılarak tüm ağın güvenli bir biçimde bölümlere ayrılmasını ve güvenlik politikalarının tek bir noktadan yönetilmesini sağlamaktadır (Kindervag, 2010).

Mikro Çekirdek ve Çevre: Ağın çok daha kolay yönetilebilen, paralel ve güvenli alt segmentlere ayrılmış biçimidir. Bölümlendirme ağ geçidinin arayüzüne bağlanan her bir alan mikro çevre olarak adlandırılmaktadır. Bu bileşenin temel amacı, benzer işlevlere sahip kaynakları (örneğin yalnızca web sunucularını veya veritabanlarını) aynı mikro alan içinde toplayarak izole bölgeler oluşturmaktır. Böylece her mikro bölgeye özgü politikalar tanımlanabilmekte ve bir segmentte ortaya çıkabilecek olası bir güvenlik zafiyetinin ağın diğer kısımlarına yatay olarak yayılması (sıçraması) büyük ölçüde engellenmektedir (Kindervag, 2010).

Veri Toplama Ağı: Sıfır Güven yaklaşımının "tüm trafiği denetle ve kaydet" ilkesini teknolojik olarak işlevsel hâle getiren özel bir ağ altyapısıdır. Ağ üzerindeki tüm verilerin (paketler veya sistem günlük mesajları), güvenlik bilgi yönetimi ile ağ analizi ve görünürlük sistemleri tarafından merkezi bir noktada toplanıp incelenmesi amacıyla tasarlanmıştır. Bu yapı, ağın içinden veya dışından geçen tüm trafiği

anlık olarak izleyip kayıt altına alarak, sistemin bütünüyle şeffaf ve denetlenebilir olmasını güvence altına almaktadır (Kindervag, 2010).

Türkiye'de Sıfır Güven mimarisinin uygulanmasındaki başlıca zorluklar; mevcut geleneksel ağların yüksek maliyetli modernizasyon gereksinimi, nitelikli siber güvenlik uzmanı açığı, eski sistemlerin güncel ve katı yasal regülasyonlara (KVKK vb.) uyarlanmasındaki yapısal güçlükler ve iş sürekliliğini ön planda tutan geleneksel kurumsal kültürün getirdiği adaptasyon problemleridir (Aldemir ve Kaya, 2020; BTK, 2025; Özker, 2022).

2.5 Siber Dirençlilik

Siber dirençlilik, bir kurumun, bilişim sisteminin veya toplumun büyük bir siber saldırı, şok veya kriz karşısında saldırıya direnme, saldırı anında dahi asgari düzeyde hizmet vermeyi sürdürebilme ve ardından hızla toparlanarak işlerliğini yeniden veya eskisinden daha güçlü bir şekilde kazanma kapasitesidir (Can, 2023). Geleneksel güvenlik anlayışının aksine siber dirençlilik, siber saldırıları tamamen sıfırlamanın imkânsız olduğu gerçeğinden yola çıkarak riskleri yönetilebilir bir seviyede tutmayı amaçlar (Can, 2023; UAB, 2016). Bu kavramın temelinde; tehditleri önceden saptama ve önleme, saldırı sırasında izlenmesi gereken adımları koordine etme ve tehdit bertaraf edildikten sonra sistemin en kısa sürede iyileştirilmesi yatmaktadır (Can, 2023).

2.5.1 Siber Dirençliliğin Kapsamı ve Önemi

Günümüzde finans, sağlık, eğitim, ulaşım ve enerji gibi kritik altyapıların tamamen bilişim ağlarına bağlı çalışması, siber dirençliliği sıradan bir teknik mesele olmaktan çıkarıp ulusal ve kamusal güvenliğin merkezine yerleştirmiştir (Can, 2023). Olası bir siber savaş, terör eylemi veya doğal afette siber alanın ve sivil altyapıların doğrudan hedef alınması ihtimali, siber dirençliliği toplumun ayakta kalması için elzem kılmaktadır. Siber dirençlilik kavramı, artık uluslararası güvenlik örgütlerinin de en temel savunma öncelikleri arasında yer almaktadır. Öyle ki NATO, siber uzayı kara, deniz, hava ve uzaydan sonra "beşinci cephe" olarak kabul etmiş; kurucu antlaşmasının 3. maddesi gereğince dirençliliği ortak bir savunma prensibi sayarak tüm üye ülkeleri sivil altyapılarını siber saldırılara karşı hazırlıklı hâle getirmekle yükümlü kılmıştır (Can, 2023).

Siber Dirençlilik Nasıl Sağlanır? Siber dirençlilik yalnızca güvenlik duvarı veya antivirüs gibi teknolojik araçlar satın alınarak inşa edilebilecek bir kalkan değildir. Aksine, katmanlar halinde ele alınması gereken "tüm toplum ve tüm devlet" yaklaşımını zorunlu kılar (Can, 2023). Güçlü bir siber dirençlilik modelinin inşası şu unsurlara dayanmaktadır:

Topyekün Hazırlıklılık ve İşbirliği: Bireylerin, özel işletmelerin, sivil toplum örgütlerinin, üniversitelerin ve devlet organlarının bütünleşik bir hazırlık içinde olması ve gerektiğinde uluslararası seviyede işbirliği yapması (Can, 2023).

Önleyici Savunma ve Sıfır Güven Mimarisi**:** Tehdit oluştuktan sonra tepki veren reaktif yapılardan ziyade; iç ağları bölen, içeriden veya dışarıdan gelen hiçbir erişim talebine peşinen güvenmeyen ve sürekli doğrulama prensibine dayanan "Sıfır Güven" gibi proaktif modellere geçiş yapılması (Erdem ve Süzen, 2025; Kindervag, 2010).

Düzenli Denetimler: Bilişim sistemlerindeki olası zafiyetlerin önceden tespit edilebilmesi ve uluslararası standartlara uyumun gözetilmesi için siber güvenlik denetimlerinin kurumsal bir zorunluluk hâline getirilmesi (Kestane, 2025).

İnsan Faktörü ve Eğitim: Teknolojik altyapılar ne kadar sağlam olursa olsun güvenlik zincirinin en zayıf halkası insan olduğundan, tüm personelin siber güvenlik konularında (oltalama vb.) sürekli eğitilerek kalıcı bir farkındalık kültürü oluşturulması (Aldemir ve Kaya, 2020; Erdem ve Süzen, 2025).

Kriz Yönetimi ve Afet Kurtarma Süreçleri: Saldırı anında ve sonrasında hizmet kesintilerini en aza indirmek için şeffaf bir kriz yönetimi planının önceden hazırlanması ve afet kurtarma merkezlerinin aktif-aktif modda çalıştırılması şarttır. Özellikle sistemleri kilitleyen fidye yazılımı tehditlerine karşı siber dirençliliği sağlayabilmek için kritik verilerin sistemden yalıtılmış ortamlarda düzenli olarak yedeklenmesi hayati önem taşımaktadır (Erdem ve Süzen, 2025).

Kamu-Özel Sektör İşbirliği: Günümüzde siber saldırıların öncelikli hedefi olan kritik altyapıların çok büyük bir kısmı özel sektör tarafından kurulmakta ve işletilmektedir. Bu nedenle ulusal güvenliği sağlamakla görevli kamu otoriteleri ile altyapıların operasyonel sorumluluğunu taşıyan özel sektör arasında anlık tehdit istihbaratı ve veri paylaşımını zorunlu kılan Kamu-Özel Sektör İşbirliği modellerinin tesis edilmesi, siber risklerin azaltılması açısından elzemdir (Özker, 2022).

2.6 Siber Tehditler ve Başlıca Saldırı Türleri

Siber dirençliliğin etkin bir şekilde sağlanabilmesi için öncelikle kurumların ve kritik altyapıların karşı karşıya kaldığı siber tehditlerin doğasının anlaşılması gerekmektedir (Aslay, 2017). Literatürde öne çıkan ve kurumların iş sürekliliğini doğrudan tehdit eden başlıca siber saldırı türleri ile tehdit aktörleri şu şekilde sınıflandırılmaktadır:

Hizmet Engelleme (DoS) ve Dağıtık Hizmet Engelleme (DDoS) Saldırıları: Hedef sistemin bant genişliğini, işlem gücünü veya kaynaklarını aşırı trafik göndererek tüketmeyi ve sistemi yasal kullanıcılar için erişilemez duruma getirmeyi amaçlayan saldırılardır (Öztürk vd., 2025). Bu saldırılar kaynaklarına göre tek kaynaklı ve çok kaynaklı olmak üzere iki ana gruba ayrılmaktadır (Öztürk vd., 2025). Tek kaynaklı olan Dos saldırıları, tek bir cihaz veya IP adresinden gelen zararlı trafikle sistemleri işlevsiz hale getirmeye çalışır ve tüm trafik belirli bir noktadan gönderildiği için kaynağını tespit etmek ve engellemek nispeten daha kolaydır (Öztürk vd., 2025). Buna karşılık çok kaynaklı olan Ddos saldırıları, farklı coğrafi bölgelerden ve fiziksel lokasyonlardan aynı anda gelen koordineli trafiği içerdiği için tespit edilmesi ve önlenmesi çok daha zor bir yapıya sahiptir (Öztürk vd., 2025). Özellikle finans, kamu ve e ticaret gibi kritik sektörlerde ciddi hizmet kesintilerine yol açarak ağ cihazlarının aşırı yüklenmesine, paket kayıplarına ve bant genişliğinin tamamen tükenmesine neden olmaktadır (Erdem ve Süzen, 2025; Öztürk vd., 2025).

Fidye Yazılımı (Ransomware) Saldırıları: Bilişim sistemlerine sızarak kritik verileri ve dosyaları şifreleyen, ardından sistemin kilidinin açılması karşılığında kurbanlardan maddi talepte bulunan zararlı yazılımlardır (Solmaz, 2023; Yeniman Yıldırım, 2018). Küresel ve ulusal çapta etkili olan türleri, sistemleri tamamen kilitleyerek kurumların iş sürekliliğini durdurma ve büyük maddi zararlara yol açma potansiyeline sahiptir (Erdem ve Süzen, 2025; Solmaz, 2023).

Oltalama (Phishing) Saldırıları: Güvenlik zincirinin en zayıf halkası olan insan faktörünü hedef alarak sahte e postalar, kısa mesajlar veya taklit web siteleri aracılığıyla kullanıcıları aldatıp sistem parolalarını, finansal verileri ve kişisel bilgileri ele geçirmeyi amaçlamaktadır (Yeniman Yıldırım, 2018). Bu yöntem, gelişmiş saldırıların ilk adımı olarak sıklıkla kullanılmakta ve hedefli senaryolarla çalışanları manipüle ederek kapalı sistemlere sızılmasını sağlamaktadır (Erdem ve Süzen, 2025).

Gelişmiş Kalıcı Tehdit (APT): Kurumların veya devletlerin kritik altyapılarına sızarak uzun süre fark edilmeden ağda barınmayı, veri toplamayı ve sistemin işleyişini bozmayı hedefleyen, yüksek düzeyde teknik beceri gerektiren karmaşık saldırı türleridir (UAB, 2020). Genellikle hedefli sistemlerin keşfedilmemiş zafiyetlerinden yararlanarak büyük bir gizlilik içinde hareket ederler ve fiziksel altyapılara dahi zarar verebilecek seviyeye ulaşabilmektedirler (Erdem ve Süzen, 2025).

Tedarik Zinciri Saldırıları: Kurumların doğrudan kendi ana sistemleri yerine, entegre oldukları veya yazılım ve donanım desteği aldıkları üçüncü taraf sağlayıcıların güvenlik açıklarından faydalanılarak gerçekleştirilen sızma operasyonlarıdır (Erdem ve Süzen, 2025). Bu yöntem, kendi iç güvenliğini üst düzeyde sağlamış kurumları bile dış tedarikçilerinin ve iş ortaklarının zafiyetleri üzerinden savunmasız bırakabilmektedir (Erdem ve Süzen, 2025).

Devlet Destekli Tehdit Aktörleri: Doğrudan devletler tarafından finanse edilen veya desteklenen, siber casusluk, ekonomik sabotaj ve ulusal kritik altyapıları çökertme gibi jeopolitik ve ideolojik hedeflerle hareket eden profesyonel gruplardır (Özker, 2022). Maddi kazançtan ziyade ulusal güvenlik ve istikrarı tehdit etmeyi amaçlayan bu aktörler, genellikle en gelişmiş siber silahları kullanarak uzun vadeli tahribat yaratmayı hedeflerler (Erdem ve Süzen, 2025).

Bu saldırılar, farklı motivasyonlarla hareket eden hackerlar, devlet destekli saldırganlar ve hacktivistler gibi çeşitli tehdit aktörleri tarafından gerçekleştirilebilir.

2.6.1 Saldırı Türlerinin Analizi

Hedef sistemin bant genişliğini ve işlem gücünü tüketmeyi amaçlayan siber saldırılarda, farklı coğrafi konumlardan eşzamanlı gerçekleştirilen çoklu lokasyon saldırıları ağ performansını ciddi şekilde düşürmekte ve tespiti zorlaştırmaktadır (Öztürk vd., 2025). Bu yıkıcı etkinin Türkiye özelindeki yansımalarına bakıldığında; 2019 ve 2020 yıllarında ülkenin en büyük bankalarını ve telekomünikasyon altyapılarını hedef alan, web sitelerine erişimi engelleyerek operasyonel süreçleri durma noktasına getiren eylemlerin tipik birer dağıtık hizmet engelleme saldırısı olduğu görülmektedir (Erdem ve Süzen, 2025; Özker, 2022). Operasyonel felç yaratma kapasitesine sahip bir diğer tehdit olan fidye yazılımları da sadece veri şifreleyip para talep eden araçlar olmaktan çıkmış, Türkiye'deki kritik kurumları derinden etkileyen silahlara dönüşmüştür (Özker, 2022). 2022 yılında Türkiye'de faaliyet gösteren bir dijital cüzdan şirketine yapılan saldırıda sistemler kilitlenmiş, Bitcoin cinsinden fidye istenmiş ve kurum operasyonel olarak büyük bir darbe alarak nakit sıkıntısı yüzünden toparlanmakta güçlük çekmiştir (Erdem ve Süzen, 2025).

Bu tür yıkıcı saldırıların ilk giriş kapısı olarak genellikle oltalama eylemleri stratejik bir rol oynamaktadır (Erdem ve Süzen, 2025). Türkiye'de finansal sistemleri hedef alan oltalama eylemleri giderek profesyonelleşmiş olup, kaydedilen 388.497 saldırının %57'sinin doğrudan ödeme işlemlerini hedef aldığı tespit edilmiştir (Erdem ve Süzen, 2025). Gelişmiş kalıcı tehditler, sisteme anlık zarar vermekten ziyade aylarca fark edilmeden ağda barınmayı ve stratejik bilgi toplamayı hedefleyen yüksek becerili saldırılardır (Özker, 2022). Türkiye bağlamında incelendiğinde; ülkenin enerji ve finans sektörlerini hedef alan uluslararası hacker gruplarının uzun vadeli siber casusluk faaliyetleri yürüttüğü görülmektedir (Erdem ve Süzen, 2025). Nitekim FireEye firmasının istihbarat raporuna göre Türkiye hedefli kötücül yazılım saldırılarında Avrupa'daki tüm ülkelerin toplamından daha fazla saldırıya maruz kalmış; Trend Micro'nun araştırmasına göre ise çevrimiçi bankacılığa yönelik saldırılarda Avrupa bölgesinde 11.516 vaka ile ilk sırada yer almıştır (Aslay, 2017).

Siber tehdit ekosistemindeki çarpan etkisini artıran bir diğer yöntem ise tedarik zinciri saldırılarıdır (Erdem ve Süzen, 2025). Saldırganlar, güvenlik duvarları güçlü olan ana hedeflere doğrudan saldırmak yerine, bu kurumların hizmet aldığı daha zayıf üçüncü taraf yazılım ve donanım tedarikçilerini hedef almaktadır (Erdem ve Süzen, 2025). Türkiye'deki finans kuruluşlarının üçüncü taraf teknoloji şirketleriyle sağladığı entegrasyonlar ve açık bankacılık uygulamaları, siber saldırganlar için yeni giriş noktaları oluşturarak tedarik zinciri zafiyetlerini artırmaktadır (Erdem ve Süzen, 2025). Tüm bu karmaşık saldırıların arkasındaki en büyük güç olan devlet destekli tehdit aktörleri ise siber uzayı asimetrik bir savaş alanına dönüştürmektedir (Genco, 2020). Bu aktörlerin birincil amacı finansal

kazanç değil, hasım devletlerin kritik altyapılarını tahrip etmek ve ekonomik istikrarı bozmaktır (Erdem ve Süzen, 2025). Türkiye'nin sahip olduğu jeopolitik konum ve barındırdığı uluslararası enerji hatları, ülkeyi devlet destekli siber operasyonların ana hedeflerinden biri haline getirmektedir (Özker, 2022). Nitekim 2018 yılında Türkiye Cumhuriyeti Merkez Bankasına yönelik gerçekleştirildiği iddia edilen siber saldırı girişimleri, ulusal ekonomik güvenliğin bu profesyonel gruplar tarafından nasıl doğrudan hedef alındığını göstermektedir (Erdem ve Süzen, 2025).

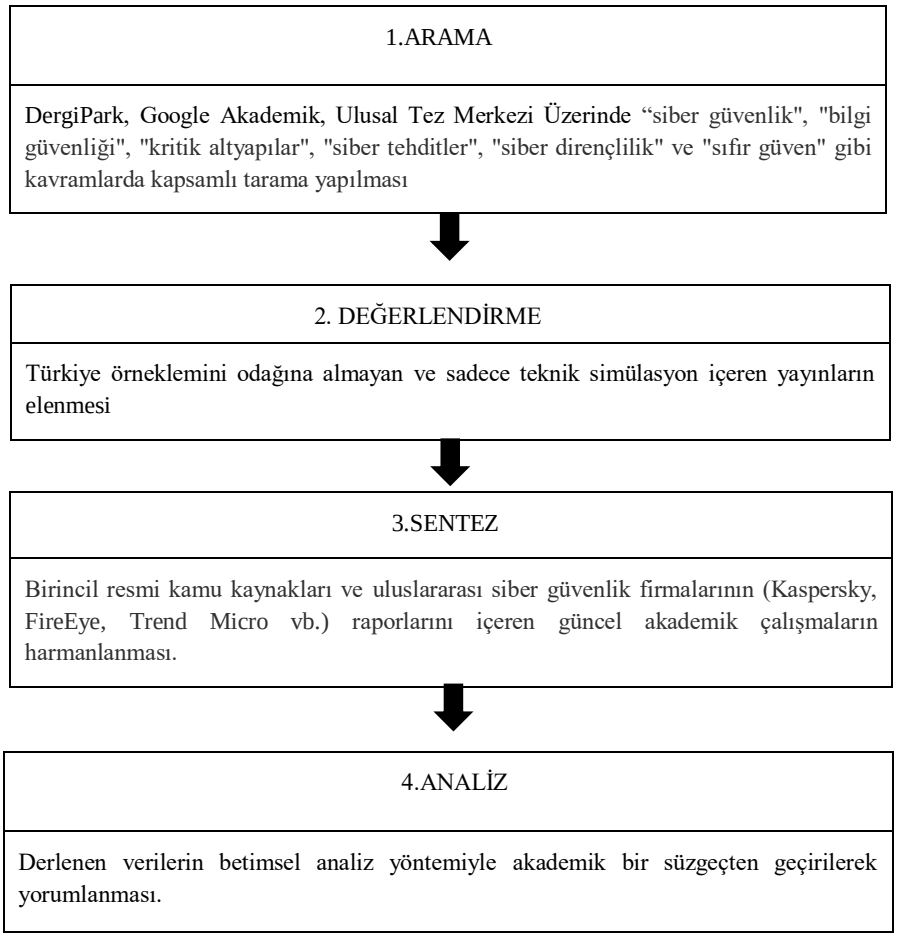
3. Yöntem

Bu çalışma, Türkiye'deki bilgi güvenliği ve siber güvenlik ekosisteminin 2015-2025 yılları arasındaki on yıllık dönüşümünü ve bu süreçteki stratejik kırılma noktalarını incelemek amacıyla nitel araştırma desenine uygun olarak tasarlanmıştır. Araştırma sürecinde, nitel literatür taramaları için uygun metodolojik çerçevelerden biri olan SALSA (Search, Appraisal, Synthesis, Analysis) modeli referans alınarak yapılandırılmış bir literatür seçimi gerçekleştirilmiştir. SALSA modeli kapsamında öngörülen dört temel aşama, araştırmanın hedefleri doğrultusunda şu şekilde yürütülmüştür.

Arama aşamasında araştırmanın veri setini oluşturmak amacıyla Türkiye'nin temel akademik veri tabanı olan DergiPark başta olmak üzere, Google Akademik ve Ulusal Tez Merkezi üzerinde kapsamlı taramalar yapılmıştır. Tarama stratejisi belirlenirken; "siber güvenlik", "bilgi güvenliği", "kritik altyapılar", "siber tehditler", "siber dirençlilik" ve "sıfır güven" temel kavramları, hem Türkçe hem de İngilizce literatürdeki karşılıklarıyla kombinasyonlar halinde ve 2015–2025 dönemini kapsayacak şekilde taranmıştır. Değerlendirme aşamasında araştırmanın temel kısıtı olarak Türkiye örneklemi belirlendiğinden, ilk aşamada ulaşılan geniş yayın havuzu üzerinde sıkı bir eleme süreci yürütülmüştür. Bu bağlamda, küresel ölçekli ancak Türkiye'nin yerel dinamiklerini, kurumsal yapısını veya ulusal mevzuatını odağına almayan tüm çalışmalar ilgisiz olarak değerlendirilerek analiz dışı bırakılmıştır. Ayrıca, sadece teknik yazılım simülasyonlarına odaklanan veya Türkiye'deki siber güvenlik politikalarının idari ve hukuki yansımalarını tartışmayan teknik içerikli yayınlar elenerek, araştırmanın kapsamı doğrudan ulusal ekosistemin dönüşümünü analiz eden çalışmalarla sınırlandırılmıştır.

Sentez aşaması çalışmanın metodolojik özgünlüğü, kamu kurumlarının (BTK, USOM, SOME) strateji belgeleri ve eylem planları gibi birincil resmi kaynaklar ile akademik literatürün harmanlanmasından kaynaklanmaktadır. Bu doğrultuda; çalışmanın yasal ve stratejik çerçevesi doğrudan ilgili kurumların yayınladığı ulusal strateji belgelerinden beslenirken, siber saldırı istatistikleri gibi nicel veriler, resmi devlet verilerini derleyen ve doğrulayan güncel akademik çalışmalar üzerinden analiz edilmiştir. Elde edilen veriler, Türkiye'nin siber güvenlik kronolojisindeki dönemsel eğilimleri yansıtacak şekilde kronolojik olarak tasnif edilmiştir. Analiz aşamasında, tasnif edilen veriler ve seçilen yerel literatürdeki bulgular betimsel analiz yöntemiyle yorumlanmıştır. Bu sayede Türkiye'nin siber güvenlik ekosisteminde yalnızca teknik önlemlere dayalı yaklaşımların yerini, nasıl daha önleyici ve stratejik bir yönetişim modeline bıraktığı bilimsel bir çerçevede ortaya konulmuştur.

Araştırmanın metodolojisi ve veri işleme süreci Şekil 1'de gösterilmiştir.



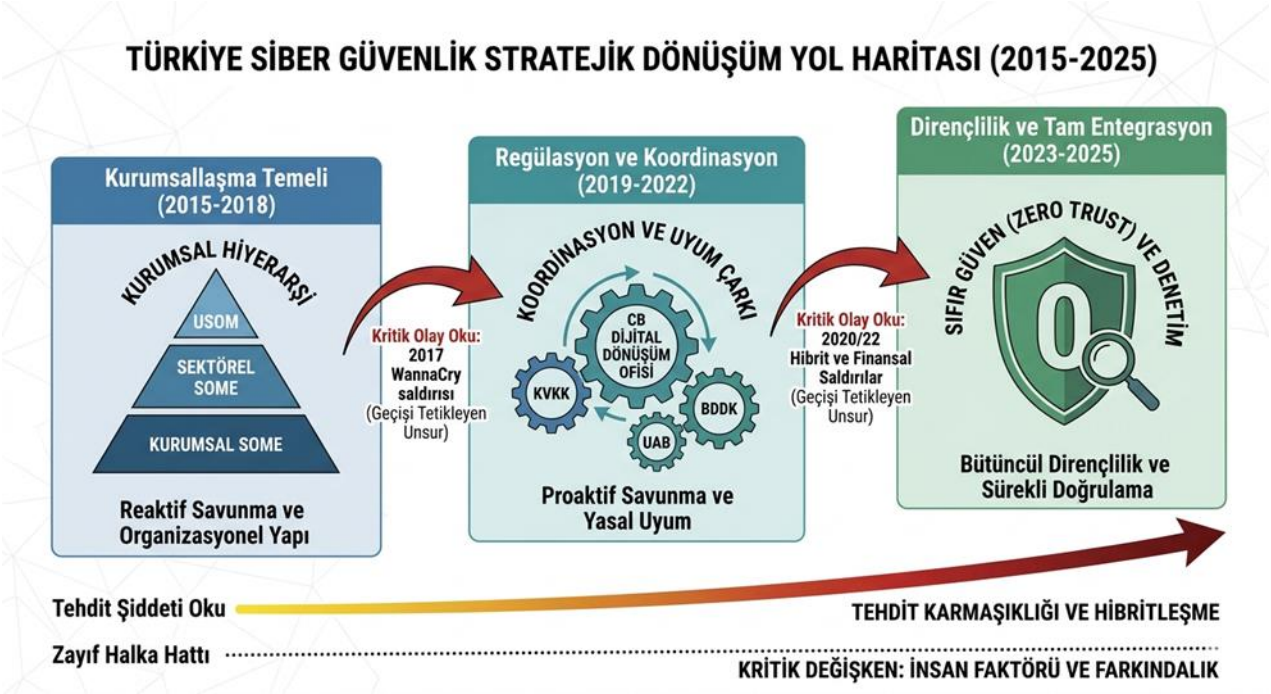
Şekil 1. Araştırma metodolojisi ve veri işleme süreci

Şekil 1'de özetlenen bu metodolojik çerçeve doğrultusunda elde edilen veriler, çalışmanın takip eden bölümünde Türkiye'nin siber güvenlik ekosistemindeki dönemsel kırılmalar ekseninde detaylı olarak analiz edilmiştir.

4. Türkiye'de Bilgi Güvenliği Yönetiminin Dönemsel Evrimi ve Kritik Kırılma Noktaları (2015-2025)

İçinde bulunduğumuz dijital çağda bilgi, yalnızca bir güç unsuru değil, aynı zamanda devletlerin, toplumların ve kurumların var olma ve bağımsızlık mücadelesinin en hayati merkezidir (Özdemirci ve Torunlar, 2018). Yaşanan bu dijital dönüşüm süreci, Türkiye'de bilgi güvenliği yönetiminin statik bir "bilgi işlem" prosedürü olmaktan çıkarak; ulusal güvenliğin ve ekonomik istikrarın merkezi bir unsuru hâline gelmesini zorunlu kılmıştır(Aldemir ve Kaya, 2020). Mevcut literatür tarandığında, bu sürecin statik bir yapıdan ziyade, tehditlerin niteliğine paralel olarak sürekli değişen dinamik bir evrim geçirdiği anlaşılmaktadır. Nitekim 2015 yılında siber güvenliğin daha çok kurumsal farkındalık boyutuyla ele alındığı çalışmalar, zamanla yerini kritik altyapıların korunmasına ve günümüzde 'dirençlilik' odaklı daha karmaşık savunma modellerine bırakmıştır (Aslay, 2017; Özker, 2022; Can, 2022). Özellikle siber tehditlerin ulaştığı devasa boyutlar ve 2025 yılı itibarıyla 101.500'ün üzerinde zararlı bağlantı girişiminin tespit edilerek erişime engellenmesi karşı karşıya olduğumuz siber tehditlerin ciddiyetini

açıkça ortaya koymaktadır (BTK, 2025). Bu doğrultuda çalışmanın bu bölümünde, Türkiye'nin siber güvenlik yolculuğu; odaklanılan temel stratejiler, karşılaşılan baskın tehditler ve alınan önlemler ekseninde üç ana kırılma dönemi altında analiz edilmiştir (Şekil 2).



Şekil 2. Türkiye Siber güvenlik stratejik dönüşüm yol haritası

4.1. I. Dönem (2015-2018): Farkındalık ve Kurumsal Yapılanma

Bu dönem, Türkiye'de siber güvenliğin teknik bir bilgi işlem sorunu olmaktan çıkıp, ulusal güvenliğin bir parçası olarak kurumsallaşmaya başladığı yıllardır. Türkiye'de bilgi güvenliğinin kurumsallaşması ve resmi bir devlet politikası haline gelmesindeki en büyük kırılma noktası, 2013 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı olmuştur. Bu resmi belge ile siber saldırıların asimetrik karakterine ve siber ortamın anonim yapısına dikkat çekilmiş; başta kritik altyapılar olmak üzere kamu ve özel sektör bilişim sistemlerinin güvenliğini sağlamak ulusal bir hedef olarak belirlenmiştir (Resmî Gazete, 2013).

Strateji belgesinde alınan kararlar doğrultusunda, siber uzayda ortaya çıkan tehditlerin hızla belirlenmesi ve olaylara ulusal/uluslararası düzeyde müdahale edilebilmesi için 7/24 esasına göre çalışacak Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve bu merkezin koordinasyonunda görev alacak Siber Olaylara Müdahale Ekipleri kurulmuştur (Resmî Gazete, 2013; Ünver, 2015). Bu kurumsal yapılanmanın sahaya indirilmesi ve kritik altyapıların korunması ise Sektörel SOME Kurulum ve Yönetim Rehberi ile sistematik bir yapıya kavuşturulmuştur. Rehber ile birlikte Türkiye'nin siber savunma organizasyonu; en üstte teknik destek ve ulusal koordinasyonu sağlayan USOM, sektör içi idari düzenleme yapan Sektörel SOME'ler ve kurumların kendi içindeki olaylara müdahale eden Kurumsal SOME'ler olmak üzere üçlü bir hiyerarşik bütünlüğe kavuşmuştur (USOM, 2014). Enerji, elektronik haberleşme, finans, ulaştırma, su yönetimi ve kritik kamu hizmetleri ülkenin en kritik altyapı sektörleri olarak belirlenmiş ve her bir sektör kendi Sektörel SOME' sini kurarak ulusal siber kalkanın yapıtaşlarını oluşturmuştur (Aldemir ve Kaya, 2020).

Bu kurumsal temeller üzerine inşa edilen ve 2015-2018 dönemine asıl damgasını vuran gelişme ise, 2016 yılında yayımlanan 2016-2019 Ulusal Siber Güvenlik Stratejisi olmuştur. Kapsamlı bir "Ortak

Akıl Platformu" neticesinde 73 kurum ve kuruluştan 126 uzmanın katılımıyla hazırlanan bu yeni planın ana amacı; siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesini ve ulusal siber uzaydaki tüm paydaşların güvenliğini sağlayacak idari ve teknolojik yetkinliğin eksiksiz kazanılmasını sağlamak olarak belirlenmiştir. Bu doğrultuda; siber savunmanın güçlendirilmesi, kritik altyapıların korunması, siber suçlarla mücadele, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin milli güvenliğe entegrasyonu gibi stratejik eylem başlıkları yürürlüğe konulmuştur (UDHB, 2016).

Ancak devlet kademesinde bu devasa yasal ve hiyerarşik adımlar atılırken, sahadaki kurumsal uygulamalar ve dönemin tehdit manzarası farklı zorluklarla karşılaşmıştır. Bu süreçte kurumlar, antivirüs ve güvenlik duvarı gibi teknik önlemlere odaklansa da "insan faktörü" ve son kullanıcı farkındalığı en zayıf halka olarak tanımlanmıştır (Aslay, 2017). Bilgi sistemlerine yönelik yaygın tehditler tarihsel süreçte bilgisayar solucanları, dağıtık hizmet engelleme saldırıları ve çeşitli zararlı yazılımlar olarak kendini gösterse de özellikle 2017 yılında küresel çapta etkili olan WannaCry fidye yazılımı saldırısı, bireysel ve kurumsal farkındalığı zorunlu kılan önemli bir kırılma noktası olmuştur (Solmaz, 2023; Yeniman Yıldırım, 2018). Nitekim dönemin literatürü incelendiğinde, devletin oluşturduğu savunma mekanizmalarına ve alınan teknik önlemlere rağmen; özellikle KOBİ'lerde ve kurumlarda bilgi güvenliği yönetimi konusunda farkındalığın yetersiz olduğu ve güvenlik politikalarının standartlara tam uygun yönetilmediği eleştirileri açıkça yer almıştır.

4.2. II. Dönem (2019-2022): Dijital Dönüşüm, Merkezi Koordinasyon ve Evrilen Tehditler

Bilgi güvenliği ekosisteminde 2019-2022 dönemi, Türkiye'de siber güvenliğin en üst düzeyde bir devlet politikası olarak yeniden yapılandırıldığı ve sektörel regülasyonların derinleştiği bir evre olmuştur. Bu dönemin en önemli kurumsal kırılma noktası, Cumhurbaşkanlığı Hükümet Sistemi'ne geçişle birlikte kurulan Dijital Dönüşüm Ofisi olmuştur. Dijital Dönüşüm Ofisi bünyesinde Siber Güvenlik Dairesi Başkanlığı'nın kurulmasıyla birlikte siber güvenlik faaliyetleri bakanlıkların alt birimlerinden çıkarak en üst makamdan koordine edilmeye başlanmıştır (Özker, 2022). Bu kurumsal dönüşümü, Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanan "2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" izlemiştir (UAB, 2020). Bu yeni plan ile ulusal kapasitenin geliştirilmesi, yeni nesil teknolojilerin güvenliği ve siber güvenliğin milli güvenliğe tam entegrasyonu temel amaçlar olarak belirlenmiştir.

Devletin en üst kademesinde atılan bu makro adımlar, sektörleri düzenleyici ve denetleyici kurumların yayımladığı katı regülasyonlarla sahaya indirilmiştir. Özellikle Bankacılık Düzenleme ve Denetleme Kurumu tarafından yayımlanan yönetmelikler, finansal kurumları bilgi sistemlerinin denetimini sağlamak ve güvenlik standartlarını zorunlu olarak uygulamakla yükümlü kılmıştır. Aynı dönemde, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun caydırıcı idari yaptırımlarla uygulanmaya başlanması, kurumları "saldırı sonrası tepkisel müdahale" anlayışından, yetkisiz erişimleri önlemeye odaklanan önleyici ve katmanlı güvenlik duruşuna geçmeye zorlamıştır.

Ancak yasal ve kurumsal alanda sağlanan bu derinleşmeye rağmen, dönemin tehdit manzarası çok daha karmaşık, organize ve yıkıcı bir boyuta evrilmiştir. Siber saldırılar artık yalnızca basit veri hırsızlığı olmaktan çıkarak; hizmetleri fiilen kullanılamaz hale getiren DDoS saldırıları özellikle 2020 yılında finans sektörünü vuran kesintiler ve sistemleri kilitleyerek operasyonları durduran fidye yazılımları, 2022 yılındaki FinTech saldırıları gibi hibrit tehditlere dönüşmüştür. Nitekim dönemin literatürü incelendiğinde, bu karmaşık saldırıların hedef kurumların sadece finansal yapısını değil, aynı zamanda müşteri güvenini ve kurumsal itibarını da derinden zedelediği görülmektedir.

4.3. III. Dönem (2023-2025): Dirençlilik, Denetim ve Hibrit Tehditler

2023-2025 yıllarını kapsayan güncel dönem, siber güvenliğin yalnızca teknik bir savunma kalkanı olmaktan çıkıp, kurumsal dirençlilik ve stratejik denetim meselesi olarak en üst düzeyde ele alındığı zirve noktasıdır. Özellikle kritik altyapılara yönelik siber tehditlerin ve engellenen zararlı bağlantı girişimlerinin 101.500 gibi çarpıcı rakamları aşması geleneksel savunma hatlarının yetersiz kaldığını kanıtlamıştır(BTK, 2025). Bu tablo karşısında, kurumların yalnızca güvenlik duvarları inşa etmesi yeterli olmamış; bilişim sistemlerinin düzenli olarak test edildiği, uluslararası standartlara uyumun gözetildiği ve zafiyetlerin önceden tespit edildiği siber güvenlik denetimleri operasyonel bir seçenek olmaktan çıkarak hayati bir zorunluluk haline gelmiştir (Kestane, 2025). Tehditlerin özellikle hibritleşen fidye yazılımları ve gelişmiş DDoS saldırılarının geldiği bu karmaşık seviye, kurumları tepkisel güvenlik duruşunu tamamen terk etmeye zorlamıştır.

Bu dönemin en belirgin stratejik dönüşümü, içeriden veya dışarıdan gelen hiçbir erişim talebine peşinen güvenilmemesi esasına dayanan Sıfır Güven mimarisinin benimsenmesi olmuştur. Sıfır Güven yaklaşımı ve en az ayrıcalık prensibi ile kurumlar, yetkisiz erişimleri ve iç tehditleri kaynağında sürekli doğrulayarak engellemeyi, dolayısıyla önleyici ve bütüncül bir savunma ağı kurmayı temel strateji olarak belirlemişlerdir.

Ancak teknolojik altyapı ne kadar güçlü olursa olsun ve siber güvenlik denetimleri ne kadar sıkı uygulanırsa uygulansın, savunma zincirinin en zayıf halkasının insan faktörü olduğu gerçeği değişmemiştir(Aldemir ve Kaya, 2020). Nitekim son yıllarda yapılan bibliyometrik analizler ve literatür çalışmaları incelendiğinde, küresel akademik ilginin geleneksel savunma yöntemlerinden ziyade 'siber güvenlik farkındalığı' ve 'siber fiziksel sistemler' üzerine yoğunlaştığı görülmektedir (Karayel ve Akbıyık, 2023). Ulusal düzeyde üretilen lisansüstü tez çalışmalarında ise siber güvenliğe yönelik ilginin giderek arttığı ve özellikle 2022 yılı itibarıyla zirveye ulaştığı tespit edilmiştir (Sanlı vd., 2024). Bu durum bilgi güvenliği ekosisteminin dönüşümünün sadece teknik yatırımlarla sınırlı kalamayacağını; ulusal ve kurumsal siber dirençliliğin ancak sıfır güven mimarisi, zorunlu siber güvenlik denetimleri ve personelin sürekli eğitimi ile harmanlanmış bütüncül bir modelle sağlanabileceğini ortaya koymaktadır.

5. Siber Tehditlere Karşı Alınan Önlemler, Mevcut Durum ve Çözüm Önerileri

Türkiye'deki siber tehdit profilinin, oltalama gibi basit yöntemlerden, fidye yazılımlarına ve kritik altyapı sabotajlarına kadar genişleyen bir yelpazede ağırlaştığı önceki bölümlerde incelenmiştir. Siber saldırıların bu hibrit ve yıkıcı karakteri; savunma stratejilerinin sadece teknik cihazların kurulumuyla sınırlı kalamayacağını, idari politikalar, yasal düzenlemeler ve denetim mekanizmalarının eş güdümlü çalıştığı bütüncül bir güvenlik mimarisini zorunlu kılmaktadır. Bu bağlamda, Türkiye'de uygulanan mevcut önlemler ve geleceğe yönelik çözüm önerileri üç ana başlık altında değerlendirilmiştir.

5.1. Teknik ve Altyapısal Önlemler

Siber saldırıların teknik boyutuna karşı kurumların aldığı ilk önlem, ağ ve veri güvenliğini sağlayan donanım ve yazılım çözümleridir. Özellikle fidye yazılımlarına karşı şifreleme ve düzenli yedekleme, verinin gizliliğini ve bütünlüğünü koruyan en temel yöntemler olarak uygulanmaktadır. KVKK kapsamında da bir zorunluluk olan şifreleme, verilerin yetkisiz kişilerce okunmasını engellerken; yedeklerin çevrimdışı ortamlarda tutulması, olası bir fidye saldırısında iş sürekliliğini sağlayan en kritik önlem olarak öne çıkmaktadır (Yeniman Yıldırım, 2018). Ağ güvenliği tarafında ise Güvenlik Duvarları, Saldırı Tespit/Önleme Sistemleri (IDS/IPS) ve Web Uygulama Güvenlik Duvarları (WAF), özellikle DDoS ve web tabanlı saldırılara karşı standart savunma hattını oluşturmaktadır (Hatipoğlu ve Tunacan, 2021). Çok Faktörlü Kimlik Doğrulama sistemlerinin yaygınlaşması; kimlik hırsızlıklarının

ve yetkisiz erişim risklerinin minimize edilmesinde en kritik savunma hattı olarak öne çıkmaktadır. (Özker, 2022).

Ancak yalnızca geleneksel ağ trafiğini izlemek ve standart güvenlik duvarları inşa etmek, evrilen karmaşık tehditler karşısında yeterli olmamaktadır. Özellikle e-devlet ve kamu uygulamalarında güvenliğin sağlanması için "Güvenli Yazılım Geliştirme Yaşam Döngüsü" nün benimsenmesi, kodlama aşamasında yapılacak güvenlik testlerinin sonradan çıkacak maliyetli zafiyetleri önlemesi açısından kritik bir çözüm önerisidir (Efe, 2019). Geleneksel savunma hatlarının ötesine geçilmesi gereken günümüz siber ekosisteminde; Nesnelerin İnterneti platformlarının yaygınlaşması ve kritik altyapı tesislerinin kalbini oluşturan SCADA sistemlerinin internete açık kısımlarının iç ağ segmentasyonu ile izole edilmesi hayati önem taşımaktadır (Efe, 2019; Genco, 2020). Ayrıca son dönemde artış gösteren çoklu lokasyon kaynaklı DDoS saldırılarının etkisini kırmak ve hizmet sürekliliğini sağlamak için, geleneksel savunma yöntemleri yerine yapay zekâ destekli önleyici savunma mekanizmalarının ulusal ağ altyapılarına entegre edilmesi gerekmektedir (Öztürk vd., 2025).

5.2. Kurumsal Yönetişim, İnsan Kaynağı ve Eğitim

Teknik altyapı ne kadar güçlü olursa olsun, insan faktörü siber güvenliğin en zayıf halkası olmaya devam etmektedir (Aldemir ve Kaya, 2020). Nitekim yapılan güncel araştırmalar, kurumlarda çalışan personelin yaklaşık %65'inin siber güvenlik konusunda yeterli bilgiye sahip olmadığını ve oltalama gibi sosyal mühendislik saldırılarına karşı son derece savunmasız olduğunu göstermektedir (Yeniman Yıldırım, 2018). Bu zafiyetin giderilmesi için kurumsal düzeyde alınması gereken en temel önlem; bilgi güvenliğini sadece bilgi işlem departmanının bir görevi olarak görmekten çıkarıp, tüm çalışanları kapsayan sürekli bir öğrenme ve farkındalık kültürü yaratmaktır. Bu kültürel dönüşüm; veri yedekleme stratejilerinin standartlaştırılması, personelin şüpheli içerikleri tanıma konusunda düzenli eğitimlere tabi tutulması ve güvenlik politikalarının tavizsiz uygulanması ile mümkündür (Solmaz, 2023).

5.3. Yasal Çerçeve, Denetim ve Sektörel İşbirliği

Ulusal güvenlik stratejisinin sürdürülebilirliği, alınan teknik ve idari önlemlerin yasal regülasyonlar ve düzenli denetimlerle desteklenmesine bağlıdır. Türkiye'de 6698 sayılı KVKK ve BDDK yönergeleri gibi düzenlemeler bu alanda önemli bir zemin oluşturmuştur (Erdem ve Süzen, 2025). Ancak bilgi güvenliği sadece finans ve kamu ile sınırlı değildir; örneğin kritik altyapıların can damarlarından biri olan havacılık ve ulaştırma sektöründe de (Sivil Havacılık Genel Müdürlüğü regülasyonları gibi) Sektörel SOME'ler arası veri paylaşımının ve denetimlerin artırılması zorunludur (Kurnaz ve Karatepe, 2019). Tüm bunlara ek olarak siber suçların sınır aşan doğası gereği, ulusal yasal çerçevenin dinamik tutulması ve siber saldırılara karşı küresel bir refleks geliştirebilmek amacıyla uluslararası örgütlerle, akademik kurumlarla ve özel sektörle kesintisiz bir işbirliği ağı kurulmalıdır (Genco, 2020).

6. Bulgular ve Tartışma

Bu çalışmada, Türkiye'deki bilgi güvenliği ekosisteminin 2015-2025 yılları arasındaki dönüşümü incelenmiş ve "Türkiye'de bilgi güvenliği ve siber güvenlik alanında yapılan çalışmaların evrimi nasıl gerçekleşmiştir?" araştırma sorusu sınanmıştır. Elde edilen dönemsel bulgular (bkz. Tablo 1), Türkiye'de siber güvenlik politikalarının yalnızca teknik bir mesele olmaktan çıkarak; yasal, idari ve mimari boyutları olan üç aşamalı bütüncül bir olgunluk modeline dönüştüğünü kanıtlamaktadır.

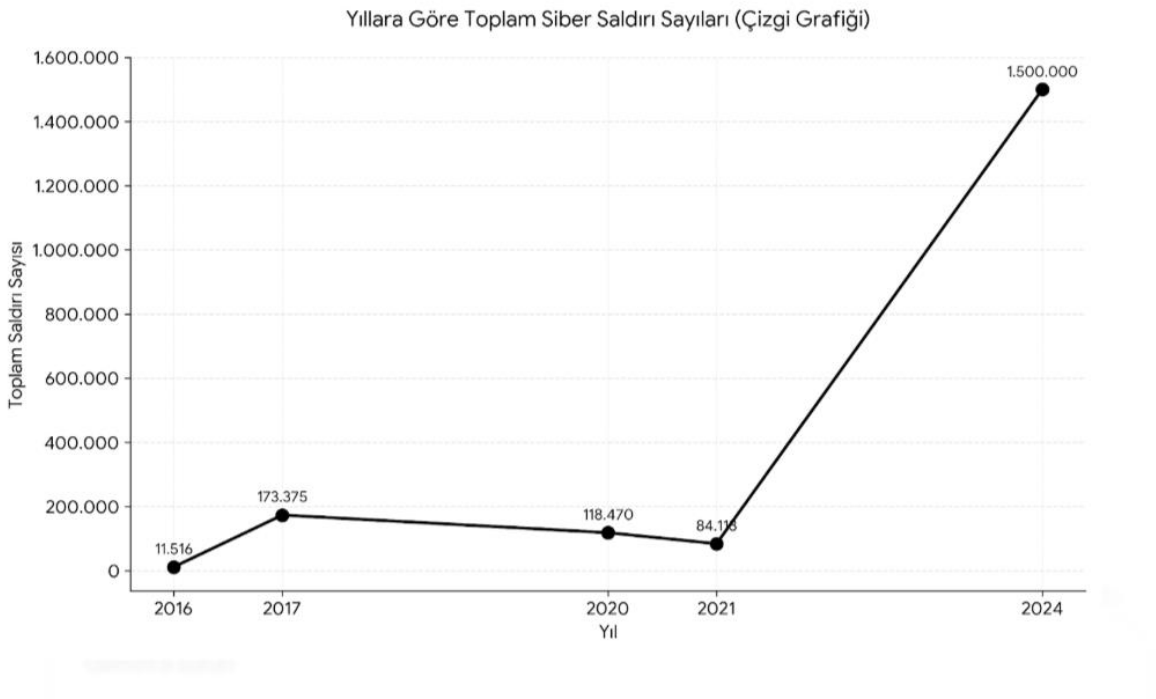
Tablo 1. Türkiye'de Siber Güvenlik Ekosisteminin Dönemsel Evrimi: Saldırı Türleri ve Stratejiler (2015-2025)

Dönem	Öne Çıkan Saldırı Türleri	Savunma Yaklaşımı Odak Noktası
I. Dönem (2015-2018)	Fidye Yazılımları : Türkiye'yi doğrudan etkileyen BadRabbit (2017) saldırıları ve Türkiye'nin fidye yazılımlarında Avrupa'da ilk sıraya yükselmesi. Kritik Altyapı Krizleri: 31 Mart 2015'te 51 ili etkileyen ulusal çaplı büyük elektrik kesintisinin yarattığı altyapı güvenliği tehdidi. Finans Sektörü Saldırıları: Türk bankacılık sistemine (2016-2017) ve TCMB'ye (2018) yönelik kapsamlı organize siber saldırılar. Botnet ve DDoS Saldırıları: Türkiye'nin dünyada en çok botnet tespit edilen ilk 5 ülkeden biri olması (2016) ve Emniyet/Havalimanı sistemlerini kilitleyen DDoS atakları. Oltalama (Phishing) ve Truva Atları: Türkiye'nin hedefli kötücül yazılım ve çevrimiçi bankacılık Truva atı saldırılarında Avrupa'da en çok hedef alınan ülke konumuna gelmesi.	Ulusal Strateji ve Kurumsallaşma: 2016-2019 Ulusal Siber Güvenlik Stratejisi'nin yürürlüğe girmesi; USOM ve SOME'lerin hiyerarşik yapılandırılması. Kritik Altyapıların İlanı: Enerji, finans ve ulaştırma gibi 6 temel sektörün resmen "Kritik Altyapı" ilan edilerek asgari güvenlik standartlarının zorunlu kılınması. Yasal Regülasyonlar: 2016'da 6698 sayılı KVKK'nın yürürlüğe girmesi ve BDDK'nın bilişim denetimlerini sıkılaştırması. Reaktif Savunma: Güvenlik duvarı ve antivirüs kullanımı; fidye yazılımlarına karşı düzenli veri yedekleme ve şifreleme. Farkındalık ve Kapasite: Sosyal mühendislik saldırılarına karşı personel eğitimleri ve ulusal siber savunma tatbikatlarının başlatılması.
II.Dönem (2019-2022)	Hacimsel DDoS Saldırıları: Banka ve telekom altyapılarını (Örn: Türk Telekom, Garanti BBVA) saatlerce kesintiye uğratan devasa saldırılar. FinTech Fidye Yazılımları: Bir Türk dijital cüzdan sistemini kilitleyerek Bitcoin talep eden siber krizler. Devlet Destekli APT Saldırıları: Enerji ve finans altyapılarını hedef alan siber casusluk odaklı (Örn: ChamelGang, SideWinder) sızmalar. Pandemi Temalı Saldırılar: Başta sağlık sektörü olmak üzere kritik altyapıları hedef alan "Koronavirüs" temalı oltalama atakları. Bankacılık Truva Atları: Finansal bilgi hırsızlığı amacıyla kullanıcıları hedef alan Truva atı sızmalarındaki yeniden artış.	Merkezi Yönetişim: CBDDO'nun kuruluşu ve 2020-2023 Ulusal Stratejisi ile üst düzey siber koordinasyon. Önleyici Yaklaşım: Tepkisel yapıdan "Sıfır Güven" ve "Siber Dirençlilik" modeline geçiş. Yapay Zeka Destekli Savunma: Erken müdahale için yerli projeler (AVCI, AZAD, KASIRGA) ve ileri tehdit avcılığı (EDR, SIEM) kullanımı. Sektörel Denetim: BDDK eliyle zorunlu sızma testleri ve API/Açık bankacılık güvenlik standartlarının getirilmesi. Ağ İzolasyonu ve Doğrulama: Bilgi teknolojileri ile operasyonel ağların birbirinden ayrılması ve çok faktörlü kimlik doğrulamanın zorunlu kılınması
III. Dönem (2023-2025)	Kritik Altyapılara Yönelik Gelişmiş Tehditler ve Oltalama: USOM koordinasyonunda engellenen yüz binlerce zararlı bağlantı ve kritik kurumlara yapılan siber güvenlik bildirimleri. Yapay Zeka Destekli Botnetler: Geleneksel savunmaları aşabilen, yapay zekâ ile organize edilmiş karmaşık ve tespiti zor yeni nesil saldırılar. Finansal Kimlik Avı: Doğrudan ödeme sistemlerini hedef alan ve yüz binlerce vakaya ulaşan Truva atı destekli oltalama kampanyaları. API ve Tedarik Zinciri Sızmaları: Açık bankacılık entegrasyonlarının ve üçüncü taraf sağlayıcıların yarattığı yeni zafiyetlerden (giriş noktalarından) faydalanan sızmalar. Web3 ve Blokzinciri Saldırıları: Klasik sistemler dışında, yeni nesil merkeziyetsiz Web3 ve blokzinciri altyapılarını hedef alan ataklar.	Sıfır Güven Mimarisi: Hiçbir erişime peşinen güvenilmeyen ve sürekli doğrulamaya dayanan bütüncül savunma modeline geçiş. Zorunlu Siber Denetimler: Düzenli sızma testleri ve uluslararası standartlara uyum denetimlerinin operasyonel zorunluluk haline gelmesi. Yapay Zeka Destekli Tehdit Avcılığı: Yapay zekâ tabanlı saldırılara karşı; yine yapay zekâ destekli otomatik tespit ve müdahale (EDR/XDR) sistemlerinin kullanımı. Güvenli Yazılım Yaşam Döngüsü: API, Web3 ve bulut zafiyetlerine karşı güvenli yazılım geliştirme süreçlerinin tasarımdan itibaren benimsenmesi. İnsan Faktörü ve Kurum Kültürü: Personelin sosyal mühendisliğe karşı eğitilmesi ve bilgi güvenliğinin kurum kültürüne dönüştürülmesi.

Literatür taramaları ve sektörel raporlar, saldırıların sadece nitelik değiştirmekle kalmayıp, sayısal hacim ve şiddet bakımından da üstel bir büyüme gösterdiğini kanıtlamaktadır. Özellikle 2024 ve 2025 verileri, tehdidin boyutunu gözler önüne sermektedir. Bu sayısal değişim Tablo 2'de, artış eğilimi ise Şekil 3'de sunulmuştur.

Tablo 2. Türkiye'de Tespit Edilen Siber Saldırı Sayıları ve Kritik Artış Oranları (2016-2025)

Yıl	Tespit Edilen Saldırı Sayısı/Oranı	Saldırıların Kapsamı ve Hedefleri
2016	11.516 adet çevrimiçi bankacılık saldırısı (Yılın ilk yarısı) (Trend Micro araştırmasından aktaran: Aslay, 2017)	Türkiye, Avrupa, Ortadoğu ve Afrika'daki tüm zararlı yazılımların %3,4'ünü oluşturmuş; hedefli kötücül yazılım ve online bankacılık saldırılarında Avrupa'da ilk sıraya yerleşmiştir. (Symantec, FireEye ve Trend Micro raporlarından aktaran: Aslay, 2017)
2017	173.375 (Yıllık Tahmini), (Günde ort. 475 saldırı) (Kurnaz ve Karatepe, 2019)	Dünya genelinde çevrimiçi erişimi engellemeye yönelik artan tehditlere paralel olarak, Türkiye'deki genel bilişim ve kritik altyapı sistemleri hedef alınmıştır. (Kurnaz ve Karatepe, 2019)
2020	118.470 adet kayıtlı siber saldırı. (UAB, 2022)	Kovid-19 salgını döneminde iletişim teknolojilerinin ve uzaktan çalışma yöntemlerinin artmasıyla birlikte, ülkedeki kurum ve kuruluşlar yoğun siber saldırıların hedefi olmuştur. Ulaştırma ve Altyapı Bakanlığı'nın (UAB) resmi verilerine göre; bu dönemde kurum sistemlerine sızmak amacıyla özellikle sahte konferans uygulamaları kullanılmış, uzaktan yönetim servislerindeki zafiyetler hedef alınmış ve doğrudan 'Kovid-19' temalı zararlı yazılımlar ile virüsler kullanılarak organize saldırılar gerçekleştirilmiştir (UAB, 2022).
2021	84.113 adet kayıtlı siber saldırı. (UAB, 2022)	Ulaştırma ve Altyapı Bakanlığı verilerine göre genel siber saldırı sayısında bir önceki yıla göre kısmi bir düşüş gözlemlenmiş ancak hedefli saldırılar devam etmiştir. (UAB, 2022)
2022	Nesnelerin İnterneti cihazlarına yönelik 27 milyondan fazla saldırı. (Kaspersky, 2023)	Elektrik ve su sistemleri gibi akıllı şehir altyapı bileşenleri yoğun şekilde hedef alınmış; bankacılık Truva atı saldırılarında ise bir önceki çeyreğe göre %11 artış yaşanmıştır. (Kaspersky, 2023)
2023	Finans sektörü tehditlerinde %43, oltalama saldırılarında %47 artış. (Kaspersky, 2023)	Finans kuruluşları ve ödeme sistemleri öncelikli hedef olmuş; bu doğrultuda oltalama gibi sosyal mühendislik saldırıları ivme kazanmıştır. (Kaspersky, 2023)
2024	Toplamda yaklaşık 1,5 milyon siber saldırı (Erdem ve Süzen, 2025).	Finans sektörü başta olmak üzere Türkiye dünyada en çok hedef alınan ilk 12 ülke arasına girmiş; saldırılar uzun süreli, karmaşık ve tespiti zor bir karaktere bürünmüştür. (Erdem ve Süzen, 2025).
2025	2025 yılı sonu itibarıyla USOM koordinasyonunda 101.500'ün üzerinde zararlı bağlantı erişime kapatılmış, 6.805 adet siber güvenlik bildirimi kritik kurumlarla paylaşılmıştır (BTK, 2025).	Saldırıların kapsamı ağırlıklı olarak oltalama, zararlı yazılım yayılması ve alan adı kötüye kullanımına odaklanmıştır. Bireysel kullanıcılardan ziyade ülkenin bilişim sistemleri ve doğrudan hizmet sunan kritik kurumları hedef alınmıştır. Bu hedefli saldırılara karşı 14 Sektörel SOME, 2.401 Kurumsal SOME ve sahada görev yapan 8.393 siber güvenlik uzmanı ile ulusal bir savunma kalkanı oluşturulmuş; TRABİS sisteminin de faaliyete geçmesiyle zararlı alan adları henüz tehdit oluşturmadan önleyici şekilde engellenmiştir(BTK, 2025).



Şekil 3. Türkiye'de Siber Saldırıların Sayısal Artış Eğilimi (2016-2024)

Tablo 1'de özetlenen literatürdeki ve sahadaki bu dönemsel evrim, resmi istatistiklere ve kurumsal veri akışına da doğrudan yansımaktadır. Nitekim sayısal eğilimleri Tablo 2'de detaylandırıldığı üzere, T.C. Ulaştırma ve Altyapı Bakanlığı (UAB, 2022) verilerine göre 2020 yılında 118.470 olarak raporlanan toplam siber olay sayısı, 2021 yılında 84.113 adet düzeyine gerilemiştir. Bu süreçte riskleri henüz ortaya çıkmadan engellemeyi amaçlayan denetim mekanizmaları ile önleyici tedbirlere ağırlık verilmiştir. Keza, Bilgi Teknolojileri ve İletişim Kurumu (BTK, 2022: 104-106) verileri incelendiğinde; USOM kanalıyla 2021 yılında 36.761 zararlı bağlantının engellendiği, kurumlara zafiyetler için 11.656 adet bildirim yapıldığı ve AVCI, AZAD, KASIRGA gibi yerli yazılımlarla uzaktan yönetim servislerinde 46.784 adet açıklığın henüz bir saldırıya zemin hazırlamadan tespit edildiği görülmektedir.

Söz konusu kurumsal ve teknik dinamizm, akademik çalışmalara da doğrudan yansımıştır. Çalışmanın bulguları mevcut literatürle karşılaştırıldığında, Türkiye'de ve küresel çapta yapılan güncel bibliyometrik analizler, siber güvenlik araştırmalarının son yıllarda üstel bir artış gösterdiğini ve özellikle 2022 yılı itibarıyla zirveye ulaştığını ortaya koymaktadır (Sanlı vd., 2024). Önceleri yalnızca ağ güvenliği ve kriptografi gibi tamamen donanımsal ve teknik konulara odaklanan akademik ilgi, günümüzde siber fiziksel sistemler, siber güvenlik farkındalığı ve insan faktörü gibi daha bütüncül ve sosyal alanlara kaymıştır (Karayel ve Akbıyık, 2023). Bu durum, siber tehditlerin artık sadece teknolojik bir sorun olarak değil, kurumsal kültür ve yönetişim ekseninde disiplinlerarası bir kriz olarak algılandığını kanıtlamaktadır (Aldemir ve Kaya, 2020).

Bu çalışmanın mevcut literatüre sunduğu en belirgin orijinal katkı; Türkiye'nin siber güvenlik ekosistemini belirli saldırı türlerinin veya izole edilmiş yılların ötesinde, yapılandırılmış on yıllık bir "makro-dönüşüm modeli" olarak kavramsallaştırmasıdır. Öte yandan, tartışılması gereken bir diğer kritik bulgu, Nesnelerin İnterneti, 5G ve bulut bilişim gibi yeni nesil teknolojilerin yaygınlaşmasıyla birlikte siber tehdit yüzeyinin kontrol edilemez bir biçimde genişlemesidir (Özker, 2022). Uluslararası siber güvenlik kurumu Kaspersky'nin resmi tehdit istihbaratı verilerinde de görüldüğü üzere, sadece 2022 yılında Türkiye'deki nesnelerin interneti cihazlarına yönelik 27 milyondan fazla siber saldırı tespit

edilmiştir (Kaspersky, 2023). Elektrik ve su sistemleri gibi akıllı şehir altyapı bileşenlerinin yoğun şekilde hedef alındığı bu dönemde, bankacılık Truva atı saldırılarında ise bir önceki çeyreğe göre %11 oranında bir artış yaşanmıştır. Özellikle enerji ve su yönetimi gibi kritik altyapı tesislerinin kalbini oluşturan SCADA sistemlerinin internete açık hale gelmesi, bu sistemleri doğrudan hedef tahtasına oturtmaktadır. Bu nedenle, geleneksel sınır güvenliği yaklaşımı yerine, kurumların iç ağlarını izole etmeleri ve hiçbir cihaza veya kullanıcıya peşinen güvenmeyen Sıfır Güven mimarisine geçiş yapmaları artık teknik bir tavsiye değil, siber dirençliliğin sürdürülebilirliği için hayati bir zorunluluktur.

7. Sonuç

Dijitalleşmenin ve bilgi teknolojilerinin hayatın her alanına entegre olması, bilgi güvenliğini yalnızca teknik bir altyapı meselesi olmaktan çıkarıp, devletlerin ve kurumların bekasını doğrudan ilgilendiren stratejik bir ulusal güvenlik unsuruna dönüştürmüştür. Bu çalışmada, Türkiye'nin bilgi güvenliği ekosisteminin 2015-2025 yılları arasındaki on yıllık dönüşümü incelenmiş; siber tehditlerin basit bireysel saldırılardan, organize, yapay zekâ destekli ve kritik altyapıları hedef alan yıkıcı boyutlara nasıl ulaştığı verilerle ortaya konulmuştur.

Elde edilen bulgular, siber saldırıların hacminde ve karmaşıklığında yaşanan katlanarak artışı açıkça göstermektedir. Özellikle Nesnelerin İnterneti cihazlarına yönelik ulaşılan devasa saldırı hacimleri ve günümüz itibarıyla USOM koordinasyonunda engellenen zararlı bağlantı sayısının her yıl yüz binleri aşması, mevcut güvenlik anlayışının sorgulanmasını zorunlu kılmıştır. Bu veriler ışığında, siber uzayda mutlak korunmanın mümkün olmadığı ve yalnızca güvenlik duvarı gibi sınır güvenliğine dayalı tepkisel önlemlerin tek başına yeterli olamayacağı net bir şekilde anlaşılmıştır.

Bu nedenle, Türkiye'nin ve kurumların siber güvenlik vizyonu; saldırı gerçekleştiğinde tepki veren tepkisel bir yapıdan, tehditleri önceden öngören, iç ağları izole eden ve hiçbir erişime peşinen güvenmeyen Sıfır Güven mimarisinin merkeze alındığı önleyici bir modele evrilmek zorundadır. Günümüzde kurumlar ve devletler için temel hedef, siber saldırıları tamamen sıfırlamak değil, siber dirençlilik kapasitesini artırarak sistemlerin saldırı anında dahi asgari düzeyde hizmet vermesini sağlamak ve riskleri yönetilebilir bir seviyede tutmaktır.

Ancak teknolojik altyapılar ne kadar ileri seviyede olursa olsun, yasal düzenlemeler ne kadar sıkılaştırılırsa sıkılaştırılsın, siber güvenlik sürecinin en zayıf halkası 'insan unsuru' olmaya devam etmektedir. Bu dirençliliğin sürdürülebilirliği; çalışanların kurumsal bir farkındalık kültürü içerisinde sürekli eğitilmesi, uluslararası standartlara uyumu düzenli olarak denetleyen 'siber güvenlik denetimlerinin' kurumsallaşması ve tüm bu süreçlerin bütüncül bir savunma modeliyle entegre edilmesi ile mümkündür.

Sonuç olarak; bilgi güvenliği ekosisteminin inşası, kurumlar için maliyetli bir bilişim gideri olarak değil, kurumsal sürdürülebilirliğin, ekonomik istikrarın ve ulusal egemenliğin en temel güvencesi olarak değerlendirilmelidir. Türkiye'nin dijital çağdaki siber bağımsızlığı, ancak teknik, idari ve insani unsurların kusursuz bir uyumla çalıştığı bu dirençlilik modelinin tavizsiz bir şekilde uygulanmasıyla teminat altına alınabilir.

Kaynakça

AFAD. (2014). Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Ankara: T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı

Akseki, B., Meydaneri, S. ve Taşdemir, C. (2023). Türkiye'de siber güvenlik ve bilgi güvenliği çalışmaları. *International Social Mentality and Researcher Thinkers Journal*, 9(73), 3902–3909. https://doi.org/10.29228/smryj.70755

Aldemir, C. ve Kaya, M. (2020). Bilgi toplumu, siber güvenlik ve Türkiye uygulamaları. *Kamu Yönetimi ve Politikaları Dergisi,* 1(1), 6–27.

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

Aydın, H. (2023). Yönetim Bilgi Sistemlerinde (YBS) Siber Güvenliğin Önemi. *Bilgisayar Bilimleri ve Teknolojileri Dergisi,* 3(2), 38-45. https://doi.org/10.54047/bibted.1138252

Aydın, İ. (2012). Bilişim sektörü ve Türkiye'nin sektördeki potansiyeli. *International Journal of New Trends in Arts, Sports & Science Education (IJTASE) ISSN: 2146-9466*, *1*(1), 180-200.

Aydınbaş, G. (2023). Bilişim Teknolojileri ve Türkiye Ekonomisindeki Yeri Üzerine Bir İnceleme. *Uluslararası Sosyal Siyasal ve Mali Araştırmalar Dergisi*, *3*(1), 18-32.

Bilgi Teknolojileri ve İletişim Kurumu (BTK). (2022). *2021 Yılı İdare Faaliyet Raporu*. Siber Güvenlik, Şebeke ve Bilgi Güvenliği Faaliyetleri (s. 104-106). Bilgi Teknolojileri ve İletişim Kurumu Yayınları, Ankara.

Bilgi Teknolojileri ve İletişim Kurumu (BTK). (2024). *2024 Yılı Faaliyet Raporu*. Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, Ankara.

Bilgi Teknolojileri ve İletişim Kurumu (BTK). (2025). *2025 Yılı Faaliyet Raporu*. Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, Ankara.

Can, A. (2022). Ulusal güvenlik açısından kritik altyapı ve siber alan: Sivil hazırlıklılık ve dirençlilik perspektifinden kavramsal bir inceleme. *Diplomasi ve Strateji Dergisi*, 3(2), 279–311.

Damar, M. (2022). Dijital Dünyanın Dünü, Bugünü Ve Yarını: Bilişim Sektörünün Gelişimi Üzerine Değerlendirme. *Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi*, 12(Dijitalleşme), 51-76. https://doi.org/10.30783/nevsosbilen.1121818

Efe, A. (2019). E-devlet tehditlerine yönelik BT güvenlik trendleri. *Uluslararası Disiplinlerarası Çalışmalar ve Yenilikçi Teknolojiler Dergisi*, 3(2), 105–110.

Erdem, M. ve Süzen, A. A. (2025). Türkiye'de finans sektöründe siber güvenlik: Tehditler, aktörler ve savunma stratejileri. *Yalvaç Akademi Dergisi*, 10(2), 1–23.

Genco, A. (2020). Türkiye'de kritik altyapı ve kritik altyapıya yönelik tehditler. *KAYTEK Kamu Yönetimi ve Teknoloji Dergisi*, 2(2), 38–46.

Hatipoğlu, C. ve Tunacan, T. (2021). Türkiye'de siber saldırı ve tespit yöntemleri: Bir literatür taraması. BŞEÜ *Fen Bilimleri Dergisi,* 8(1), 430–445. https://doi.org/10.35193/bseufbd.838732

C. H. Hur, S. -P. Kim, Y. -S. Kim and J. -H. Eom, "Changes of Cyber-Attacks Techniques and Patterns after the Fourth Industrial Revolution," *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Prague, Czech Republic, 2017, pp. 69-74, doi: 10.1109/FiCloudW.2017.79.

Kaspersky. (2023). *Kaspersky Security Bulletin: Cyberthreats and IoT Vulnerabilities İntelligence Report*. Kaspersky Labs.

Karayel, T. ve Akbıyık, A. (2023). Siber güvenlik araştırmalarına küresel bir bakış: Yayın trendleri ve araştırma yönelimleri. *Gazi Üniversitesi Bilişim Teknolojileri Dergisi,* 16(3), 283–296. https://doi.org/10.17671/gazibtd.1291783

Kestane, Ö. (2025). Siber saldırılar ve siber güvenlik denetimi gereksinimi. İzmir Serbest Muhasebeci *Mali Müşavirler Dayanışma Dergisi*, 8(1), 41–49. https://doi.org/10.69599/izd.2746

Kindervag, J. (2010, September 14). *No more chewy centers: Introducing the Zero Trust Model of information security* (Forrester Report). Forrester Research.

Kindervag, J. (2010, November 5). *Integrate security into your network's DNA: The Zero Trust Network architecture* (Forrester Report). Forrester Research.

Kurnaz, S. ve Karatepe, S. (2019). Kritik alt yapıların güvenliği kapsamında Türkiye'deki hava alanlarının siber güvenliği. Havacılık ve Uzay Çalışmaları Dergisi, (Özel Sayı), 75–92.

Özdemirci, F. ve Torunlar, M. (2018). Bilgi-değişim-siber güvenlik-bağımsızlık. *Bilgi Yönetimi Dergisi, 1*(1), 78-83

Özker, U. (2022). Türkiye'de kritik altyapı ve siber güvenlik. EDAM & Konrad-Adenauer-Stiftung.

Öztürk, D., Aktolun, A., Emektar, M. ve Harmancı, F. M. (2025). Dağıtık siber saldırıların internet hizmetlerinin kullanılabilirliği üzerindeki etkisi: DDoSphere ile deneysel bir analiz. Alfa Mühendislik ve Uygulamalı Bilimler Dergisi, 3(1), 35–50. https://doi.org/10.70988/ajeas.1628985

Resmî Gazete. (2013, 20 Haziran). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm

Sanlı, Y. B., Baltacı, F., Güven, E. ve Eren, T. (2024). Siber güvenlik çalışmaları üzerine bibliyometrik analiz. Gazi Üniversitesi Bilişim Teknolojileri Dergisi, 17(3), 223–229. https://doi.org/10.17671/gazibtd.1473206

Solmaz, S. B. (2023). Siber güvenlik tarihindeki dönüm noktaları: Tehditlerin evrimi ve savunma stratejileri. Siber Güvenlik ve Savunma Dergisi, 1(1), 1–15.

T.C. Ulaştırma ve Altyapı Bakanlığı. (2022, 27 Şubat). *Ulaştırma ve Altyapı Bakanı Karaismailoğlu: Siber kalkan güçlendi, saldırı sayısı azaldı*. Strateji Geliştirme Başkanlığı Haberleri. https://sgb.uab.gov.tr/haberler/ulastirma-ve-altyapi-bakani-karaismailoglu-siber-kalkan-guclendi-saldiri-sayisi-azaldi

Ulaştırma ve Altyapı Bakanlığı (UAB). (2020). 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. Ankara http://www.sp.gov.tr/upload/xSPTemelBelge/files/HwolM+ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB). (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi*. Ankara https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf)

Ulusal Siber Olaylara Müdahale Merkezi (USOM). (2014). *Sektörel SOME Kurulum ve Yönetim Rehberi*. Erişim adresi: https://www.usom.gov.tr/dosya/1470335484-Sektorel%20SOME%20Rehberi.pdf

Ünver, M. (2015). Türkiye'de siber güvenlik. Bilgi Güvenliği Derneği Yayınları.

Yeniman Yıldırım, E. (2018). Bilişim sistemlerine yönelik siber saldırılar ve siber güvenliğin sağlanması. 2. Uluslararası Mesleki Bilimler Sempozyumu (IVSS 2018) bildiri kitabı içinde (s. 494–503). Mesleki Bilimler Dergisi.