Studies on Social Science Insights
Yıl: 2024, Cilt: 4, Sayı: 2, ss.70-95
http://dx.doi.org/10.53035/SOSSCI.88

Siber Güvenliğin Kalkınma Planları Bağlamında İncelenmesi: Nitel Bir İçerik Analizi

Examining Cyber Security in the Context of Development Plans: A Qualitative Content Analysis

Çalışma Başvuru Tarihi: 21.08.2024
Çalışma Kabul Tarihi: 31.08.2024
Çalışma Türü: Araştırma Makalesi

Hilmi SÖZEN*

Anahtar Kelimeler:

Güvenlik, Teknoloji, Dijitalleşme, Siber Güvenlik, Kalkınma Planı.

ÖZET

Güvenlik, insanlık tarihinin her döneminde temel bir kaygı unsuru olarak varlığını sürdürmüştür. Uluslararası ilişkilerden bilgi teknolojilerinin evrimine kadar geniş bir spektrumda, güvenlik kavramı, disiplinlerarası bir inceleme konusu olarak önem kazanmıştır. Günümüzde, siber tehditlerin artışı ve teknolojinin geniş çapta benimsenmesi gibi dinamikler, güvenlik stratejilerini daha kapsamlı bir biçimde değerlendirme gerekliliğini doğurmuştur. Dijitalleşmenin artmasıyla birlikte, siber güvenlik; ekonomik, sosyal ve politik kalkınmayı etkileyen kritik bir unsur haline gelmiştir. Bu bağlamda, siber güvenlik stratejilerinin, ulusal kalkınma planları ile entegrasyonu büyük bir önem taşımaktadır. Bu çalışmanın temel amacı, Türkiye'nin Beş Yıllık Kalkınma Planları bağlamında siber güvenlik konusunun ele alınış biçimini sistematik bir yaklaşımla analiz etmek ve değerlendirmektir. Bu çalışma kapsamında, Türkiye'nin sekizinci, dokuzuncu, onuncu, on birinci ve on ikinci kalkınma planları detaylı bir şekilde incelenmiştir. Bu çalışmada, nitel araştırma yöntemi kullanılarak verilerin toplanması doküman analizi tekniğiyle gerçekleştirilmiş; elde edilen veriler içerik analizine tabi tutularak, kalkınma planlarında siber güvenlik konusunun nasıl yer aldığı, hangi temalar etrafında şekillendiği ve zaman içerisinde nasıl bir evrim geçirdiği irdelenmiştir. Araştırmanın bulguları, siber güvenlik temasının kalkınma planlarında giderek artan bir öneme sahip olduğunu ortaya koymaktadır. Özellikle son iki kalkınma planında, siber güvenlik teriminin kullanım sıklığında belirgin bir artış gözlemlenmiştir. Bulgular, siber güvenliğin kalkınma politikalarındaki rolünü açığa çıkararak, gelecekteki planlar için önemli ipuçları sunmaktadır.

Keywords:

Security, Technology, Digitalization, Cyber Security, Development Plan

ABSTRACT

Security has remained a fundamental concern throughout human history. From international relations to the evolution of information technologies, the concept of security has gained importance as an interdisciplinary subject of study. Today, dynamics such as the increase in cyber threats and the widespread adoption of technology have led to the need to evaluate security strategies in a more comprehensive manner. With increasing digitalization, cybersecurity has become a critical element affecting economic, social and political development. In this context, the integration of cybersecurity strategies with national development plans is of great importance. The main purpose of this study is to analyze and evaluate the way cybersecurity is addressed in the context of Turkey's Five-Year Development Plans with a systematic approach. Within the scope of this study, Turkey's eighth, ninth, tenth, eleventh and twelfth development plans were analyzed in detail. In this study, the qualitative research method was used to collect data through document analysis, and the data obtained were subjected to content analysis to examine how the issue of cyber security was included in the development plans, around which themes it was shaped and how it evolved over time. The findings of the study reveal that the theme of cybersecurity has an increasing importance in development plans. Especially in the last two development plans, there has been a significant increase in the frequency of use of the term cybersecurity. The findings reveal the role of cybersecurity in development policies and provide important clues for future plans.

* Dr., Bağımsız Yazar, Selçuk Üniversitesi, hilmiszn42@hotmail.com, ORCID: 0009-0004-7038-8941.

1. GİRİŞ

Güvenlik kavramının tanımı üzerine yapılan tartışmalar, uluslararası ilişkiler teorisinde önemli bir yer tutmaktadır. Arnold Wolfers, güvenlik kavramını, edinilmiş değerlere karşı tehditlerin olmadığı bir durum olarak tanımlamıştır. Fakat Baldwin, Wolfers'ın bu tanımını, özellikle 'tehditlerin yokluğu' kısmı bakımından, muğlak bulmuştur. Bu nedenle Baldwin, tanımı 'edinilmiş değerlere zarar verme ihtimalinin az olduğu' şeklinde daha net bir ifadeyle yeniden formüle etmiştir (Yakubu and Shuaibu, 2016: 5). Bu değişen tanımlar, güvenlik kavramının esasını anlamak ve modern çağın karmaşık tehditlerine daha etkin bir biçimde yanıt verebilmek açısından kritik bir öneme sahiptir. Bu temel kavram, bireylerin ve toplumların hayati öneme sahip güvencelerini sağlarken, aynı zamanda devletin varoluşunun temel dayanaklarından biri olarak değerlendirilmektedir. Bu sebepten ötürü, insan hayatının merkezinde yer alan güvenlik, insanlık tarihi boyunca dikkat çekici bir dinamizme sahip olan, sürekli evrilen ve değişen sosyo-politik bir fenomendir. Bu bağlamda, ilk çağlardan günümüze kadar, tehditlerin ve korunma ihtiyaçlarının evrimiyle birlikte, güvenliğin niteliği ve uygulanma şekli dönemsel olarak muazzam bir gelişim göstererek önemini her zaman korumuştur (Birdişli, 2020: 235).

Siber güvenlik, günümüzün dijital çağında, ulusal güvenliğin muhafazasında hayati bir rol oynayan, stratejik bir öneme sahip bir disiplin olarak kendini göstermektedir. Teknolojinin hızla gelişmesi ve dijitalleşmenin yaygınlaşması, bireylerin, kurumların ve devletlerin siber tehditlere karşı daha savunmasız hale gelmesine yol açmıştır. Bu bağlamda, siber güvenliğin stratejik bir öncelik olarak belirlenmesi, ulusal kalkınma planlarının ayrılmaz bir parçası haline gelmiştir. Türkiye, son yıllarda siber güvenlik alanında önemli adımlar atarak, bu konudaki politikalarını güçlendirmeyi hedeflemiştir. Bu çalışma, Türkiye'nin ekonomik kalkınma stratejileri içerisinde siber güvenlik unsurlarının rolünü ve önemini derinlemesine incelemeyi ve bu bağlamda geniş bir analitik çerçeve geliştirmeyi amaçlamaktadır. Siber güvenlik, ulusal güvenlikten ticarete, eğitimden sağlığa kadar birçok alanda giderek artan bir etkiye sahip olduğundan, bu konunun kalkınma politikaları ile entegrasyonu kritik bir öneme sahiptir. Çalışmanın temel bileşenleri şunlardır:

❖ Kapsamlı İnceleme: Araştırma, Türkiye'nin beş yıllık kalkınma planlarını sistematik bir şekilde inceleyerek, siber güvenlik teriminin bu belgelerde ne sıklıkla yer aldığını belirleyecektir. Bu, siber güvenliğin zamanla nasıl bir öncelik kazandığını ve bu alandaki politikaların nasıl evrildiğini anlamak için kritik bir adımdır.

❖ Nitel Araştırma Yöntemi: Araştırma, nitel araştırma yöntemi benimseyerek, siber güvenlik kavramının derinlemesine analizini yapmayı amaçlamaktadır. Bu yöntem, sayısal verilerin ötesine geçerek, siber güvenliğin kalkınma planlarındaki yerini ve önemini daha iyi kavrayabilmek için bağlamı ve içerikleri incelemeye olanak tanır.

❖ Sistematik Analiz: Araştırma, Türkiye'nin 8., 9., 10., 11. ve 12. beş yıllık kalkınma planlarını detaylı bir şekilde inceleyecek. Bu inceleme, her bir planın metninde "siber güvenlik" teriminin geçip geçmediğini, hangi bağlamlarda kullanıldığını ve ne sıklıkla tekrarlandığını belirlemek için yapılacaktır.

❖ Zaman İçindeki Değişim: Araştırma, siber güvenliğin zaman içindeki önemini değerlendirerek, bu kavramın Türkiye'nin kalkınma politikalarındaki yerinin nasıl değiştiğini ortaya koymayı hedeflemektedir. Bu, siber güvenliğin ulusal güvenlik, ekonomik kalkınma ve toplumsal istikrar açısından ne kadar kritik bir alan haline geldiğini anlamak için önemlidir.

❖ Politikaların Evrimi: Çalışma, siber güvenlik alanındaki politikaların evrimini inceleyerek, Türkiye'nin bu alandaki stratejik yaklaşımını ve uygulamalarını değerlendirecektir. Bu, siber güvenlik konusundaki farkındalığın ve stratejilerin nasıl geliştiğini anlamak için önemli bir perspektif sunar.

Sonuç olarak, bu çalışma, Türkiye'nin kalkınma planlarında siber güvenliğin yerini ve önemini derinlemesine inceleyerek, bu alandaki politikaların gelişimini ve ulusal güvenlik açısından taşıdığı önemi daha iyi anlamayı amaçlamaktadır. Bu tür bir analiz, gelecekteki stratejilerin şekillendirilmesine ve siber güvenlik alanındaki politikaların güçlendirilmesine katkıda bulunabilir.

2. KAVRAMSAL AÇIDAN SİBER GÜVENLİK

Güvenlik fenomeni, insanlık tarihinin başlangıcından bu yana, toplumların varlığını ve gelişimini şekillendiren kritik bir faktör olarak ön plana çıkmıştır. Ancak, bu kavramın bilimsel olarak ele alınıp derinlemesine incelenmesi ve özel çalışmaların yapılması oldukça yeni bir olgudur. İlk olarak uluslararası ilişkiler alanında çalışma konusu olan güvenlik, zamanla diğer disiplinlerin de dikkatini çeken ve inceleme konularından biri haline gelen önemli bir odak noktası haline gelmiştir. Bu süreç, güvenliğin giderek daha geniş bir perspektifle ele alındığını ve öneminin arttığını göstermektedir. İlgili kavram, tarihsel süreç içerisinde çağın özgül koşullarının bir yansıması olarak, çeşitli ve evrimsel biçimlerde tanımlanma sürecinden geçmiştir. Zaman, kişi, grup ve devlet bazında değişen bu tanımlar, güvenliğin "esası tartışılan" bir kavram olmasına yol açmıştır. Bu durum, güvenliğin anlamının sürekli olarak yeniden değerlendirildiği ve farklı bağlamlarda değişkenlik

gösterdiği anlamına gelmektedir (Çakır ve Arınmış Uzun, 2021: 355). "Güvenlik" kelimesi, Oxford İngilizce Sözlüğü'nün çevrimiçi versiyonunda sadece yüzeysel bir şekilde tanımlanmış olup, "tehlike veya tehditten uzak olma durumu" olarak özetlenmektedir (Bay, 2016: 4). Benzer şekilde, güvenlik, temel olarak korku, tehlike ve tehditlerden korunma veya kendini güvende hissetme durumu olarak açıklanmaktadır. Bu tanımlar, güvenliğin yalnızca fiziksel bir olgu olmadığını, aynı zamanda psikolojik bir boyutu da içerdiğini ortaya koymaktadır. Öte yandan, güvenlik kavramının öznelerin algısına ve nesnel koşullara bağlı olduğu ve bu yönüyle farklı kişiler tarafından farklı şekillerde değerlendirilebileceği de vurgulanmaktadır. Dolayısıyla, güvenlik kavramı, zihinsel ve fiziksel süreçlere odaklanan, kişiden kişiye değişebilen bir yapıya sahiptir (Ak, 2013: 9). Ancak, özellikle siber güvenlik bağlamında, bu tanımlar, kelimenin gerçek kullanımının karmaşıklığını göz ardı etmektedir (Bay, 2016: 4). Kamu medyasında son zamanlarda artan ilgiye rağmen, siber güvenlik konusu yeni değildir; neredeyse yirmi yıldır hükümet, endüstri ve akademik çevreler arasında ciddi tartışmaların odağında yer almaktadır (Rowe vd., 2011: 113). 1990'lı yıllarda bilgisayar mühendisleri tarafından geliştirilen terim olan "siber güvenlik", ağa bağlı bilgisayarlar ile ilişkili güvenlik sorunlarını ifade etmektedir (Öğün ve Kaya, 2013: 163).

‘Siber güvenlik’, geniş bir şekilde kullanılan bir terim olup, tanımları oldukça değişken, sıklıkla öznel ve bazen bilgi verici olmayan bir niteliğe sahiptir. Bu bağlamda, siber güvenliğin kapsamlı ve çok yönlü yapısını tam olarak ifade eden standart bir tanım mevcut değildir (Craigen vd., 2014: 13-18; Schatz vd., 2017: 55-56; Fischer, 2016: 1). Başka bir deyişle, söz konusu terim, siyasetçilerden bilgisayar uzmanlarına, BT yöneticilerinden teknoloji girişimcilerine, sağlık sektörü profesyonellerinden ulusal güvenlik operatörlerine kadar geniş bir yelpazede sürekli olarak kullanılmaktadır. Ancak, bu kadar geniş bir kesimin bir tanım konusunda anlaşması neredeyse imkânsız gibi görünmektedir. Farklı bakış açıları ve sektörler arasındaki çeşitlilik, siber güvenliğin tanımı konusunda çeşitli görüşlerin olduğunu işaret etmektedir (Bay, 2016: 4).

Öncelikle belirtilmelidir ki, "siber" ön eki, elektronik ve bilgisayar tabanlı teknolojiyi temsil etmektedir. Bu kelime, günümüzün dijital çağında sıkça kullanılan ve teknolojinin sürekli gelişimiyle birlikte önemi artan bir kavramı işaret etmektedir (Maurer, 2011: 8). Genel olarak bu sözcük, dilbilim alanında, bilgisayar veya bilgisayar ağlarıyla ilişkilendirilen bir kavram olup, genellikle sanal varlıkları tanımlamak amacıyla kullanılan bir terimdir. Bu kavram, dil bilimi açısından incelendiğinde, İngilizce kökenli "cyber" kelimesine gönderme yaparak, genellikle "bilgisayar ağlarına ait olan", "internete ilişkin" ve "sanal gerçeklik" gibi

anlamlarda kullanılır. Günümüzde, bilişim ve iletişim ağlarının oluşturduğu dijital alanı ifade eden "siber" kavramı oldukça karmaşık bir yapıya sahiptir (Çakır ve Arınmış Uzun, 2021: 357).

Bu ön ekten yola çıkarak siber güvenlik, genel anlamda, bir kuruluşa ait olan veya başka bir kuruluşun ağına bağlanan bilgi işlem varlıklarının bütünlüğünü, gizliliğini ve kullanılabilirliğini korumayı amaçlayan bir disiplin olarak belirtilmektedir (Kaur and Ramkumar, 2022: 5767). Uluslararası Telekomünikasyon Birliği'nin siber güvenlik tanımı, kurumların, kuruluşların ve kullanıcıların siber alandaki varlıklarını korumak için kullanılan araçları, politikaları, güvenlik kavramlarını ve teminatları, kılavuzları, risk yönetimi yaklaşımlarını, faaliyetleri ile uygulamaları içeren bir teknoloji bütününü ifade etmektedir (Karasoy ve Babaoğlu, 2021: 129-130). Bu tanım, siber güvenliğin yalnızca teknik önlemleri değil, aynı zamanda politikaları, yönetim yaklaşımlarını ve pratik uygulamaları da kapsadığını vurgulamaktadır. Bir diğer tanımda ise siber güvenlik, bilgi ve bilgi sistemlerini (ağlar, bilgisayarlar, veri tabanları, veri merkezleri ve uygulamaları) uygun prosedürel ve teknolojik güvenlik önlemleriyle koruma faaliyeti olarak açıklanmaktadır (Tonge vd., 2013: 67). Bilimsel bir perspektiften siber güvenlik, "siber uzayı ve siber uzay destekli sistemleri, hukuki olarak fiili mülkiyet haklarından farklı kılan olaylardan korumak için kullanılan kaynakların, süreçlerin ve yapıların organizasyonu ve toplanması" olarak tanımlanmaktadır. Bu kapsamlı tanım, geniş bir yelpazede etkili olmayı ve yasal bir dayanağa sahip olmayı amaçlamaktadır (Bay, 2016: 5). Bu tanımlamalardan hareketle, siber güvenliğin temel hedefi, çalınan veya ortak çalışmaya dayalı verilerin korunmasıdır. Bu hedefe ulaşmak için, siber güvenliğin üç ana amacına odaklanılmaktadır. İlk olarak, bilgilerin gizliliğini korumak önemlidir. İkincisi, bilginin bütünlüğünün korunması esastır. Son olarak, bilgiye erişimi sağlamak ve hizmetlerin kullanılabilirliğini garanti etmek önemlidir. Bu üç hedef, siber güvenliğin kapsamlı bir yaklaşımının temelini oluşturmaktadır (Vijaykumar Dalave vd., 2022: 1372).

3. KALKINMA PLANLARINDA SİBER GÜVENLİK

İnsanlık tarihi boyunca, yaşam kalitesinin artırılması ve bu iyileşmenin sürdürülebilir olması amacıyla, ihtiyaçlar doğrultusunda kesintisiz bir gelişim ve yenilenme dinamiği çerçevesinde çeşitli çalışmalar gerçekleştirilmiştir. Her toplum, tarihsel süreç içerisinde farklı ihtiyaçlar geliştirmiştir; bu ihtiyaçlar, toplumların kırsal ya da kentsel oluşundan bağımsız olarak evrensel bir etkileşim içindedir. Bu bağlamda, kalkınma, toplumların bu değişim sürecine adaptasyonunu ve dönüşümünü ifade eden, dinamik ve sürekli evrilen bir kavram olarak ele alınabilmektedir (Arslan ve Türkmen, 2023: 256). Daha yalın bir anlatımla, kalkınma,

yalnızca üretim hacminin ve kişi başına düşen gelirin arttırılması anlamına gelmez; aynı zamanda, az gelişmiş toplumlarda ekonomik ve sosyo-kültürel yapıların dönüştürülmesini ve modernize edilmesini de içermektedir. Kalkınma planlaması ise, uzun vadeli kalkınma politikalarının belirli ilkeler çerçevesinde şekillendirilmesini ifade etmektedir. Kapsamlı bir perspektifle ele alındığında, kalkınma planlaması; bir ülkenin ekonomik, sosyal ve siyasi değerlerini dikkate alarak, belirlenen bir zaman dilimi içerisinde toplumun erişmek istediği sosyo-ekonomik hedeflere ve niceliksel olarak tanımlanmış amaçlara en etkin yoldan ulaşılmasını sağlamak amacıyla, kaynakların özgül kurumlar tarafından idare edilmesi süreci olarak tanımlanmaktadır (Özdemir, 2014: 3-4).

Kalkınma planları, ekonomik, siyasal ve toplumsal politika alanlarının entegrasyonunu sağlayan ve bu politikaların koordinasyonunu temin eden temel stratejik belgelerdir (Barbak, 2017: 263). Türkiye Cumhuriyeti'nde bu görev, 1960 yılında kurulan ve ülkenin uzun vadeli kalkınma stratejilerini tasarlamakla yükümlü Devlet Planlama Teşkilatı (DPT) tarafından üstlenilmiştir. 2011 yılında gerçekleştirilen yapısal bir reform ile DPT, Kalkınma Bakanlığı adı altında yeniden organize edilmiştir. İlerleyen süreçte, 2018 yılında, Kalkınma Bakanlığı'nın fonksiyonları Maliye Bakanlığı'nın Bütçe ve Mali Kontrol Genel Müdürlükleri ile entegre edilerek, Cumhurbaşkanlığı bünyesinde yeni bir yapı olan Strateji ve Bütçe Başkanlığı'nın temelleri atılmıştır (Denizli Polat, 2024: 1077). Bu dönüşüm, Türkiye'nin kalkınma politikalarının daha etkin bir şekilde koordine edilmesini ve uygulanmasını amaçlamaktadır.

Türkiye'de devletin tüm organlarının, önceden belirlenmiş hedefler ve politikalar doğrultusunda koordineli bir şekilde faaliyet göstermesini sağlayan kalkınma planlamasının ilk örneği, 1932-1937 dönemini kapsayan Birinci Kalkınma Planı ile ortaya konmuştur. Anayasal bir zeminde şekillenerek sistemli bir biçimde oluşturulan planlı kalkınma süreci, 1963 yılında yürürlüğe giren Birinci Beş Yıllık Kalkınma Planı'yla başlatılmıştır (Kızılboğa Özaslan ve Alıcı, 2014: 316). Türkiye'de ekonomik ve sosyal gelişmeyi yönlendiren temel politika belgeleri arasında, 1963 yılında başlatılan ve günümüzde on ikinci dönemi uygulanan Beş Yıllık Kalkınma Planları öne çıkmaktadır. Türkiye'nin ilk kalkınma planları, kamu sektörü için emredici, özel sektör için ise rehber niteliğinde olmuştur. Kamu sektörü, mevzuatın izin verdiği ölçüde bu planları uygulamakla yükümlü kılınmıştır. Özel sektör ise, daha çok teşvik edici politikalarla desteklenmiş ve özendirilmiştir. Kamu sektörünün geniş uygulama alanı ve güçlü yaptırım kapasitesi, kalkınma sürecinde ona daha ağırlıklı bir rol

vermiştir. Bu durum, kalkınma dinamiklerinin şekillenmesinde kamu sektörünün öncü bir etken olmasına yol açmıştır (Özdemir, 2014: 10; Akça, 2016: 722).

1963 yılından itibaren başlayıp 2028 yılına dek uzanan süre zarfında, Türkiye'nin uygulamaya koyduğu on iki adet kalkınma planı incelendiğinde, siber güvenlik konusunun doğrudan bir yaklaşımla ele alınmadığı görülmektedir. Ancak, 2000'lerin başından itibaren, dijital dönüşüm süreçlerinin hız kazanması ve bilgi toplumuna geçişin öneminin artmasıyla birlikte, siber güvenlik konusu kalkınma planlarında daha fazla öne çıkmaya başlamıştır. Bu durum, siber güvenlik alanında kalkınma planlamalarının ve politikalarının geliştirilmesinin, ülkenin kalkınma hedefleri içindeki yerini pekiştirmesi açısından önem arz etmektedir. Türkiye'de siber güvenlik konusuna değinen belli başlı kalkınma planları şunlardır:

3.1. 8. Beş Yıllık Kalkınma Planı (2001-2005)

Bu plan, Türkiye'nin uzun vadeli stratejilerini belirleyen önemli bir belgedir. Bu planda, siber güvenlik konusunda spesifik detaylara yer vermemekte; ancak bilgi ve iletişim teknolojilerinin evrimini teşvik eden ve bu sektördeki altyapıyı güçlendirmeyi hedefleyen genel hükümleri kapsamaktadır. Ulusal bilgi güvenliğini destekleyici yasal düzenlemelerin ve tedbirlerin entegre edildiği, bu alanda stratejik bir yaklaşımı temsil eden ilk kalkınma planını tanımlayan VIII. Beş Yıllık Kalkınma Planı'nın "Temel Amaç, İlke ve Politikaları (2001-2005)" bölümünde belirtilen plan hedefleri doğrultusunda, bilgi ve iletişim ağlarının geliştirilmesi öncelikli hedefler arasında yer almaktadır. Örneğin, plan dahilinde, üniversitelerin bilgi ve iletişim teknolojileri altyapısının yanı sıra ulusal ve uluslararası ağ bağlantılarının güçlendirilmesi öngörülmektedir. Bu bağlamda, söz konusu geliştirmelerin, eğitim ve araştırma faaliyetlerinin kalitesini artıracağı ve küresel bilgi ağına entegrasyonu kolaylaştıracağı ifade edilmektedir (DPT, 2000: 128-219).

3.2. 9. Kalkınma Planı (2007-2013)

Bu plan, siber güvenlikle ilgili doğrudan bilgileri kapsamamakta; bunun yerine, elektronik devlet uygulamaları ve bilgi toplumu stratejilerini ele almaktadır. Bu yaklaşım, geniş kapsamlı bir çerçevede, dijital dönüşüm süreçlerinin ve politikalarının bütünleşik bir anlayışını yansıtmaktadır. Planlama dönemi içerisinde, elektronik devlet yatırımlarının, diğer kamu hizmetleri yatırımları arasında öncelikli bir konuma getirilmesi öngörülmektedir. Bu bağlamda, kullanım oranları yüksek ve ekonomik geri dönüşü fazla olan hizmet alanlarına yönelik elektronik devlet yatırımlarına ağırlık verilmesi planlanmaktadır. Ayrıca, Bilgi ve İletişim Teknolojilerinin (BİT) geniş kitlelere yayılması ve bu teknolojilerin etkin

kullanımının teşvik edilmesi, plan döneminin temel taşlarından biri olarak belirlenmiştir (DPT, 2006: 58-96).

3.3. 10. Kalkınma Planı (2014-2018)

Bu plan, Türkiye'nin 2014-2018 yıllarını kapsayan ve siber güvenlik konusuna da değinen geniş bir stratejik çerçeve sunmaktadır. Özellikle, ulusal ve uluslararası güvenlik politikalarıyla uyum içinde, bireylerin, kurumların ve devletin karşı karşıya olduğu tehditleri adresleyen siber suçlarla mücadelede etkinliğin artırılması amaçlanmaktadır. Bu kapsamda, bilişim teknolojilerinin hızla gelişmesi ve bu gelişmelerin tetiklediği siber suç oranlarındaki artışa yanıt olarak, 2011 yılında Emniyet Genel Müdürlüğü bünyesinde özel bir birim kurulmuştur. Bu birim, siber güvenlik alanındaki yenilikleri dikkatle izleyerek, siber suçlarla mücadelede stratejik tedbirler geliştirip uygulamaktadır. Ek olarak, "*Ulaştırma, Denizcilik ve Haberleşme Bakanlığı*" bünyesinde oluşturulan Siber Güvenlik Kurulu ile siber güvenlik alanındaki çalışmalar daha da hız kazanmıştır. Ayrıca, plan dahilinde, kişisel verilerin korunmasına ve ulusal bilgi güvenliği sahasında hukuki temellerin sağlamlaştırılmasına yönelik tamamlanması öngörülen düzenlemelerin gerçekleştirileceği ifade edilmiştir (Kalkına Bakanlığı, 2013: 37-98). Bu hükümler, Türkiye'nin siber alanda karşılaşabileceği tehditlere karşı daha dirençli bir yapı oluşturmayı ve ulusal güvenliği sağlamayı amaçlamaktadır.

3.4. 11. Kalkınma Planı (2019-2023):

Türkiye Cumhuriyeti'nin Cumhurbaşkanlığı Hükümet Sistemi altında hazırlanan ilk kalkınma planı olan On Birinci Kalkınma Planı, 2019 ile 2023 yıllarını kapsayacak şekilde, siber güvenlik başta olmak üzere çeşitli alanlarda stratejik amaçlar tespit eden ve bu doğrultuda bir yol haritası sunan bir belgedir. Plan, siber güvenlikle ilgili olarak, özellikle kritik altyapıların korunması ve siber saldırılara karşı dirençliliğin artırılması gibi konulara odaklanmaktadır. Bu bağlamda, ihtiyaç duyulan alanlarda siber güvenlik standartlarının oluşturulması, bilgi güvenliği yönetim sistemlerinin kurulması, siber güvenlik tatbikatının düzenlenmesi, üniversitelerde siber güvenlik lisans ve yüksek lisans programlarının oluşturulması ve siber olaylara müdahale kapasitesinin geliştirilmesi gibi önlemler öngörülmektedir. Ayrıca, siber güvenlik ürün ve teknoloji projelerinin geliştirilmesi, toplumun tüm kesimlerinde siber güvenlik kültürünün ve insan kaynağının geliştirilmesinin sağlanması, siber güvenlik eğitimlerinin düzenlenmesi, siber güvenlik farkındalığının artırılması ve bu alanda uzman insan kaynağının yetiştirilmesi de planın hedefleri arasında yer almaktadır. Kalkınma Planı, siber güvenlik politikalarının uygulanmasında koordinasyon ve iş birliğinin güçlendirilmesini, ulusal ve uluslararası düzeyde iş birliklerinin artırılmasını ve siber güvenlikle ilgili mevzuatın

güncellenmesini de içermektedir (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2019: 109-184). Bu hükümler, Türkiye'nin siber güvenlik alanında daha güçlü bir yapıya kavuşmasını ve siber tehditlere karşı daha etkin bir şekilde mücadele edebilmesini amaçlamaktadır.

3.5. 12. Kalkınma Planı (2024-2028):

Bu plan, Türkiye'nin 2053 vizyonu doğrultusunda hazırlanmış ve ülkenin sürdürülebilir ve kapsayıcı büyüme hedeflerini destekleyen bütüncül bir yol haritası olarak belirlenmiştir. Plan, siber güvenlik konusuna özel bir önem atfetmekte ve bu alanda çeşitli hükümler içermektedir. Bu hükümler; finansal piyasaların siber güvenlik standartlarının belirlenmesi, siber güvenlik yeniliklerine adaptasyonun sağlanması, ulusal siber güvenliğin korunması için stratejik, düzenleyici ve teknolojik inisiyatiflerin alınması, Siber Güvenlik Stratejisi ve Eylem Planı'nın revize edilmesi, ulusal siber güvenlik çabalarının en yüksek düzeyde koordine edilmesi, siber tehditlerin erken saptanması ve önlenmesine yönelik tedbirlerin uygulanması, ulusal siber güvenlik teknik altyapısının güçlendirilmesi, gereksinim duyulan alanlarda siber güvenlik standartlarının geliştirilmesi, yerel siber güvenlik ekosisteminin desteklenmesi, özellikle kamu kurumlarında yerli siber güvenlik ürünlerinin kullanımının teşvik edilmesi, siber güvenlik farkındalığının ve kalifiye insan kaynağının artırılması, siber güvenlik sektöründe nitelikli iş gücünün yetiştirilmesi ve kariyer fırsatlarının iyileştirilmesine yönelik programların hayata geçirilmesi, toplumsal siber güvenlik bilincinin artırılması, çocukların siber suçlar ve siber zorbalık konularında bilgilendirilmesi, eğitim programlarında siber suçlara karşı farkındalık oluşturulması, güvenlik kurumlarının teknik kapasitesinin artırılarak siber suçlarla mücadele etkinliğinin güçlendirilmesi ve kamu kurumlarının siber tehditlere karşı korunmasının sağlanması gibi önemli maddeleri içermektedir (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023: 1-235). Bu maddeler, siber güvenlik alanında ulusal düzeyde bir çerçeve oluşturmayı ve bu alandaki gelişmeleri desteklemeyi amaçlamaktadır.

Bu kalkınma planları, Türkiye'nin siber güvenlik alanındaki gelişimini ve stratejilerini şekillendiren önemli belgeler olmuştur. Siber güvenlik, bilgi ve iletişim teknolojilerinin güvenliği, kişisel verilerin korunması ve ulusal güvenlik gibi geniş bir yelpazede ele alınmıştır. Özellikle son yıllarda, artan siber tehditler ve dijital dönüşüm süreçleri ile birlikte siber güvenlik konusuna daha fazla önem verilmektedir.

4. KALKINMA PLANLARINDA SİBER GÜVENLİĞİN DEĞERLENDİRİLMESİ

4.1. Araştırmanın Amacı ve Önemi

Bu çalışma, Türkiye'nin 8., 9., 10., 11. ve 12. beş yıllık kalkınma planlarında "siber güvenlik" teriminin ne sıklıkta yer aldığını inceleyerek, bu kavramın zaman içerisindeki önemini ve gelişimini nitel araştırma yöntemiyle doküman analizi kapsamında derinlemesine değerlendirmeyi amaçlamaktadır. Bu doğrultuda, Türkiye'nin kalkınma politikalarında siber güvenliğin konumunu ve etkisini daha iyi kavramaya yönelik kapsamlı bir çerçeve sunulması hedeflenmektedir.

Türkiye'nin kalkınma planlarında siber güvenlik, stratejik bir öncelik olarak her geçen gün daha da büyük bir önem kazanmaktadır, bu da ulusal güvenlik ve sürdürülebilir kalkınma hedefleri açısından kritik bir unsur haline gelmektedir. Siber güvenlik, günümüzde ulusal güvenliğin sağlanmasında merkezi ve vazgeçilmez bir öneme sahiptir. Bu bağlamda, söz konusu çalışma, Türkiye'nin siber güvenlik politikalarının güçlendirilmesi ve bu alandaki stratejik önceliklerin tespiti açısından politika yapıcılar, akademisyenler ve siber güvenlik uzmanları için önemli bir referans niteliği taşımaktadır.

4.2. Araştırmanın Yöntemi

Son dönemlerde, sosyal ve beşerî bilimler alanında, nitel araştırma yöntemleri ve bunlara ilişkin yöntemlerin kullanımının yaygınlaştığı görülmektedir (Sert vd., 2023: 4071; Özdemir ve Tuti, 2023: 217). Tarihsel süreçte, nitel araştırma, doğal fenomenlerin tanımlanması çabasından yola çıkarak 'doğal araştırma', araştırmacının probleme dair subjektif görüşlerini içermesi nedeniyle 'yorumlayıcı araştırma', ve incelenen konunun belirli bir sosyal çevrede detaylı bir şekilde ele alınmasından ötürü 'alan araştırması' gibi çeşitli adlarla anılmıştır. Nitel araştırma, sosyal bilimlerde artan bir öneme sahip olup, incelenen problem üzerinde derinlemesine bir kavrayış geliştirmek, eleştirel bir sorgulama süreci yürütmek ve olgunun doğal bağlamındaki gerçekliğini anlamak için vazgeçilmez bir yöntem olarak öne çıkmaktadır (Yıldırım, 1999: 7; Baltacı, 2019: 369). Bu çalışma kapsamında, sosyal ve beşerî bilimler alanındaki araştırmalarda sıklıkla başvurulan nitel araştırma yöntemi benimsenmiştir. Araştırmanın odağında, belirli bir durumun derinlemesine incelenmesi yer almaktadır.

4.3. Araştırmada Verilerin Toplanması

Nitel araştırmalar, genellikle üç ana bilgi kategorisi toplamayı hedefler: çevresel bilgiler, süreçle ilgili veriler ve bireysel algılar. Çevresel bilgiler, araştırmanın gerçekleştirildiği sosyo/kültürel, demografik, psikolojik ve fiziksel çevre özelliklerini içermektedir ve bu

bilgiler, süreç ve algılarla ilgili veriler için bir temel oluşturarak, farklı ortamlarla karşılaştırmalar yapılmasını sağlamaktadır. Süreçle ilgili veriler, araştırma sürecinde meydana gelen olayları ve bu olayların araştırma grubu üzerindeki etkilerini belgelemektedir. Algılarla ilgili bilgiler ise, araştırma grubunun süreç hakkındaki düşüncelerini ve yorumlarını ifade etmektedir (Yıldırım, 1999: 10). Bu üç bilgi türünün toplanabilmesi için, araştırmacıların nitel veri toplama tekniklerinden; özellikle görüşme, gözlem ve yazılı dokümanların/metinlerin analizi yöntemlerini etkin bir şekilde kullanmaları gerekmektedir (Baltacı, 2019: 374). Dokümanlar, nitel araştırmaların temelini oluşturan ve uzun yıllardır kullanılan önemli veri kaynaklarıdır. Araştırmacılar, veriyi derinlemesine incelemek amacıyla geniş bir doküman yelpazesini kullanmaktadır: kitaplardan mektuplara, dergilerden günlük ve haritalara, çizelgelerden istatistiklere, anayasa ve yönetmeliklerden yasal metinlere, gazetelerden fotoğraflara, anılardan röportajlara, eğitim ve sağlık kayıtlarından kamu belgelerine, resimlerden videolara ve mesajlara kadar pek çok kaynağı değerlendirmektedirler. Son yıllarda, metodolojinin bir unsuru olarak doküman analizi üzerine yazılan araştırma raporları ve akademik makalelerde gözle görülür bir artış söz konusudur. Bu durum, doküman analizinin araştırma süreçlerindeki öneminin ve uygulanabilirliğinin arttığını göstermektedir (Kıral, 2020: 170).

Bu çalışmada, veri toplama teknikleri arasında yer alan doküman tekniği kullanılmıştır. Doküman analizi, nitel araştırmaların önemli bir bileşeni olmasına rağmen, sıklıkla göz ardı edilen bir tekniktir. Bu yaklaşım, mevcut metinlerin derinlemesine incelenmesini sağlayarak, araştırmacılara, başka yöntemlerle ulaşamayacakları veri ve anlayışları elde etme fırsatı sunmaktadır. Genel anlamda, doküman tekniği, basılı ve elektronik formatlarda (bilgisayar tabanlı ve internet aracılığıyla iletilen) materyallerin incelenmesi veya değerlendirilmesi amacıyla uygulanan sistematik bir yöntemdir. Bu teknik, kitaplar, gazeteler, akademik dergiler ve kurumsal raporlar gibi geniş bir belge yelpazesinin sistematik incelemesini kapsamaktadır (Morgan, 2022: 64; Bowen, 2009: 27). Bu analiz sürecinde, analiz için uygun dokümanların titizlikle seçilmesi, bu sürecin başarısında kritik bir öneme sahiptir. Bu çalışma, siber güvenlik alanında kurumsal raporlar niteliğindeki 8., 9., 10., 11. ve 12. kalkınma planlarını incelemektedir. Bu planlar, sektördeki gelişmeleri ve geleceğe yönelik stratejileri belirleyen önemli belgelerdir. Analiz, bu planların siber güvenlik perspektifinden nasıl bir yol haritası sunduğunu ortaya koymaktadır.

Bu çalışmanın amacı, 2000'lerin başından itibaren dijital dönüşüm süreçlerinin ivme kazanması ve bilgi toplumuna geçişin artan önemi bağlamında, siber güvenlik konusunun

kalkınma planlarındaki yerini incelemektir. Bu bağlamda, araştırma 2001 ile 2028 yılları arasını kapsayan yirmi yedi yıllık bir zaman diliminde oluşturulan beş kalkınma planını mercek altına almaktadır. Söz konusu dönemdeki kalkınma planlarının siber güvenlikle ilgili içerikleri detaylı bir şekilde analiz edilmekte ve değerlendirilmektedir. Çalışma kapsamında yer alan kalkınma planlarına, Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı'nın resmi internet portalı üzerinden ulaşılmıştır. Bu kaynak, ilgili planların detaylı analizi ve değerlendirmesi için başvurulan birincil ve güvenilir bir referanstır. Akademik çalışmalarda, bu tür resmî belgelere erişim, araştırmanın sağlamlığı ve doğruluğu açısından büyük önem taşımaktadır. Bu nedenle, söz konusu planlarla ilgili verilerin bu resmi kanal aracılığıyla edinilmesi, çalışmanın metodolojik bütünlüğünü ve kredibilitesini pekiştirmektedir.

Nitel araştırmalar kapsamında, dokümanlardan elde edilen verilerin kodlanması, analizi ve yorumlanması süreçleri, disiplinli ve metodik bir yaklaşımı zorunlu kılmaktadır. Dokümanlar, bir araştırmanın temel veri setini teşkil ettiğinde, bu dokümanların araştırmanın hedefleri doğrultusunda detaylı bir içerik analizi sürecinden geçirilmesi gerekmektedir. Bu prosedür, dokümanların içerdiği açık ve kapalı anlamların sistematik bir biçimde incelenmesini mümkün kılarak, araştırmanın derinlemesine anlaşılmasına olanak tanımaktadır (Denizli Polat, 2024: 1078; Sak vd., 2021: 236).

4.4. Araştırmada Verilerin Analizi

Araştırma süreci esnasında elde edilen veriler, genellikle betimsel, içerik, söylev ve metin analizi gibi çeşitli ayrıştırma işlemlerine tabi tutulmaktadır. Bu işlemler, verilerin daha derinlemesine incelenmesini ve anlamlandırılmasını sağlayarak, araştırmanın amacına hizmet eden bilgilerin ortaya çıkarılmasına olanak tanımaktadır (Baltacı, 2019: 377). Veri analizi süreçlerinde, içerik analizi ve tematik analiz yöntemleri yaygın olarak tercih edilmektedir (Sak vd., 2021: 236). Bu çalışma kapsamında, veri setinin sistematik bir biçimde incelenmesi ve yorumlanması amacıyla içerik analizi yöntemi tercih edilmiştir.

İçerik analizi, araştırma başlangıcında veya ilerleyen aşamalarda oluşturulabilecek kategoriler veya temalar üzerinden yürütülmektedir. Daha sonra, analiz birimleri olarak belirlenen sözcükler, temalar, karakterler, cümleler, paragraflar, maddeler veya içerikler gibi unsurlar çıkarılmaktadır. Bunlar, ilgili kategori veya tema altında sınıflandırılmalı; ardından, dokümanlardan elde edilen veriler, araştırmanın gereksinimleri ve içeriğine bağlı olarak niceliksel olarak dönüştürülebilmektedir veya yüzdelik olarak ifade edilebilmektedir (Kıral, 2020: 182-183). Bu çalışmada, dokümanlar kendi başlarına bir araştırma veri seti oluşturacak

şekilde derlenmiştir. Söz konusu dokümanlar, araştırmanın hedeflerine uygun olarak detaylı bir içerik analizine tabi tutularak, elde edilen verilerin bilimsel incelemeye uygunluğu sağlanmıştır.

Dokümanların içerik analizi sürecinde, belirli bir metodoloji izlenmektedir. Bu süreç dört temel aşamadan oluşmaktadır: İlk olarak, analiz edilecek veri setinden uygun örneklem seçimi yapılmaktadır. Ardından, bu verilerin sınıflandırılması ve analizi için kategoriler geliştirilmektedir. Üçüncü aşamada, analiz birimi belirlenerek, hangi veri parçalarının analize dahil edileceği saptanmaktadır. Son olarak, elde edilen bulguların sayısallaştırılması ile analitik sonuçlara ulaşılmaktadır. Doküman analizi yöntemlerinde, özellikle geniş veri setlerinin bütünüyle incelenmesi pratik olmayabilir. Bu nedenle, analiz sürecinin ilk aşamasında, araştırmanın konusu olan veri setinden uygun bir örneklem seçimi kritik öneme sahiptir (Sak vd., 2021: 236). Bu çalışma kapsamında, on iki adet yayımlanmış kalkınma planının tümünü detaylı bir şekilde incelemek yerine, analizin yönetilebilirliği ve pratikliği göz önünde bulundurularak, son beş yıllık döneme ait en güncel beş kalkınma planı örneklem olarak seçilmiştir. Bu yaklaşım, araştırmanın odaklanmasını sağlamakta ve daha derinlemesine bir analiz yapılabilmesi için gerekli olan yönlendirmeyi sunmaktadır.

Kategorilerin geliştirilmesi aşamasında, araştırmacı, araştırma sürecine başlamadan önce, ilgili alandaki teorik çerçeveleri temel alarak veya özgün kategoriler ve temalar oluşturarak çalışmaya başlayabilmektedir. Bir diğer aşama olan analiz biriminin belirlenmesi sürecinde, araştırmanın hedeflerine göre farklı analiz birimlerinin kullanılabileceği ifade edilmektedir. Bu birimler; sözcük, tema, karakter, cümle veya paragraf, madde ve içerik gibi çeşitli düzeylerde olabilir. Her bir analiz birimi, araştırmanın amacına hizmet edecek şekilde özenle seçilmelidir. Son aşama olan sayısallaştırma, belirli bir dokümanda yer alan kavramlar, olaylar veya değerlendirmelerin varlık derecesini tespit etme amacı güden bir süreçtir. Araştırmacılar, topladıkları verileri niceliksel olarak ifade etmeyi tercih edebilirler (Sak vd., 2021: 236-237). Belirtilen bu aşamaların uygulanması, çalışmada izlenerek gerçekleştirilmiştir. Şöyledir:

Bu çalışmada, beş kalkınma planı üzerinden yürütülen araştırmanın kapsamı belirlenmiştir. Araştırmanın analitik çerçevesini oluşturan temel terim/birim olarak "siber güvenlik" ifadesi seçilmiş ve bu bağlamda, her bir kalkınma planında bu terimin ne sıklıkla geçtiği tespit edilmiştir. Elde edilen veriler, söz konusu terimin kullanım sıklığını gösteren tablolar halinde sistematik bir şekilde sunulmuştur. Bu metodolojik yaklaşım, terimin kalkınma planlarındaki önemini ve sıklığını kantitatif olarak ortaya koymakta ve böylece siber güvenlik alanındaki

politik önceliklerin zaman içindeki değişimini analiz etme imkânı sağlamaktadır. Bu çalışmanın kapsamı, veri analizi için MAXQDA gibi yazılımların kullanımını gerektirmeyecek ölçüde sınırlı olduğundan, verilerin analizi araştırmacı tarafından sayma yöntemi ile gerçekleştirilmiştir. Bu yaklaşım, araştırmanın niteliğine uygun düşen ve daha basit bir analiz sürecini mümkün kılan bir yöntemdir. Araştırmacının bu tercihi, çalışmanın özgün koşullarını ve veri setinin özelliklerini dikkate alarak yapılmıştır.

Araştırma kapsamında ele alınan kalkınma planları çerçevesinde, araştırmanın siber güvenlik konusuna uygun olarak temalar oluşturulmuştur. Bu temalar, ulusal kalkınma hedeflerine katkıda bulunacak biçimde seçilmiştir. Araştırma, bu temaların kapsamlı bir analizini yaparak, ilgili planların etkinliğini ve uygulanabilirliğini değerlendirmeyi amaçlamaktadır. Temalar şöyledir:

1. Merkez Kurumu
2. Güvenlik Kurulu
3. İnsan Gücü
4. İşgücü
5. Eğitim
6. Siber Güvenlik Ekonomisi
7. Kurumsal ve Bireysel Farkındalık
8. Siber Güvenlik Teknolojileri ve Çözümleri
9. Hukuki ve Düzenleyici Çerçeve

Belirli temalar çerçevesinde, 'siber güvenlik' kelimesinin ne sıklıkla tekrar edildiği tespit edilmiş ve bu veriler tablo formatında gösterilmiştir. Ardından, bu temalara ilişkin bulgular, kalkınma planlarından yapılan alıntılarla desteklenerek analiz edilmiştir. Bu analiz, söz konusu temaların kapsam ve önemini daha iyi anlamak için kritik bir öneme sahiptir. Ayrıca, bu çalışma, siber güvenliğin kalkınma süreçlerindeki etkileri hakkında derinlemesine bir anlayış sağlamaktadır.

4.5. Araştırmanın Güvenilirliği ve Sınırlılıkları

Bilimsel araştırmaların toplum ve akademik çevreler tarafından kabul edilebilirliği, bu çalışmaların belirli bir geçerlik ve güvenilirlik düzeyine sahip olmasını zorunlu kılmaktadır. Araştırma sürecinde kullanılan veri toplama yöntemleri, seçilen araştırma tasarımı ve uygulanan veri analiz tekniklerinin geçerliliği ve güvenilirliği, araştırmanın genel inandırıcılığını ve kabul edilirliğini doğrudan etkilemektedir. Nicel araştırmalar, çeşitli istatistiksel ölçme yöntemleri sayesinde geçerlik ve güvenilirlik açısından daha kesin sonuçlar

sunabilmekteyken, nitel araştırmaların doğası gereği bu tür kesin bir geçerlik ve güvenilirlik değerlendirmesi yapmak daha zordur (Baltacı, 2019: 380). Güvenilirlik, içerik analizi bağlamında, çeşitli araştırmacılar tarafından gerçekleştirilen kodlamaların, konsensüs ve tutarlılık açısından ne derece benzer sonuçlar üretebildiğinin bir ölçütü olarak değerlendirilebilir (Neuendorf & Kumar, 2015: 3). Miles ve Huberman (1994) tarafından belirtildiği üzere, kodlayıcılar arası güvenilirlik oranı, uzlaşılan kodların toplamına oranla hesaplanır ve başlangıçta bu oranın %70'ten yüksek olması beklenmemektedir. Ancak, zamanla ve veri setinin büyüklüğüne bağlı olarak, bu oranın %80'e ulaşması, hatta %90'ı aşması tavsiye edilmektedir (Aktaran Arastaman vd., 2018: 58).

Bu çalışmada, güvenilirlik perspektifinden hareketle, iki ayrı uzman, "siber güvenlik" kavramını analitik bir birim olarak benimseyerek, kalkınma planlarında siber güvenlik başlığı altında sınıflandırılan temaları detaylı bir şekilde incelemiş ve elde edilen bulguları sistematik bir biçimde kayıt altına almıştır. Bu süreçte, siber güvenlikle ilgili tematik alanların kapsamlı bir değerlendirilmesi yapılmış, bu alanların kalkınma planlarındaki yerleri ve önemleri irdelenmiştir. Verilerin karşılaştırmalı analizi yapıldığında, iki farklı uzmanın elde ettiği bulgular arasında önemli bir uyumun varlığı tespit edilmiştir. Bu uyum, çalışmanın güvenilirliğini artıran ve metodolojik bütünlüğü pekiştiren bir faktör olarak kabul edilmektedir.

Araştırma sürecinde karşılaşılan sınırlamaların farkında olmak ve bu sınırlamaları mümkün olduğunca gidermeye çalışmak, elde edilen sonuçların güvenilirliği için kritik önem taşımaktadır. Ancak, bir çalışmanın içkin sınırlamalarının tamamını ortadan kaldırmak her zaman mümkün olmayabilir. Bu, araştırmanın doğasında var olan bir gerçektir ve bilimsel topluluk tarafından kabul edilen bir durumdur. Bu nedenle, araştırmacılar, sınırlamaları açıkça tanımlamalı ve sonuçların yorumlanmasında bu sınırlamaların potansiyel etkilerini dikkate almalıdır (Sözen ve Göküş, 2023: 243). Bu çalışma kapsamında, siber güvenlik alanında gerçekleştirilen araştırmanın belirli sınırlamaları bulunmaktadır. İlgili sınırlamalar aşağıda detaylandırılmıştır.

- Verilerin toplanması, Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı'nın resmi internet portalından elde edilmesi yoluyla gerçekleştirilmiştir. Bu portal, ilgili verilere erişim için birincil kaynak olarak hizmet vermektedir ve kullanıcıların ihtiyaç duydukları bilgilere hızlı ve etkin bir şekilde ulaşmalarını sağlamaktadır.
- Veri Kaynağı Sınırlamaları: Türkiye'nin kalkınma hedeflerini belirleyen ve bu doğrultuda politikalar geliştiren Beş Yıllık Kalkınma Planları, sekizinci, dokuzuncu, onuncu,

on birinci ve on ikinci dönemleri kapsayacak şekilde ele alınmıştır. Araştırma, yalnızca bu beş kalkınma planı üzerinden yürütülmüştür.

- Siber güvenlik terimi, dokuz temel tema altında sınıflandırılmıştır; bu temalar, alanın kapsamlı bir anlayışını sağlamak için bir araya getirilmiştir. Her tema, siber güvenlik disiplininin farklı bir yönünü temsil etmektedir.

4.6. Bulgular

Analiz edilen kalkınma planları çerçevesinde, siber güvenlik teriminin kullanım sıklığına ilişkin elde edilen veriler, aşağıda tablolar halinde detaylandırılmıştır. Söz konusu tablolar, incelenen her bir plan dönemi itibarıyla siber güvenlik konusuna atfedilen önemin bir göstergesi niteliğindedir. Bu bağlamda, tabloların sistematik bir analizi, siber güvenlik alanında zaman içindeki gelişmelerin ve politika yapıcıların bu konuya olan yaklaşımlarının evrimini anlamak açısından kritik bir öneme sahiptir.

Tablo 1: Türkiye'nin Beş Yıllık Kalkınma Planları'nda Siber Güvenlik Teriminin Kullanım Sıklığı

Kalkınma Planları	Kullanım Sıklığı	Kullanım Önemi	Gelişme ve Değişim
8. Beş Yıllık Kalkınma Planı	0	-	-
9. Beş Yıllık Kalkınma Planı	0	-	-
10. Beş Yıllık Kalkınma Planı	2	Düşük	Artış eğilimi belirgin değil
11. Beş Yıllık Kalkınma Planı	23	Orta	Önemli artış
12. Beş Yıllık Kalkınma Planı	28	Yüksek	Devam eden artış

Tablo, Türkiye'nin Beş Yıllık Kalkınma Planları (BKP) kapsamında siber güvenlik teriminin kullanım sıklığını ve önem derecesini detaylandırarak, ülkenin siber güvenlik stratejilerinin zaman içindeki gelişimini ve önceliklendirilmesini analiz etmektedir. Tabloya göre, siber güvenlik teriminin kullanım sıklığı ve önemi farklı planlarda değişiklik göstermektedir. Sekizinci planda "siber güvenlik" terimi hiç kullanılmamıştır. Bu durum, erken dönem kalkınma planlarında siber güvenliğin öncelikli bir konu olarak ele alınmadığını veya siber güvenlik kavramının henüz politika dokümanlarında yer bulmadığını göstermektedir. Bu dönemde bilgi teknolojilerinin gelişimi henüz başlangıç aşamasındadır ve siber güvenlik, kalkınma planlarının odak noktası arasında yer almamaktadır. Dokuzuncu planda da "siber güvenlik" terimi kullanılmamıştır. Bu, önceki planla benzer şekilde, siber güvenliğin stratejik bir öncelik olarak değerlendirilmeye devam edilmediğini göstermektedir. Onuncu planla birlikte bu terim iki kez anılmıştır. Bu, siber güvenliğin ulusal gündemde yer almaya başladığının ilk işaretlerinden biri olarak kabul edilebilir. Bu dönem, bilgi teknolojileri ve internetin yaygınlaşmaya başladığı, dolayısıyla siber güvenlik konusuna yönelik ilginin artmaya başladığı bir zaman dilimini temsil eder. Ancak, siber güvenlik konusu hala yüksek derecede öncelikli bir konu olarak görülmemekte ve belirgin bir artış eğilimi

göstermemektedir. On birinci planın uygulanmasıyla, 'siber güvenlik' teriminin frekansında kayda değer bir artış gözlemlenmiş ve bu terimin kullanımı yirmi üçe ulaşarak önemi 'orta' seviye olarak tanımlanmıştır. Bu durum, siber güvenliğin stratejik bir öncelik haline geldiğinin ve devlet politikalarında daha merkezi bir rol oynamaya başladığının göstergesidir. Siber güvenlik konusundaki artan vurgunun, teknoloji ve bilgi güvenliği konularındaki artan tehditler ve uluslararası gelişmelerle ilişkili olabileceği düşünülmektedir. On ikinci plana gelindiğinde, bu planda siber güvenlik terimi 28 kez kullanılmıştır ve kullanım önemi yüksektir. Bu artış, Türkiye'nin siber güvenlik konusunu stratejik bir öncelik olarak kabul ettiğini ve bu alandaki riskler ve gereksinimlerin daha fazla önemsenmeye başlandığını göstermektedir. Bu dönemde siber güvenlik, ülkenin kalkınma stratejilerinde devam eden bir artış eğilimi göstermekte ve daha kapsamlı bir stratejik planlamanın parçası haline gelmiştir.

Kalkınma planları bağlamında yürütülen doküman incelemesi neticesinde, siber güvenlik konusunun altında yatan tema başlıkları detaylı bir şekilde analiz edilmiştir. Bu analiz, araştırmanın geniş çerçevesi içerisinde, siber güvenlik kurulu ve merkez kurumu, özellikle siber güvenlik alanında insan gücü ile işgücü ve ekonomisinin dinamiklerini, kurumsal ve bireysel düzeyde eğitim ve farkındalığın artırılmasının yollarını, siber güvenlik teknolojileri ve çözümlerinin gelişimini ve hukuki ile düzenleyici çerçevenin etkilerini ele almaktadır. Bu tematik alanlar, siber güvenliğin çok yönlü yapısını ve bu alandaki stratejik yaklaşımların kapsamlı bir değerlendirmesini sağlamak amacıyla belirlenmiştir. Kalkınma planları kapsamında, "siber güvenlik" teriminin belirlenen temalar içerisinde ne sıklıkla tekrar edildiği tespit edilmiş ve bu bulgular aşağıda yer alan tabloda detaylandırılmıştır.

Tablo 2: Kalkınma Planlarında Yer Alan Temalar İçerisinde "Siber Güvenlik"

TEMALAR	8. Kalkınma Planı	9. Kalkınma Planı	10. Kalkınma Planı	11. Kalkınma Planı	12. Kalkınma Planı
Merkez Kurumu	X	X	X	1	X
Güvenlik kurulu	X	X	1	X	X
İnsan Gücü	X	X	X	X	1
İşgücü	X	X	X	X	3
Eğitim	X	X	X	3	3
Siber Güvenlik Ekonomisi	X	X	X	X	4
Kurumsal ve Bireysel Farkındalık	X	X	X	7	4
Siber Güvenlik Teknolojileri ve Çözümleri	X	X	X	2	5
Hukuki ve Düzenleyici Çerçeve	X	X	1	6	8

Bu tablo, Türkiye'nin Sekizinci Kalkınma Planı'ndan On İkinci Kalkınma Planı'na kadar uzanan dönemde siber güvenlik konularının ele alınış biçimlerinin karşılaştırmalı bir analizini sunmaktadır. Tablo, her bir kalkınma planında siber güvenlikle ilgili temaların varlığını ve bu

temaların yoğunluğunu incelemektedir. Analiz, siber güvenlik alanında öne çıkan temaların zaman içindeki değişimini ortaya koymaktadır. Tablonun analizi aşağıdaki gibidir:

- Sekizinci ve Dokuzuncu Kalkınma Planlarında "Siber Güvenlik" konusu ve ilgili temaların ele alınmaması, o dönemlerde kalkınma planlarının daha ziyade ekonomik büyüme, altyapı gelişimi, eğitim ve sağlık gibi geleneksel kalkınma alanlarına odaklanmasından kaynaklanmaktadır. Siber güvenlik ve dijital güvenlik konuları, bu yıllarda sistematik bir yaklaşımla değerlendirilmemiş, ancak Onuncu Kalkınma Planı ile birlikte, dijitalleşmenin artan hızı ve siber tehditlerin yükselişi sonucunda, bu planlarda yer edinmeye başlamıştır.
- Merkez Kurumu: Bu tema, 11. Kalkınma Planı'nda merkez kurulması konusuna atıfta bulunulduğunu göstermektedir. Kalkınma planının 496.1 maddesi uyarınca, kritik enerji altyapısının güvenliğinin sağlanması amacıyla bir Siber Güvenlik Operasyon Merkezi'nin kurulması öngörülmektedir. Önceki planlarda yer almayan bu unsurun, 11. Kalkınma Planı ile birlikte gündeme alınması, siber güvenliğin artık merkezileştirilmiş ve kurumsal bir yapıda ele alındığını göstermektedir. Bu durum, siber güvenliğin idari yapılar içerisinde daha belirgin bir yer edinmeye başladığının bir göstergesidir.
- Güvenlik Kurulu: Bu tema, siber güvenlikle ilgili stratejik kararların alındığı kurulları veya güvenlik konseyi gibi yapıların önemini vurgulamaktadır. 10. Kalkınma Planı bu konuda bir öncelik belirlemişken, diğer planlar genel olarak bu yapıyı desteklemiş ancak somut adımlar atılmamıştır. Bu durum, 10. kalkınma planının 720. maddesinde ele alınmaktadır.
- İnsan Gücü: Bu tema, yalnızca 12. Kalkınma Planı'nda 1 kez (688.6. maddesi) siber güvenlikle ilişkilendirilmiştir. Bu bağlamda, siber güvenlik alanında insan kaynağına duyulan ihtiyaç ve bu alanda uzmanlaşmış personelin önemi, 12. Kalkınma Planı'nda daha net bir şekilde tanımlanmış görünmektedir. Bu da siber güvenlik politikalarının etkin bir şekilde uygulanabilmesi için nitelikli insan gücünün stratejik bir öncelik olarak ele alındığını göstermektedir.
- İşgücü: Bu tema, siber güvenlik sektöründe çalışacak genel işgücü potansiyelini ve bu alandaki istihdam politikalarını ele almaktadır. Siber güvenlik alanında çalışan iş gücünün artırılmasına yönelik hedeflerin, özellikle 12. Kalkınma Planı'nda önceki dönemlere göre daha belirgin bir şekilde vurgulandığı görülmektedir (3 puan). Bu artış, siber güvenlik sektöründe daha fazla iş gücü ihtiyacının doğduğunu ve bu ihtiyaca yönelik planların yapıldığını göstermektedir.
- Eğitim: Eğitim, siber güvenlik temalarının geliştirilmesi ve yaygınlaştırılmasında kritik bir rol oynamaktadır. Bu tema, On Birinci ve On İkinci Kalkınma Planları kapsamında her birinde üç defa incelenmiştir. Bu durum, eğitim politikalarının, siber güvenlik

mevzusundaki boşlukları doldurma amacıyla yeniden yapılandırıldığını ve bu önemli alanın eğitim sistemimizde daha geniş bir yer edinmeye başladığını işaret etmektedir. Bu gelişme, siber güvenlik bilincinin artırılması ve bu alandaki uzman sayısının çoğaltılması yönünde atılan adımların bir yansıması olarak değerlendirilebilir.

- Siber Güvenlik Ekonomisi: Siber güvenliğin ekonomik boyutu, 12. Kalkınma Planı'nda en yüksek öneme sahip olmuştur. Bu tema, 12. Kalkınma Planı'nda 4 kez ele alınmış olup, bu durum, siber güvenliğin ekonomik boyutunun daha fazla dikkate alınmaya başlandığını göstermektedir. Bu, siber güvenliğin sadece bir teknik gereklilik olmaktan çıkıp ekonomik bir faktör olarak değerlendirildiğini ve bu bağlamda ekonomik politikaların da siber güvenlik perspektifine entegre edildiğini ortaya koymaktadır.
- Kurumsal ve Bireysel Farkındalık: Bu tema, siber güvenliğin sadece teknik bir konu değil, aynı zamanda geniş bir toplumsal bilince ihtiyaç duyan bir alan olarak değerlendirildiğini göstermektedir. Siber güvenlik konusunda farkındalığın arttırılması gerekliliği, 11. ve 12. Kalkınma Planları kapsamında önemli ölçüde yükselmiş (sırasıyla 7 ve 4 kez tekrar) ve bu durum, kurumsal ve bireysel düzeyde siber güvenlik bilincinin geliştirilmesine yönelik stratejilerin güçlenmesine işaret etmektedir. Bu eğilim, siber tehditlerin artan karmaşıklığı ve sıklığı karşısında hem devlet kurumlarının hem de vatandaşların siber ortamlarda daha bilinçli ve korunaklı hareket etmelerinin önemini vurgulamaktadır.
- Siber Güvenlik Teknolojileri ve Çözümleri: Bu tema, 11. ve 12. Kalkınma Planları'nda giderek artan bir önemle ele alınmış olup (2 ve 5 kez), Türkiye'nin siber güvenlik teknolojileri ve çözümleri geliştirme konusundaki kararlılığının güçlü bir göstergesi olmuştur. Bu durum, ülkenin bu alandaki yetkinliklerini artırma ve uluslararası siber tehditlere karşı koyma kapasitesini güçlendirme hedefine olan bağlılığını göstermektedir.

Hukuki ve Düzenleyici Çerçeve: Siber güvenlik alanında hukuki düzenlemeler, 10. Kalkınma Planı'ndan itibaren öncelikli bir tema olmuştur. 11. ve 12. Kalkınma Planlarında (6 ve 8 kez) ise bu çerçevenin daha da genişletildiği ve güçlendirildiği görülmektedir. Bu Kalkınma Planları bağlamında, hukuki ve düzenleyici çerçevenin oluşturulması, stratejik bir öncelik olarak ön plana çıkmıştır. Bu durum, altı ve sekiz puanlık değerlendirmelerle vurgulanmıştır. Özellikle siber güvenlik alanında, mevcut yasal düzenlemelerin güçlendirilmesi ve bu düzenlemelerin uygulanabilirliğinin artırılması, bu planların temel taşlarından biri olarak kabul edilmektedir. Bu bağlamda, siber güvenlik politikalarının etkin bir şekilde uygulanabilmesi için gerekli olan hukuki altyapının sağlamlaştırılması, ulusal güvenliğin

korunması ve siber tehditlere karşı koyma kapasitesinin artırılması açısından kritik bir öneme sahiptir.

Genel bir değerlendirme yapıldığında, Türkiye'nin siber güvenlik konusunda zaman içinde artan bir bilinç ve stratejik yaklaşım geliştirdiği açıkça görülmektedir. Başlangıç dönemlerinde genel hatlarıyla ve dolaylı yollarla ele alınan siber güvenlik meseleleri, ilerleyen kalkınma planlarında daha spesifik ve ayrıntılı bir incelemeye tabi tutulmuştur. Bu evrim, özellikle On Birinci ve On İkinci Kalkınma Planlarında belirginleşmiş, söz konusu planlar siber güvenlik alanında kurumsal yapılanmanın güçlendirilmesi, eğitim olanaklarının genişletilmesi, toplumsal farkındalığın artırılması ve mevzuatın iyileştirilmesi gibi çeşitli boyutlarda önemli gelişmeler kaydedilmiş olduğunu göstermektedir. Bu gelişmeler, Türkiye'nin siber güvenlik konusunda daha bütüncül ve entegre bir politika izlediğinin ve bu alanda uluslararası standartlara ulaşma yolunda kararlı adımlar attığının bir göstergesi olarak değerlendirilebilir. Bu bağlamda, Türkiye'nin siber güvenlik stratejisindeki bu dönüşüm, ülkenin dijital altyapısını koruma ve siber tehditlere karşı direnç geliştirme kapasitesini artırmak adına atılmış stratejik bir adım olarak kabul edilmelidir.

5. SONUÇ VE ÖNERİLER

Siber güvenlik konusunun Türkiye'nin Beş Yıllık Kalkınma Planları içindeki öneminin zamanla arttığını ve stratejik bir öncelik olarak daha açık bir biçimde ele alındığını göstermektedir. İlk yıllarda düşük bir öneme sahipken, sonraki yıllarda bu konunun önceliklendirilmesi ve kullanım sıklığındaki artış, siber güvenliğin ulusal kalkınma hedefleri açısından kritik bir unsur haline geldiğini gözler önüne sermektedir. Bu eğilim, siber güvenlik stratejilerinin gelişim sürecinin ve ülkenin bu alandaki politikalarının nasıl evrildiğinin anlaşılması açısından değerli bir içgörü sunmaktadır. Başka bir deyişle, erken dönem planlarında siber güvenlik konusunun ihmal edildiği görülürken, son yıllarda bu kavramın önemi ve stratejik rolü hızla artmıştır. Bu eğilim hem artan dijitalleşme hem de siber tehditlerin karmaşıklığının politika yapıcılar tarafından daha fazla dikkate alındığını ve bu alanda daha kapsamlı stratejilerin geliştirildiğini yansıtmaktadır. Örneğin, 8. ve 9. beş yıllık planlarda siber güvenlik, genellikle diğer teknolojik gelişmelerin bir parçası olarak ele alınırken, 10. planla birlikte bu alana daha fazla odaklanılmaya başlanmıştır. 11. ve 12. planlarda ise siber güvenlik, ulusal güvenlik stratejisinin temel bir bileşeni olarak belirgin bir şekilde ön plana çıkmaktadır. Bu dönemlerde, siber güvenlikle ilgili yasal ve kurumsal altyapının güçlendirilmesi ve eylem planlarının oluşturulması ve güncellenmesi yol haritasının belirlenmesi gibi önemli adımlar atılmıştır. Ayrıca, siber tehdit istihbaratında

yapay zekâ kullanımının artırılması, yerli siber güvenlik ekosisteminin geliştirilmesi ve siber güvenlik alanında nitelikli iş gücünün yetiştirilmesine yönelik programların geliştirilmesi gibi konular da 12. Kalkınma Planı'nda özellikle vurgulanmıştır. Bu gelişmeler, Türkiye'nin siber güvenlik konusundaki farkındalığının ve kapasitesinin arttığını göstermektedir. Siber güvenlik, sadece teknolojik bir mesele olmanın ötesinde, ekonomik kalkınma ve ulusal güvenlikle doğrudan ilişkili bir konu haline gelmiştir. Bu nedenle, Türkiye'nin siber güvenlik politikalarının güçlendirilmesi, ulusal ve uluslararası düzeydeki yeni nesil tehditlere karşı hazırlıklı olmak açısından büyük önem taşımaktadır. Siber güvenlik uzmanları, politika yapıcılar ve akademisyenler için bu alandaki gelişmeleri takip etmek ve analiz etmek, gelecekteki stratejilerin şekillendirilmesinde kritik bir rol oynayacaktır. Türkiye'nin siber güvenlik alanında attığı adımlar, dijital dönüşüm sürecindeki diğer ülkeler için de bir model teşkil edebilir ve uluslararası iş birliklerinin geliştirilmesine katkı sağlayabilir. Bu bağlamda, siber güvenlik politikalarının güçlendirilmesi, Türkiye'nin kalkınma hedeflerine ulaşmasında ve uluslararası alanda rekabetçi bir konuma gelmesinde önemli bir faktör olarak değerlendirilmelidir.

Bu araştırma sonucunda elde edilen veriler, Türkiye'nin kalkınma stratejileri içerisinde siber güvenlik önlemlerinin daha etkin ve kapsamlı bir biçimde entegre edilmesinin zorunluluğunu vurgulamaktadır. Siber güvenlik, ulusal kalkınma hedefleri doğrultusunda stratejik bir öncelik olarak kabul edilmeli ve bu bağlamda aşağıda sıralanan öneriler dikkate alınarak politika geliştirilmelidir:

- Siber Güvenlik Stratejilerinin Geliştirilmesi: Kalkınma planlarında siber güvenlik konusuna daha geniş bir yer verilmesi, bu alandaki stratejilerin daha ayrıntılı ve somut hedeflerle desteklenmesi önem arz etmektedir. Özellikle dijital altyapıların korunması, kritik bilgi sistemlerinin güvenliği ve kişisel verilerin korunması gibi alanlarda spesifik politikalar ve uygulama mekanizmaları oluşturulmalıdır.
- Eğitim ve Farkındalık Programlarının Yaygınlaştırılması: Siber güvenlik kültürünün toplumsal düzeyde benimsenmesi için eğitim ve farkındalık programlarının yaygınlaştırılması gerekmektedir. Kalkınma planlarına hem eğitim sisteminde hem de kamuoyu nezdinde siber güvenlik farkındalığının artırılmasına yönelik hedefler eklenmelidir.
- Özel Sektör ile İş Birliğinin Artırılması: Siber güvenlik alanında kamu ve özel sektör arasındaki iş birliği, kalkınma planlarının başarısı için kritik öneme sahiptir. Özel sektörün bilgi ve tecrübesinden yararlanmak, siber güvenlik çözümlerinin geliştirilmesinde ve uygulanmasında önemli bir avantaj sağlayacaktır. Bu kapsamda, kamu-özel sektör iş birliğini

teşvik eden politikalar geliştirilmesi ve bu iş birliğinin somut projelerle desteklenmesi önerilmektedir.

✸ Uluslararası İş Birliğinin Geliştirilmesi: Siber güvenlik, ulusal sınırları aşan bir konudur ve bu alanda uluslararası iş birliği büyük önem taşımaktadır. Türkiye'nin, siber güvenlik alanında uluslararası kuruluşlar ve diğer ülkelerle daha aktif bir iş birliği içinde olması, küresel tehditlere karşı daha etkili bir savunma mekanizması oluşturulmasına katkı sağlayacaktır.

✸ Ar-Ge Yatırımlarının Artırılması: Siber güvenlik alanında yenilikçi çözümler geliştirmek ve yerli teknolojiler üretmek, ulusal güvenliğin sağlanması açısından stratejik bir öneme sahiptir. Kalkınma planlarında Ar-Ge yatırımlarına daha fazla kaynak ayrılması, Türkiye'nin bu alandaki rekabet gücünü artıracaktır. Ayrıca, üniversiteler ve araştırma kuruluşları ile iş birliği yaparak siber güvenlik teknolojilerinde ileri düzeyde araştırmaların desteklenmesi gerekmektedir.

Bu öneriler doğrultusunda, Türkiye'nin kalkınma planlarında siber güvenliğe daha fazla odaklanması ve bu alandaki kapasitesini artırması, dijital dünyadaki risklere karşı daha hazırlıklı olmasını sağlayacaktır. Böylece hem ulusal güvenlik güçlendirilmiş olacak hem de ekonomik kalkınma süreçleri daha güvenli bir zemine oturtulacaktır.

KAYNAKLAR

Ak, T. (2013). Ulusal Güvenlik-Çevresel Güvenlik Ekseninde Silahlı Kuvvetler Çevre İlişkisi [Yayımlanmamış Doktora Tezi]. Ankara Üniversitesi.

Akça, Y. (2016). Türkiye'nin Kalkınma Planlarında Turizm Politikası. *International Conference on Eurasian Economies*, 721-726.

Arastaman, G., Öztürk Fidan, İ., & Fidan, T. (2018). Nitel Araştırmada Geçerlik ve Güvenirlik: Kuramsal Bir İnceleme. *Van Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, 15(1), 37-75.

Arslan, A., ve Türkmen, A. (2023). Türkiye'de Kalkınma Politikaları ve Bölgesel Kalkınma Planlarının Dönüşümü. *Toplum Ekonomi ve Yönetim Dergisi*, 4(Özel), 254-272. https://doi.org/10.58702/teyd.1354976

Baltacı, A. (2019). Nitel Araştırma Süreci: Nitel Bir Araştırma Nasıl Yapılır?. *Ahi Evran Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 5(2), 368-388

Barbak, A. (2017). Türkiye'de Kamu Politikası Sürecinde Güvenlik-Kalkınma Bağı: Ulusal Kalkınma Planları Üzerine Bir Araştırma. *Uluslararası İktisadi ve İdari İncelemeler Dergisi*, (18), 263-288.

Bay, M. (2016). What Is Cybersecurıty? In Search Of An Encompassing Definition For The Post-Snowden Era. *French Journal For Media Research*, 1-28. ISSN 2264-4733

Birdişli, F. (2020). Uluslararası Güvenliğin Tarihsel Gelişimi ve Postmodern Güvenlik Dönemi. *Güvenlik Bilimleri Dergisi*, UGK Özel Sayısı, 235-260 DOI:10.28956/gbd.696034

Bowen, G. A., (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, 9(2), 27-40. DOI 10.3316/QRJ0902027.

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), 13-21. DOI: 10.22215/timreview/835

Çakır, H. ve Arınmış Uzun, S. (2021). Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi (JEBPIR),* 7(2), 353-379

Denizli Polat, A. A. (2024). Türkiye Cumhuriyeti'nde Kadın İşgücü ve İstihdamı: Kalkınma Planları Perspektifinden Bir İnceleme. *Gaziantep University Journal of Social Sciences*, 23(3), 1072-1092. https://doi.org/10.21547/jss.1359298

DPT. (2000). *Uzun Vadeli Strateji ve Sekizinci Beş Yıllık Kalkınma Planı (2001-2005*). 11 Haziran 2024 tarihinde https://www.sbb.gov.tr/wp-content/uploads/2022/07/Uzun_Vadeli_Strateji_ve_Sekizinci_Bes_Yillik_Kalkinma_Plani-2001-2005.pdf adresinden alındı.

DPT. (2006). *Dokuzuncu Kalkınma Planı (2007-2013*). 17 Haziran 2024 tarihinde https://www.sbb.gov.tr/wp-content/uploads/2022/07/Dokuzuncu_Kalkinma_Plani-2007-2013.pdf adresinden alındı.

Fischer, E.A. (2016). Cybersecurity Issues and Challenges: In Brief. *Congressional Research Service*, 1-12. CRS Report for Congress, R43831

Kalkınma Bakanlığı. (2013). *Onuncu Kalkınma Planı (2014-2018*). 2 Temmuz 2024 tarihinde https://www.sbb.gov.tr/wp-content/uploads/2022/08/Onuncu_Kalkinma_Plani-2014-2018.pdf adresinden alındı.

Karasoy, H.A. ve Babaoğlu, B. (2021). Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı. *Yasama Dergisi*, (44), 123-155

Kaur, J. & Ramkumar, K.R. (2022). The Recent Trends İn Cyber Security: A Review. *Journal Of King Saud University – Computer And Information Sciences*, 34 (8), 5766–5781. https://doi.org/10.1016/j.jksuci.2021.01.018

Kıral, B. (2020). Nitel Bir Veri Analizi Yöntemi Olarak Doküman Analizi. *Siirt Üniversitesi Sosyal Bilimler Enstitüsü Dergis*i, 8(15), 170-189.

Kızılboğa Özaslan, R., ve Alıcı, O. V. (2014). Kalkınma Planlarında Yerel Yönetimler ve Yapılan Reformlar Çerçevesinde Mukayese. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 11(26), 315-342

Maurer, T. (2011). Cyber Norm Emergence at the United Nations– An Analysis of the UN's Activities Regarding Cyber-security. *Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project,* Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs, http://belfercenter.org

Miles, M. B., & Huberman, A. M. (1994). An Expanded Sourcebook: Qualitative Data Analysis (Second edition). Thousand Oaks, CA: SAGE Publications, Inc.

Morgan, H. (2022). Conducting a Qualitative Document Analysis. *The Qualitative Report*, 27(1), 64-77. https://doi.org/10.46743/2160-3715/2022.504

Neuendorf, K.A. & Kumar, A. (2015). Content Analysis. The International Encyclopedia of Political Communication, First Edition. Edited by Gianpietro Mazzoleni, DOI: 10.1002/9781118541555.wbiepc065

Öğün, M.N. ve Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi*, 9(18), 145-181

Özdemir, M. ve Tuti, G. (2023). Nitel Araştırma Desenleri: Metodolojik Bir Temellendirme. *Çankırı Karatekin Üniversitesi Karatekin Edebiyat Fakültesi Dergisi*, 11(2), 217-235. https://doi.org/10.57115/karefad.1331759

Özdemir, V. (2014). Türkiye'de Planlı Kalkınma Deneyimleri. Marmara Üniversitesi, 1-27

Rowe, D.C., Lunt, B.M., & Ekstrom, J.J. (2011, 20-22, October). The Role of Cyber-Security in Information Technology Education. *SIGITE '11: Proceedings of the 2011 conference*

on Information technology education, 113–122. New York, USA. https://doi.org/10.1145/2047594.2047628

Sak, R., Şahin Sak, İ. T., Öneren Şendil, Ç., & Nas, E. (2021). Bir Araştırma Yöntemi Olarak Doküman Analizi. *Kocaeli Üniversitesi Eğitim Dergisi*, 4(1), 227-250. http://doi.org/10.33400/kuje.843306

Schatz, D., Bashroush, R. & Wall, J. (2017). Towards a Mor ds a More Representative Sensitive Definition of Cyber Security e Definition of Cyber Securit. *Journal of Digital Forensics, Security and Law*, 12(2), 53-74. DOI: https://doi.org/10.15394/jdfsl.2017.1476

Sert, H., Ölçer Demirkıran, S., Arslan Göz, P. & Beler, H. (2023). Bir Nitel Araştırma Yöntemi: Görüşme. *Journal of Social, Humanities and Administrative Sciences*, 9(71), 4071- 4075. DOI: http://dx.doi.org/10.29228/JOSHAS.7 4031

Sözen, H. ve Göküş, M. (2023). Büyükşehir Belediyelerinde Engelli Vatandaşlara Sunulan Hizmetlerin Karşılaştırmalı Bir Analizi. 1. Basım, Nobel Bilimsel Yayınevi: Ankara.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2019). *On Birinci Kalkınma Planı (2019-2023*). 17 Temmuz 2024 tarihinde https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf adresinden alındı.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2023). *On İkinci Kalkınma Planı (2024-2028).* 23 Temmuz 2024 tarihinde https://www.sbb.gov.tr/wp-content/uploads/2023/12/On-Ikinci-Kalkinma-Plani_2024-2028_11122023.pdf adresinden alındı.

Tonge, A.M., Kasture, S.S. & Chaudhari, S.R. (2013). Cyber Security: Challenges For Society- Literature Review. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 12(2), 67-75. e-ISSN: 2278-0661. https://www.iosrjournals.org/

Vijaykumar Dalave, C., Alok Lodh, A. & Vijaykumar Dalave, T. (2022). A Study of Cyber Security Challenges and Developing Tendencies in the Latest Technologies. *International Journal for Research in Applied Science & Engineering Technology (IJRASET*), 10(X), 1371-1375. DOİ: https://doi.org/10.22214/ijraset.2022.47183

Yakubu, U.İ. and Shuaibu, M. (2016). The Concept of Security and the Emerging Theoretical Perspectives, Zaria International Conference on the Theme "Corruption, Security and National Development" Held between 28th and 30th September 2016 at the ABU

Yıldırım, A. (1999). Nitel Araştırma Yöntemlerinin Temel Özellikleri ve Eğitim Araştırmalarındaki Yeri ve Önemi. *Eğitim ve Bilim*, 23(112), 7-17