Almanya'nın Kamu Güvenliği Politikaları: Strateji Belgeleri Üzerinden Bir İnceleme

Onur Ağırdil*

Öz

Bu çalışma, Almanya'nın 2021–2024 yılları arasında yayımlamış olduğu sekiz strateji belgesi üzerinden ülkenin kamu güvenliği politikalarını tematik analiz yöntemiyle incelemektedir. Araştırma kapsamında toplam 33 kod belirlenmiştir. Söz konusu kodlar beş ana tema altında sınıflandırılmıştır. Bu temaları "demokratik güvenlik ve katılımcı yönetişim", "dijital güvenlik ve teknolojik kapasite", "kapsayıcı dayanıklılık ve kriz yönetişimi", "önleyici güvenlik ve aşırılıkla mücadele" ile "bütünleşik suçla mücadele ve istihbarat iş birliği" şeklinde sıralamak mümkündür. Bulgular, Almanya'nın güvenlik anlayışının sadece askeri tehditlere karşı savunma stratejisi değil; aynı zamanda demokratik değerlerin korunması, dijital tehditlerin yönetimi ve toplumsal dayanıklılığın inşasını önceleyen bütüncül bir yönetişim modeli olduğunu göstermektedir. Strateji belgeleri üzerinden elde edilen veriler, Almanya'nın güvenlik politikalarında çok aktörlü, normatif ve önleyici bir yaklaşım benimsediğini ortaya koymaktadır.

Anahtar Kelimeler: Güvenlik Çalışmaları, Güvenlik Politikaları, Kamu Düzeni, Kamu Güvenliği, Tematik Analiz.

Germany's Policy on Public Security: An Analysis Through Strategy Documents

Abstract

This study analyzes Germany's policy on public security through a thematic examination of eight strategy documents published between 2021 and 2024. A total of 33 codes were identified within the scope of the research. These codes are categorized under five main themes: "democratic security and participatory governance," "digital security and technological capacity," "inclusive resilience and crisis governance," "preventive security and counter-extremism," and "integrated crime prevention and intelligence cooperation." The findings reveal that Germany's security approach is not limited to military defense strategies but also prioritizes the protection of democratic values, management of digital threats, and the construction of societal resilience. The data obtained from these strategy documents demonstrate that Germany adopts a multi-actor, normative, and preventive approach to its security policies.

Keywords: Security Studies, Security Policies, Public Order, Public Security, Thematic Analysis.

*Araştırma Görevlisi | Polis Akademisi, İç Güvenlik Fakültesi
onuragirdil@gmail.com | ORCID: 0000-0002-3544-2306
DOI: 10.36484/liberal.1683028
Liberal Düşünce Dergisi, Yıl: 30, Sayı: 118, Bahar 2025, ss.199-230.
Gönderim Tarihi: 24 Nisan 2025 | Kabul Tarihi: 18 Mayıs 2025

Giriş

Güvenlik kavramı, 21. yüzyılın dinamik tehdit ortamı karşısında sadece askeri güçle temellendirilen açıklamalardan sıyrılarak, dijitalleşme, toplumsal kutuplaşma, çevresel krizler ve kurumsal direnç gibi unsurları da içerisine alan çok boyutlu bir çerçeveye evrilmiştir. Güvenlik kavramının çok boyutlu dönüşümü devletlerin güvenlik stratejilerinde normatif değerleri, yönetişim reformlarını ve teknolojik kapasiteyi bir arada ele almalarını zorunlu kılmaktadır (Gebremeskel vd., 2022:46). Bu doğrultuda Avrupa Birliği'nin merkez ülkelerinden biri olan Almanya, söz konusu dönüşümün öncülerinden biri konumundadır (Miller, 2012:11). Gerek sahip olduğu Federal yapısı, gerekse sivil toplum tarihten bu yana edinmiş olduğu çok katmanlı kriz tecrübeleri, Almanya'nın güvenlik politikalarında katılımcı ve önleyici bir yaklaşımı benimsemesine zemin hazırlamaktadır (Goedecke, 2012:68).

Bu çalışma, Almanya'nın 2021–2024 yılları arasında yayımlamış olduğu sekiz ulusal güvenlik belgesini tematik analiz yöntemiyle inceleyerek, ülkenin güvenlik paradigmasında ön plana çıkan temaları tespit etmeyi amaçlamaktadır. Çalışmada analiz edilen sekiz temel strateji belgesi, Almanya›nın güvenlik politikasında yaşanan yapısal, normatif ve teknolojik dönüşümü kapsamlı biçimde yansıtma kapasitesine sahip olmaları nedeniyle seçilmiştir. Belirlenen belgeler, belirli bir güvenlik alanına odaklanan teknik metinler olmasının ötesinde; aynı zamanda Almanya'nın yürüttüğü kamu politikasında güvenlik kavramını nasıl tanımladığına, önceliklerini nasıl belirlediğine ve tehditlere nasıl yanıt verdiğine ışık tutan yüksek politika dokümanlarıdır. Ayrıca seçilen belgeler, hem normatif düzeyde (örneğin demokrasi, katılım, hukukun üstünlüğü gibi değerleri önceleyen belgeler) hem de uygulayıcı düzeyde (örneğin kritik altyapıların korunması, siber güvenlik veya suçla mücadeleye dair teknik stratejiler) bu dönüşümün izlenmesini mümkün kılmaktadır. Söz konusu belgeler aşağıda sıralanmıştır:

1. "Siber Güvenlik Stratejisi " (2021)
2. "Koalisyon Anlaşması" (2021–2025)
3. "Polis Odaklı Suçla Mücadele Stratejisi" (2022)
4. "Afetlere Karşı Dayanıklılığın Güçlendirilmesine İlişkin Strateji Belgesi" (2022)
5. "Kritik Altyapıların Korunmasına İlişkin Çatı Strateji Belgesi" (2023)
6. "Ulusal Güvenlik Stratejisi" (2023)
7. "Anayasayı Koruma Raporu" (2023)

8. "Aşırılıkla Mücadele ve Demokrasi Güçlendirme Stratejisi" (2024)

Strateji belgeleri incelenirken 33 kod belirlenmiştir. Bu kodlar açıkça ifade edilen politika hedeflerinden ve **örtük şekilde vurgulanan güvenlik önceliklerinden** türetilmiştir. Bu bağlamda çalışmada yalnızca belgelerde geçen anahtar kavramlar ve kurumsal bağlamı da dikkate alınarak anlamlı bütünler oluşturulmuştur. Her belge için ayrı ayrı yapılan ilk kodlama süreci sonunda, belgede tekrar eden yapılar, vurgu yapılan güvenlik alanları, stratejik hedefler ve kullanılan dil analiz edilerek temsil gücü yüksek, özgül ve analitik kodlar tanımlanmıştır. Kodların belirlenmesinde üç temel kriter esas alınmıştır:

a. Politika belgelerinde açıkça tanımlanmış stratejik öncelikler
b. Kurumlar arası koordinasyonun ifade edildiği başlıklar
c. Toplumsal risklere yönelik yapısal müdahale alanları

Bu kriterler doğrultusunda her belge için ortalama 4–5 ana kod oluşturulmuş ve toplamda 33 kod tanımlanmıştır. Bu kodlar daha sonra kavramsal yakınlıkları ve içeriksel benzerlikleri dikkate alınarak beş ana tematik küme altında birleştirilmiştir. Bu tematik çerçeve, çalışmanın analiz kısmında hem belge içi hem de belgeler arası karşılaştırmaya imkân tanımıştır. Çalışmada yer alan 33 kod ve ilgili olduğu temaları şu şekilde sınıflandırılmıştır:

Tablo 1. Tema ve İlgili Olduğu Kodlar

Tema	**İlgili Kodlar**
Demokratik Güvenlik ve Katılımcı Yönetişim	Demokratik düzenin korunması
	Uluslararası güvenlik iş birlikleri
	Sivil toplumun güçlendirilmesi
	Polis teşkilatında demokratik reformlar
	Dijital gözetimin hukuki sınırlandırılması
	Polis eğitimlerinde ırkçılıkla mücadele
	Toplumsal meşruiyetin güçlendirilmesi
Dijital Güvenlik ve Teknolojik Kapasite	Siber güvenlik ve dijital direnç
	Kamu kurumlarında dijital direnç
	Yapay zekâ destekli erken uyarı sistemleri
	Kritik altyapıların güvenlik standartları
	Bireysel dijital farkındalık ve siber okuryazarlık
	Dijital dezenformasyon

Kapsayıcı Dayanıklılık ve Kriz Yönetişimi	Toplumsal dayanıklılık ve krizlere hazırlık Minimum güvenlik standartlarının belirlenmesi Sektörler arası bağımlılık analizi Kamu-özel iş birliği ile risk paylaşımı Acil hazırlık planlarının kurumsallaşması Dayanıklılık odaklı yönetişim reformları Kurumlar için risk tabanlı hazırlık sistemleri Kurumsal öğrenme ve yeniden yapılanma Toplumsal kapasite geliştirme ve öz yardım
Önleyici Güvenlik ve Aşırılıkla Mücadele	Demokratik değerlerin erken yaşta aşılanması Radikalleşmenin erken tespiti için çok aktörlü sistemler Dijital aşırılıkla mücadele Ayrımcılığa maruz kalan gruplar için destek Aşırı sağ tehdidine karşı önleyici istihbarat Dini gerekçeli aşırıcılıkla mücadele
Bütünleşik Suçla Mücadele ve İstihbarat İş Birliği	Organize suçlara karşı istihbarat koordinasyonu Siber suçlarla mücadelede teknik kapasite Finansal suçlarla mücadelede şeffaflık Toplum temelli suç önleme yaklaşımı Yabancı istihbarat faaliyetleri ve demokratik tehdit

Söz konusu 33 kod, beş ana tema altında yapılandırılmıştır. Tema başlıklarının seçimi, doğrudan kodların kavramsal kümelenmesinden türetilmekle beraber aynı zamanda Almanya'nın güvenlik stratejilerinde belirginleşen eğilimleri yansıtan analitik çatı kavramlar olarak tanımlanmıştır. Bu tematik başlıkları sırasıyla "demokratik güvenlik ve katılımcı yönetişim", "dijital güvenlik ve teknolojik kapasite", "kapsayıcı dayanıklılık ve kriz yönetişimi", "önleyici güvenlik ve aşırılıkla mücadele" ile "bütünleşik suçla mücadele ve istihbarat iş birliği" şeklinde sıralamak mümkündür. Böylelikle çalışma, Almanya'nın güvenlik stratejilerinin çok aktörlü, normatif ve teknoloji odaklı yapısını bütüncül bir çerçevede değerlendirmektedir.

Strateji belgelerinde yer alan temalar güvenlikleştirme kuramı, risk toplumu ve yönetişim teorisi bağlamında değerlendirilebilir. Güvenlikleştirme kuramı açısından bir konunun "güvenlik meselesi" hâline gelmesinin nedeni,

söz konusu tehdidin siyasi aktörlerce güvenlik tehdidi olarak inşa edilmesine bağlıdır. Bu noktada öncelikle bir meselenin kamuya açık bir söylem düzeyinde, tehdit olarak tanımlanması söz konusudur. Ardından ortaya atılan tehdit unsuru toplumsal düzeyde kabul görürse "güvenlikleştirilmiş" olur (Buzan vd., 1998:61). Belgelerde ön plana çıkan "önleyici güvenlik" teması, bu kuramsal çerçeve ile yakından ilişkilidir. Özellikle "radikalleşmenin erken tespiti", "dijital aşırılıkla mücadele" ve "aşırı sağ tehdidine karşı geliştirilen önleyici istihbarat mekanizmaları" potansiyel tehditlerin henüz gerçekleşmeden güvenlik gündemine alınmasını mümkün kılmaktadır. Bu noktada önleyici güvenlik politikaları, güvenlikleştirme sürecinin erken aşamada işleyişe geçirilmesi anlamına gelmektedir. Belgelerde yer alan çok aktörlü izleme sistemleri ve dijital tehditlere karşı geliştirilen algoritmik izleme mekanizmaları, güvenlikleştirme sürecinin kurumsallaşmış örnekleri olarak okunabilir.

Almanya'nın strateji belgelerinde güvenliğin kapsamı geniş tutulmuştur. Siber saldırılar, dezenformasyon, altyapı kırılganlıkları ve aşırılık gibi riskleri içerisine almış durumdadır. Bu durum Beck'in tanımladığı modernleşmenin yan etkileriyle baş etme çabası ile örtüşmektedir. Nitekim Beck'e göre risk toplumunda artık güvenliğin nesnesi değişmiştir. Toplumun kendisinden kaynaklı riskler, klasik güvenlik tehditlerinden farklılaşmıştır (Beck,1992:21). Örneğin, "Afetlere Karşı Dayanıklılığın Güçlendirilmesine İlişkin Strateji" belgesinde, **öngörülemeyen krizlere hazırlıklı olma** ve senaryo temelli tatbikatlar vurgusu yapılmıştır. "Kapsayıcı Dayanıklılık ve Kriz Yönetişimi" teması ile ilişkili olan bu durum, Beck'in "refleksif modernlik" anlayışındaki "toplumun kendi ürettiği belirsiz risklerle yüzleşmesi" ile ilişkilidir. Toplumun kendi ürettiği risklerle yüzleşmesi ile ifade edilmek istenen, modern toplumların kendi gelişmişlik düzeylerinin bir sonucu olarak ortaya çıkan risklerle karşı karşıya kalması durumudur (Beck,1992:36).

Beck'in risk toplumu kuramının merkezinde, risklerin yönetim süreçlerinde tek bir merkezî otoritenin yetersiz kalabileceği vurgusu yer almaktadır. Bu doğrultuda ulus-devletlerin tek başına karar verici olduğu bir modelin, yeni risk gerçekliğinde yetersiz kalabileceğinin altı çizilmiştir (Beck, 1992:18). Bu durum Almanya'nın güvenlik belgelerinde açıkça görülmektedir. Güvenliğin planlanmasında, **özel sektör, STK'lar ve yerel yönetimlerle iş birliğinin vurgulanması,** risklerin kolektif olarak yönetilmesini zorunlu kılan "risk toplumu" kavramsallaştırmasına uygun düşmektedir. Bu doğrultuda risk toplumu kuramının "Kapsayıcı Dayanıklılık ve Kriz Yönetişimi" teması ile ilişkilendirmek mümkündür.

Yönetişim kuramı karar alma ve uygulama süreçlerinde sivil toplum, özel sektör, yerel yönetimler ve uluslararası kuruluşlar gibi farklı aktörlerin etkileşimini mümkün kılmaktadır. Yönetişim yaklaşımı hiyerarşik ve merkeziyetçi yönetim biçimlerinin yerini, daha yatay ve katılımcı bir ağ yapılanmasına bırakması gerektiği düşüncesine dayanır (Rhodes,2000:59). Almanya'nın güncel güvenlik stratejilerinde görülen çok aktörlü güvenlik anlayışı, bu kuramsal zemine doğrudan karşılık gelmektedir. Örneğin söz konusu belgelerde yer alan "kamu-özel iş birliği ile risk paylaşımı", "toplumsal kapasite geliştirme", "çok düzeyli yönetişim reformları" gibi kodlar, güvenlik meselesinin devletin tekelinden çıkarılarak kolektif bir sorumluluk olarak tanımlandığını göstermektedir. Dolayısıyla yönetişim kuramı, Almanya'nın güvenlik politikalarında görülen aktör çeşitliliğini, yatay karar alma mekanizmalarını ve kapsayıcı güvenlik uygulamalarını teorik olarak açıklamak açısından işlevsel bir çerçeve sunmaktadır.

Bu çalışma, Almanya'nın güvenlik stratejilerinde ortaya çıkan yönelimleri analiz ederken üç temel varsayıma dayanmaktadır: İlk olarak, Almanya'da güvenlik politikaları yalnızca askeri tehditlere değil; dijitalleşme, toplumsal dayanıklılık ve demokratik yönetişim gibi çok boyutlu risk alanlarına yanıt verecek şekilde yeniden yapılandırılmaktadır. İkinci olarak, strateji belgeleri, devletin güvenlik vizyonunu yansıtan teknik metinler olmanın ötesinde, aynı zamanda normatif değerler ile kurumsal önceliklerin iç içe geçtiği siyasi belgelerdir. Üçüncü olarak ise, Almanya'nın güvenlik anlayışı çok aktörlü, önleyici ve veri temelli bir yönetişim modeline evrilmektedir. Bu durum, strateji belgelerinden elde edilen kod-tema ilişkileri aracılığıyla somut biçimde izlenebilmektedir.

İlgili Çalışmalar

Almanya'nın güvenlik politikalarının 2000 sonrası dönemde geçirdiği dönüşüm Didier Bigo ve Lucia Zedner tarafından incelenmiştir. Almanya'nın güvenlik anlayışındaki yapısal ve kavramsal kırılmalar söz konusu akademisyenler tarafından eleştirel güvenlik çalışmaları bağlamında ele alınmıştır. Didier Bigo, Almanya gibi Avrupa ülkelerinde göçmenlerin nasıl bir "tehdit" unsuru haline getirildiğini analiz ettiği çalışmasında, süreci "güvenlikleştirme" kavramı üzerinden açıklamıştır. Bigo'ya göre göç, suç ve terörizm gibi olgular, politika yapıcılar tarafından kasıtlı olarak güvenlikleştirilerek, kamuoyunda "huzursuzluk hali" yaratılmaktadır. Bu yaklaşım, Almanya'nın 2000'li yıllardan itibaren özellikle göçmen topluluklara yönelik güvenlik odaklı yaklaşımlarını anlamada kritik bir çerçeve sunar. Bigo'ya göre, "liberal rejimler tarafın-

dan uygulanan illiberal uygulamalar, terör korkusu bahane edilerek kamusal özgürlükleri tehdit etmektedir" (Bigo, 2002:66). Almanya'nın özellikle 11 Eylül sonrasında iç ve dış güvenlik alanlarını birleştirerek, göçmenleri potansiyel tehdit olarak konumlandırması bu yaklaşımın pratik örneklerinden biridir (Bigo, 2008, s. 34). Bigo bir diğer çalışmasında Almanya gibi Schengen üyesi ülkelerin serbest dolaşımı korumaya çalışırken aynı zamanda sınır kontrollerini dışsallaştırarak güvenlik politikalarını sınırların ötesine taşıdığını ifade etmiştir (Bigo ve Guild, 2005:2). Sınır güvenliği konusunda alınan önlemler Avrupa yurttaşlığı idealinden ciddi bir sapma olarak değerlendirilmektedir (Çıdam, 2025:168). Diğer yandan Bigo, Almanya'nın AB'nin veri temelli gözetim araçlarını aktif biçimde kullandığını ve böylelikle gelen göçmenlerin biyometrik izleme, veri eşleştirme gibi yöntemlerle önceden tanımlanarak "risk puanlamasına" tabi tutulduğunu ifade etmektedir (Bigo, 2014:215).

Lucia Zedner ise güvenlik politikalarının normatif çerçevesini sorgulayarak, "güvenlik" kavramının çoğu zaman tek boyutlu algılandığını vurgulamıştır. Bu algı zamanla hukuk devleti ilkeleriyle çelişebilmektedir. Zedner'e göre, Almanya gibi liberal demokratik ülkelerde güvenliğin "negatif" (tehditten korunma) ve "pozitif" (özgürlüğün güvence altına alınması) yönleri birlikte değerlendirilmelidir (Zedner, 2003:157). Almanya Federal Anayasası, bir yandan temel hak ve özgürlükleri güvence altına alırken diğer yandan, alınan güvenlik tedbirleri ile bu haklar zedelenebilmektedir. Zedner, ceza adalet sisteminin "önleyici" tedbirlere yönelmesinin, bireylerin haklarını henüz suç işlenmeden sınırlayabileceğini vurgulamıştır (Zedner ve Ashworth, 2014:65). Son olarak Almanya'nın güvenlik paradigmasının risk yönetimi ve terör korkusu etrafında yeniden şekillendiği ifade etmiştir (Zedner, 2012:34). Güvenlik meselesi teknik bir hâl aldıkça, polisin ya da adli sistemin sorumluluğunun yanında teknoloji şirketlerinin ve veri merkezlerinin sorumluluğu da devreye girmektedir. Zedner buradan yola çıkarak güvenliğin teknikleştikçe hukuki denetimin dışına taşma eğilimi gösterdiğini vurgulamıştır. (Zedner, 2012:11).

Güvenlik politikalarının strateji belgeleri üzerinden analiz edilmesi, devletlerin güvenlik anlayışındaki dönüşümleri, önceliklerini ve yönetişim yaklaşımlarını sistematik biçimde ortaya koyma açısından güçlü bir çerçeve sunmaktadır. Bu çerçevede yapılan literatür taramasında, farklı ülkelerde güvenlik belgeleri temelinde yürütülen çalışmalar dikkat çekmektedir. İngiltere, ABD, Fransa ve Türkiye gibi ülkeler güvenlik stratejilerinde güvenlik kavramının askerî tehditlerden çok daha öteye geçtiğini gösteren örnekler sunmaktadır. Bu bağlamda aşağıda, söz konusu ülkelerde strateji belgeleri üzerinden yürütülmüş çalışmalar derlenmiştir.

Claire Cassedy yapmış olduğu çalışmada İngiltere'nin strateji belgelerini güvenlik ekseninde incelemiştir. Çalışma neticesinde "güvenlik" kavramının zamanla ulusal savunma çerçevesini aşarak ekonomik istikrar, enerji güvenliği ve toplumsal bütünlüğü de içerecek biçimde genişlediği tespit edilmiştir (Cassedy, 2013:42). Bu kavramsal genişleme, özellikle 11 Eylül sonrası dönemde belirginleşmiştir. Cassedy'nin çalışmasında dikkat çeken bir başka bulgu, İngiltere'nin güvenlik belgelerinde "katılımcı güvenlik" anlayışının ABD'ye kıyasla daha belirgin biçimde vurgulanması olmuştur. Buna göre ABD belgelerinde, güvenliğin daha çok merkezi devlet mekanizması tarafından sağlanan bir hizmet gibi sunulduğu görülürken, İngiltere'de bu sorumluluk alanının paylaşıldığı ifade edilmiştir (Cassedy, 2013:65).

Peter Layton ise İngiltere'nin strateji belgelerinde güvenlik politikalarının büyük strateji, risk yönetimi ve fırsatçılık olmak üzere üç temel yaklaşım arasında salındığını belirtmiştir (Layton, 2015:300). Diğer yandan Layton karar alıcıların risk temelli planlama yaparken "stratejik esneklik" iddiasında bulunduğunu, ancak bu esnekliğin belgede belirsizlik yarattığını vurgulamıştır. İncelemiş olduğu belgelerin genel olarak bir yandan geniş coğrafi etki alanına sahip olmak isteyen bir dış politika vizyonu sunarken, diğer yandan bütçe temelli tehdit önceliklendirmesi yaptığını ifade etmiştir. Bu durumun belgelerin uygulamada net bir stratejik yön çizememesine neden olduğunu vurgulamıştır (Layton, 2015:301).

Anne Hammerstad ve Ingrid Boas'ın söylem analizi çalışması, İngiltere'nin 2010'lara ait Ulusal Güvenlik Stratejisi belgelerinde risk kavramının belirgin biçimde ön plana çıktığını ortaya koymuştur (Hammerstad ve Boas, 2015:258). Hammerstad ve Boas ayrıca strateji belgelerinde "önlenemez belirsizlik" anlatısının öne çıktığını ve bu durumun kamuoyunda sürekli bir güvensizlik atmosferi oluşturduğunu belirtmiştir. Yazarlar, strateji belgelerinde dile getirilen risk söyleminin gelecekteki potansiyel kriz senaryolarını da kapsayacak şekilde genişletildiğini tespit etmiştir (Hammerstad ve Boas, 2015:464).

Yine Ettinger'ın 2018 tarihli başka bir çalışması, ABD'nin 2017 "Ulusal Güvenlik Stratejisi"ni analiz etmiştir. Ettinger, "Önce Amerika" söyleminin yerleşik dış politika normlarıyla çatıştığını savunmuştur (Ettinger, 2018:141). Diğer yandan strateji belgelerinde süreklilik vurgusunun özellikle ABD'nin küresel liderlik rolü bağlamında ortaya çıktığını belirtmiştir. Soğuk Savaş sonrası tüm stratejilerde Amerikan liderliğinin istikrar sağlayıcı unsur olarak sunulduğu; bu nedenle dış politika doktrinlerinin söylem düzeyinde farklılaşsa da öz itibarıyla benzer hedefleri sürdürdüğü vurgulanmıştır (Ettinger,

2017:36). Song ve arkadaşları tarafından yürütülen karşılaştırmalı bir analizde, ABD ve İngiltere'nin ulusal siber güvenlik stratejileri, konu modelleme tekniğiyle incelenmiştir. Çalışma, bu iki ülkenin önceliklerinde yapısal farklılıklar bulunduğunu ve ABD'nin daha merkezî bir tehdit tanımı geliştirirken, İngiltere'nin daha çok kamu-özel sektör işbirliğine dayalı bir yapı benimsediğini göstermektedir (Song vd., 2021:8).

Ahmet Emre Köker'in (2022) çalışması, Fransa'nın ulusal siber güvenlik stratejisini inceleyerek, bu ülkenin dijital tehditlere karşı geliştirdiği kurumsal kapasiteyi ve resmi strateji belgelerini analiz etmektedir. Çalışmada Fransa'nın 2008 tarihli "Beyaz Kitap" ile birlikte siber güvenliği ulusal güvenliğin temel bileşeni olarak tanımladığı belirtilmiştir (Köker,2022:3). Ayrıca, Köker'in çalışmasında Fransa'nın siber stratejisinin beş temel hedef üzerine inşa edildiği aktarılmaktadır. Bu hedefleri "vatandaşların korunması, kamu kurumlarının dirençliliğinin artırılması, farkındalık düzeyinin yükseltilmesi, Avrupa düzeyinde iş birliği ve teknoloji geliştirme" şeklinde sıralamak mümkündür (Köker, 2022:4). Bu hedefler, Fransa'nın dijital güvenliği hem iç tehditlere karşı koruma hem de küresel norm inşası aracı olarak kullandığını göstermektedir. Ahmadi'nin çalışmasında Fransa'nın güvenlik politikaları "stratejik kültür" çerçevesinde ele alınmakta ve resmi strateji belgeleri üzerinden Avrupa savunma iş birliğine yaklaşımları değerlendirilmektedir. Ahmadi, Fransa'nın 2013 ve 2017 "Beyaz Kitapları" ile 2018 "Stratejik Gözden Geçirme" belgesini analiz ederek, Fransa'nın hem ulusal egemenliğini koruma hem de Avrupa stratejik özerkliğini güçlendirme çabalarını vurgulamaktadır (Ahmadi, 2021:18).

Akın Aytekin'in çalışması, Türkiye'nin "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı"nı analiz ederek bu alandaki bir sistematik değerlendirme sunmuştur. Aytekin'e göre, Türkiye'nin stratejik belgelerinde siber tehditlerin önemine dair farkındalık artmış olsa da, uygulama ve kurumsal koordinasyon açısından önemli eksiklikler bulunmaktadır (Aytekin, 2015:49). Çalışma, Türkiye'nin siber güvenlik yaklaşımının daha çok reaktif bir çerçevede kaldığını, önleyici stratejilerin yeterince gelişmediğini vurgulamaktadır. Ayrıca, Aytekin'in İngiltere ve ABD'nin siber güvenlik stratejileriyle yaptığı karşılaştırma sonucunda, Türkiye'nin belgesinin daha az teknik ayrıntı içerdiği ve sektörler arası iş birliğinin stratejik belgede yeterince yapılandırılmadığı görülmektedir (Aytekin, 2015:58). Yazar, belgenin revize edilerek daha ölçülebilir hedefler içermesi, özel sektör ve akademiyle entegrasyonu güçlendirmesi gerektiğini belirtmektedir. Murat Aslan'ın çalışması, Türkiye'nin güvenlik anlayışındaki kavramsal dönüşümü dönemsel olarak ele almıştır. Özellikle 2000 sonrası döneme odaklanmıştır. Aslan, Türkiye'nin güvenlik anlayışının

Soğuk Savaş sonrası süreçte giderek genişlediğini, askeri tehditlerin yanı sıra enerji, gıda, çevre gibi konuların da güvenlik belgelerine girdiğini belirtmektedir (Aslan, 2022:295). Ayrıca, Türkiye'nin son yıllarda daha proaktif ve yer yer müdahaleci olarak nitelenebilecek bir güvenlik stratejisi geliştirdiği vurgulanmaktadır.

Güvenlik Kavramının Dönüşümü: Almanya Örneği

Güvenlik kavramının anlamı tarihsel süreç içerisinde anlamı birçok kez dönüşmüştür. Başlangıçta bireyin fiziki varlığını koruma amacıyla tanımlanan güvenlik, modern dönemde devletlerin sınırlarını ve egemenliğini önceleyen askeri bir olgu olarak konumlandırılmıştır (Birdişli, 2017:63). Özellikle modern devlet sisteminin 1648 Vestfalya Anlaşması ile şekillenmesi ile beraber güvenlik kavramı, ulusal sınırlar içerisinde devletin tekelinde bir işlev olarak yapılandırmıştır. Güvenliğe dair bu kavrayış, Soğuk Savaş dönemine kadar neredeyse tartışmasız biçimde kabul görmüştür (Gözen, 2015:70). Soğuk Savaş boyunca uluslararası ilişkilerde baskın paradigma niteliğinde olan realizm, güvenliği sıklıkla askeri kapasiteyle ilişkilendirmiştir. Bu doğrultuda devletin güvenliğini sağlamak amacıyla caydırıcılık, savunma ve güç dengesi gibi araçları ön plana çıkardığı görüşünü ortaya koymuştur (Walt, 1991:212).

Ancak 1970'li yıllardan itibaren yaşanan bazı sorunlar güvenliğin sadece askeri tehditlerle sınırlı bir mesele olmadığını ortaya koymuştur. Söz konusu sorunlara enerji krizleri, çevresel felaketler, terör olayları ve küresel ekonomik dalgalanmalar örnek olarak verilebilir. Nitekim bu dönemden itibaren güvenlik kavramı hem genişlemiş hem de derinleşmiştir (Buzan vd.,1998:25). Bu noktada genişleme vurgusu güvenliğin yalnızca askerî alanla sınırlı kalmayıp siyasi, ekonomik, toplumsal ve çevresel boyutları da kapsayacak şekilde çok boyutlu hâle gelmesini ifade ederken; derinleşme ise güvenliğin yalnızca devlet düzeyinde değil, birey, toplum ve küresel aktör düzeyinde de değerlendirilmesi anlamına gelmektedir (Bilgin, 2006:15). Bu dönüşümle birlikte uluslararası ilişkiler literatüründe yeni güvenlik yaklaşımları kendini göstermiştir. Kopenhag Okulu tarafından ortaya konan "güvenlikleştirme" kavramsallaştırması bu çerçevede önemli bir teorik yenilik olarak kabul edilmiştir (Buzan vd., 1998:32).

Diğer yandan Paris Okulu, güvenlik çalışmalarında eleştirel bir yaklaşımı benimsemiştir. Özellikle güvenliğin nasıl teknikleştiği ve yönetildiği üzerine odaklanan bir ekoldür. Temel farklılığı, güvenliğin yalnızca söylemle değil, pratiklerle, kurumlarla ve gündelik yönetim biçimleriyle kurulduğunu savunmasıdır. En önemli temsilcisi Didier Bigo olan Paris Okulu'na göre gü-

venlik kavramı teknikleştikçe, siyasetin dışına itilmiştir. Böylelikle teknokratik merkezli karar alma süreçleri daha fazla ön plana çıkmıştır. Sonuç olarak devlet dışı aktörler (örneğin polis, sınır muhafızları, veri analistleri, özel güvenlik şirketleri) güvenlik alanını "yönetişimsel" biçimde şekillendirir hâle gelmiştir (Bigo, 2022:34).

Soğuk Savaş'ın ardından güvenlik çalışmalarında ortaya çıkan alternatif yaklaşımlardan biri de Galler Okulu'dur. Bireylerin güvenliğini merkeze alan Galler Okulu'na göre güvenlik teorileri insanların daha güvenli ve özgür bir yaşam sürmesini sağlamaya katkı sunmalıdır. Okulun en dikkat çeken katkısı ise özgürleştirme kavramıdır. Bu kavram, bireylerin ya da toplulukların hayatlarını etkileyen baskılardan, engellerden ve sınırlamalardan kurtulmasını ifade eder. Galler Okulu'na göre yalnızca savaş ya da terör gibi klasik tehditler değil; yoksulluk, eğitimsizlik ve siyasi baskı gibi unsurlar da insanların güvenliğini tehdit eder. Bu anlayışta gerçek güvenlik, askeri güçle değil, bireylerin özgürlük alanlarının genişletilmesiyle sağlanabilir. Bu nedenle, Galler Okulu için güvenlik ve özgürlük birbiriyle yakından ilişkili iki temel değerdir (Çifçi, 2024:154).

Soğuk Savaş'ın sona ermesi uluslararası sistemdeki tehdit algılarının doğasını köklü biçimde değişmiştir. Artık sınır aşan tehditler, devlet dışı aktörler ve öngörülemeyen krizler güvenliğin merkezine yerleşmiştir (Mathews,1989:162). Güvenlik politikaları söz konusu bu gelişmelerden nasibini almıştır. Bu noktada "kimin güvenliği?" sorusuna cevaben "insan güvenliği" yaklaşımı öne çıkmıştır. Böylelikle bireyin yaşam hakkı, sağlık, eğitim, ekonomik istikrar gibi temel ihtiyaçlarının güvenliğin konusu olması gerektiği savunulmuştur (UNDP,1994:22). Aynı şekilde, iklim değişikliği, pandemi gibi küresel tehditler, devlet merkezli güvenlik anlayışının sınırlarını zorlamış ve yönetişim temelli, kapsayıcı güvenlik yaklaşımlarını zorunlu hâle getirmiştir (Kaldor, 2007:91; Nye, 2010:119).

Soğuk Savaş dönemindeki geleneksel güvenlik anlayışı, zaman içerisinde yerini daha geniş kapsamlı ve çok aktörlü bir güvenlik yaklaşımına bırakmıştır (Arslan, 2024:62). Güvenliğe dair bu dönüşümden Almanya da etkilenmiştir. Doğu ve Batı Almanya'nın birleşmesinin ardından terör ve şiddete dayalı eylemlerin arttığı gözlenmiştir (Dilbirliği, 2017:159). Nitekim Almanya'nın kitlesel göç, çevre felaketleri ve bölgesel çatışmalar gibi yeni tehditlere karşı bütüncül bir güvenlik vizyonu geliştirmesi gerekmiştir. Bu noktada güvenlik politikaları dışişleri, içişleri, kalkınma ve istihbarat kurumlarının koordinasyonunu içeren bütüncül bir yapıda şekillenmiştir. Stengel'in analizine göre Almanya, güvenliğini sağlamak için krizleri kaynağında önlemeye

odaklanan, sivil-askeri işbirliğine dayalı, proaktif bir strateji benimsemiştir. Öncesinde çatışma önleme politikaları için formüle edilmiş olan "kapsamlı güvenlik" çerçevesi, artık genel güvenlik politikasının temel direği haline getirilmiştir (Stengel, 2020:37).

Söz konusu dönüşüm, Almanya'nın güvenlik politikalarının uygulayıcı aktörlerini ve meşruiyet zeminini de değiştirmiştir. Soğuk Savaş öncesi güvenlik politikaları büyük ölçüde devletin tekil otoritesiyle şekillenen, askeri tehditlere karşı ulusal çıkar ve egemenlik vurgusuyla meşrulaştırılan bir çerçeveye dayalıdır. Ancak bu çerçeve yerini, çok aktörlü yönetişim yapılarına dayanan ve uluslararası etik sorumluluklarla gerekçelendirilen normatif bir güvenlik anlayışına bırakmıştır (Stengel, 2020:43–45). Güvenliğin yeni doğası, kalkınma yardımları, diplomatik girişimler ve istihbarat faaliyetlerini içerisine almıştır. Böylece Almanya'nın güvenlik politikası, askeri güç kullanımının yanında insan hakları, barış inşası ve küresel yönetişim gibi değerleri de içine alan çok boyutlu bir yapıya kavuşmuştur. Kısacası bu süreçte güvenliğin tanımının genişlediğini ifade etmek mümkündür.

Yukarıda kısaca bahsedilen teorik çerçevedeki dönüşüm, devletlerin resmî güvenlik stratejilerine de yansımıştır. Dijitalleşmenin yaygınlaşmasıyla birlikte siber güvenlik, dezenformasyon, veri güvenliği ve yapay zekâ tabanlı tehditler, yeni güvenlik paradigmasının ana bileşenleri hâline gelmiştir (Singer ve Friedman, 2014:41). Diğer yandan göç dalgasıyla gelen ayrımcılık ve bunun neticesinde alevlenen toplumsal kutuplaşma; aşırıcılık ve radikalleşme gibi toplumsal sorunları da beraberinde getirmiştir (Sankot, 2016:16). Bu konular artık doğrudan ulusal güvenliğin ilgi alanı içinde değerlendirilmektedir (Bigo, 2002:64). Bu nedenle çağdaş güvenlik anlayışı, sadece devletin bekasını merkeze alan anlayışın ötesine geçmiştir (Stewart, 2022:85). Diğer bir ifadeyle çağdaş güvenlik anlayışının bireylerin refahı, kurumların direnci ve toplumun dayanıklılığı gibi faktörleri de içeren bütüncül bir yapı kazandığını ifade etmek mümkündür (Mutlu, 2020:43; Arends, 2015:27).

Tüm bu teorik ve tarihsel çerçeve, Almanya gibi gelişmiş, liberal-demokratik bir hukuk devleti açısından özel bir anlam taşımaktadır. Almanya›nın tarihsel tecrübeleri –özellikle İkinci Dünya Savaşı sonrası militarizmden uzaklaşma ve çok taraflılık politikası benimsemesi– güvenlik politikalarının hem normatif değerlere hem de kolektif iş birliğine dayanmasını sağlamıştır (Berenskoetter, 2005:84). Dış tehditlerin bertaraf edilmesinin yanında, demokrasinin korunması ve geliştirilmesi, toplumsal barışın sağlanması, dijital dünyada yeni tehdit türlerine karşı toplumsal direnç geliştirilmesi gibi konular Almanya'nın güvenlik anlayışında çok katmanlı bir sistem olarak şekillen-

miştir (Sokolov, 2024:56). Nitekim 2023 yılında yayımlanan Ulusal Güvenlik Strateji Belgesi, Almanya'nın klasik askeri güvenlikten çok daha öte bir anlayışı benimsediğini ve güvenliği demokratik değerler, dijital direnç, toplumsal dayanıklılık ve uluslararası iş birliği gibi çeşitli boyutlarda tanımladığını açıkça ortaya koymaktadır (Agafonova, 2024:4).

Bu doğrultuda Almanya'nın güvenlik politikaları toplumun tüm kesimlerini kapsayacak şekilde, önleyici ve direnç odaklı bir strateji inşa etmeye yönelmiştir. Bu strateji tehditleri bertaraf ederek demokratik yaşamın sürekliliğini sağlamayı hedeflemektedir. Almanya'nın güvenlik konusunu salt bir "düzeni koruma" dürtüsüyle ele aldığını ifade etmek zordur. Eğitim politikalarından medya okuryazarlığına, altyapı planlamasından toplumsal kapsayıcılığa kadar pek çok alanda güvenlik politikalarıyla bütünleşik çözümler geliştirilmiştir. Almanya'nın bu kapsayıcı yaklaşımı kendi ulusal çıkarlarının yanında aynı zamanda Avrupa ve küresel güvenlik mimarisini de katkı sunan bir niteliğe sahiptir.

Almanya'da Güvenlik Kurumlarının Strateji Belgeleri

Strateji belgeleri devletlerin belli bir konudaki politik yönelimlerini anlama noktasında kritik öneme sahiptir. Almanya'da kurumların güvenlik politikaları hakkında yayınlanan söz konusu belgeler, kamuoyunun ve parlamentonun bu konuda bilgilendirilmesine olanak sağlayan temel referans metinlerdir (Mirković, 2024:91). Diğer yandan güvenlik strateji belgeleri kurumsal koordinasyonun sağlanmasında da önemli bir işleve sahiptir. Bu noktada kurumsal zihniyeti anlamada bir ayna görevi gören belgeler aynı zamanda geleceğe yönelik eylem planları sunarak farklı birimlerin ortak bir vizyonda birleştirilmesini de sağlamaktadır (Banasik, 2018:189). Diğer bir ifadeyle güvenlik stratejileri teknik metinlerin ötesinde aynı zamanda normatif tercihlerin ve geleceğe dair kolektif vizyonun ifadesi olarak görülmektedir (Taran, 2021:64).

Almanya'da güvenlik alanında çeşitli kurumlar tarafından yayımlanan strateji belgeleri ve raporlar, devletin farklı güvenlik birimlerini ortak bir vizyon etrafında birleştirir. Federal Hükûmet, genel güvenlik siyasetini belirleyen kapsamlı belgeler çıkarmaktadır. Örneğin 2023'te yayınlanan "Ulusal Güvenlik Stratejisi", hükümetin güvenlik perspektifini bütüncül bir şekilde ortaya koymuştur. İç güvenlik konularında stratejiler geliştiren bir diğer kurum, birçok ülkede olduğu gibi, Federal İçişleri Bakanlığı'dır. Örneğin "Ulusal Siber Güvenlik Stratejisi", "Kritik Altyapıların Korunmasına İlişkin Çatı Stratejisi" ve "Afetlere Karşı Dayanıklılığın Güçlendirilmesine İlişkin Strateji" Bakanlıkça hazırlanmıştır. Ek olarak Anayasayı Koruma Teşkilatı ve Fede-

ral Kriminal Dairesi gibi kurumlar her yıl kendi uzmanlık alanlarında durum raporları sunmaktadır. Örneğin Anayasayı Koruma Teşkilatı'nın yayımladığı Anayasayı Koruma Raporu ülkedeki aşırı uç akımlar ve terör tehditlerini değerlendiren bir belge niteliğindedir. Benzer şekilde, Federal Kriminal Dairesi'nin yayınladığı "Polis Odaklı Suçla Mücadele Stratejisi" suç trendlerine dair veriler sunmakla beraber, bu konudaki mücadele stratejilerini kamuoyuyla paylaşmıştır. Farklı kurumların yayımladığı tüm bu belgeler, Alman güvenlik mimarisinde kurumsal koordinasyonu sağlayarak her bir birimin kendi alanındaki bilgi ve öngörülerini ortak bir güvenlik siyaseti doğrultusunda bir araya getirmektedir.

Koalisyon Anlaşması (2021-2025)

2021 yılında Almanya'da Sosyal Demokrat Parti, Yeşiller ve Hür Demokrat Parti arasında imzalanan "*2021–2025* Koalisyon Anlaşması", iç güvenlik politikalarında reformist ve dijitalleşme odaklı bir güvenlik anlayışını benimsemektedir. Bu belge, klasik kamu güvenliği çerçevesini genişleterek insan hakları, şeffaflık, teknolojik denetim mekanizmaları ve polis reformları gibi alanları da kapsamaktadır. Belgeden elde edilen dört temel kodu "polis teşkilatının demokratik denetime açık şekilde reforme edilmesi", "dijital gözetim araçlarının yasal çerçeveye oturtulması", "yapısal ırkçılıkla mücadele kapsamında polis eğitimlerinin yeniden yapılandırılması" ve "kolluk kuvvetlerinin toplumsal meşruiyetinin güçlendirilmesi" şeklinde sıralamak mümkündür (Koalisyon Anlaşması, 2021:96–101).

Polis teşkilatının reformu kapsamında federal ve eyalet düzeyinde şeffaflık komisyonları kurulması, veri koruma kurallarına uygun denetim sistemlerinin uygulanması ve hata yapan kolluk görevlileri için disiplin süreçlerinin hızlandırılması önerilmektedir (Koalisyon Anlaşması, 2021:97). Dijital gözetim teknolojilerinin kullanımı ise yalnızca orantılılık ve yargı denetimi ilkesine bağlı olarak mümkün kılınmış; özellikle yüz tanıma teknolojileri ve veri madenciliği araçlarının sınırlandırılması öngörülmüştür (Koalisyon Anlaşması, 2021:98). Yapısal ırkçılıkla mücadele amacıyla polis akademilerinde çeşitliliğe duyarlı eğitim modülleri ve bağımsız araştırmalar yapılması teşvik edilmektedir (Koalisyon Anlaşması, 2021:99). Son olarak kolluk kuvvetlerinin toplumla olan ilişkisinin güçlendirilmesi amacıyla güven artırıcı önlemler, katılımcı denetim mekanizmaları ve sivil toplumla diyalog geliştirme programları gündeme getirilmiştir (Koalisyon Anlaşması, 2021:100). Bu belge, Almanya'nın kamu güvenliği paradigmasında demokratik değerler ile

güvenlik uygulamaları arasında denge kurma çabasını yansıtmaktadır. Kodları şu şekilde tablolaştırmak mümkündür:

Tablo 2. Kodların Koalisyon Anlaşması'ndaki Görünürlülüğü

Kodlar	Açıklama	Öne Çıkan Politikalar
Polis Teşkilatında Demokratik Reformlar	Kolluk kuvvetlerinin denetlenebilirliğini artırmak ve şeffaflık sağlamak	Şikâyet mekanizmaları, bağımsız izleme komisyonları, hata yapan görevliler için açık disiplin süreci
Dijital Gözetimin Hukuki Sınırlandırılması	Gözetim teknolojilerinin yalnızca hukuki zemine oturtularak kullanılması	Yüz tanıma sistemlerinin sınırlandırılması, dijital araçların yargı denetimine tabi olması
Polis Eğitimlerinde Irkçılıkla Mücadele	Yapısal ayrımcılığı azaltmak amacıyla polis akademilerine insan hakları temelli eğitim eklenmesi	Çeşitlilik eğitimi, akademik denetim, bağımsız araştırmaların desteklenmesi
Toplumsal Meşruiyetin Güçlendirilmesi	Kolluk kuvvetleri ile toplum arasında güven inşasına yönelik politika önerileri	Diyalog atölyeleri, sivil toplumla iş birliği, polis-vatandaş ilişkilerini geliştiren projeler

Siber Güvenlik Strateji Belgesi (2021)

Almanya'nın dijital güvenlik politikalarını belli bir sistem üzerine oturtan "*Siber Güvenlik Strateji Belgesi*", Federal İçişleri Bakanlığı tarafından 2021 yılında yayımlanmıştır. Söz konusu belge, devlet kurumlarından özel sektöre kadar siber tehditlere yönelik çok katmanlı bir koruma anlayışını ön plana çıkarmaktadır. Belgede kamu kurumlarının dijital direnç kapasitesinin artırılması, yapay zekâ ve veri analitiği tabanlı erken uyarı sistemlerinin geliştirilmesi, kritik altyapıların siber güvenlik standartlarının güncellenmesi ve bireysel dijital farkındalık ve siber okuryazarlık düzeyinin yükseltilmesi şeklinde 4 kod belirlendiği görülmektedir.

Öncelikle kamu kurumlarına yönelik olarak yazılım ve sistem mimarisinin kurgulanırken güvenlik konusunun merkeze alınması gerektiği vurgulanmıştır (Federal İçişleri Bakanlığı, 2021:17). Diğer yandan yapay zekâ destekli erken tespit sistemlerine dikkat çekilmiştir. Bu konuyla ilgili olarak, tehditlerin geleneksel yöntemlerle tespit edilemediği durumlarda algoritmik analiz ve otomatik istihbarat toplama kapasitesinin önemine dikkat çekilmiştir (Federal İçişleri Bakanlığı, 2021:22). Kritik altyapılar kapsamında

ise enerji, sağlık, finans ve ulaşım gibi sektörlerdeki dijital sistemlerin risk analizlerinin düzenli aralıklarla yapılmasının altı çizilmiştir. Hatta bu sistemlerin güvenlik seviyelerinin ölçümünde şeffaf kriterlerle göz önünde bulundurulması önerilmektedir (Federal İçişleri Bakanlığı, 2021:28). Son olarak, vatandaşların dijital tehditlere karşı korunmasında toplumsal farkındalığın artırılması, medya okuryazarlığı eğitimi ve bireylerin siber hijyen konusunda bilinçlendirilmesi hedeflenmiştir (Federal İçişleri Bakanlığı, 2021:33). Bu doğrultuda belge, siber güvenlik konusuna sadece teknik açıdan yaklaşmamış, aynı zamanda bu alanı toplumsal bir sorumluluk alanı olarak da yeniden tasarlamaya çalışmıştır. Belgede yer alan söz konusu kodları şu şekilde tablolaştırmak mümkündür:

Tablo 3. Kodların Siber Güvenlik Strateji Belgesi'ndeki Görünürlüğü Tablosu

Kod	**Açıklama**	**Öne Çıkan Politikalar**
Kamu Kurumlarında Dijital Direnç	Devlet sistemlerinin güvenlik mimarisi açısından yeniden yapılandırılması	Yazılım ve donanım altyapısının güvenlikli inşa edilmesi
Yapay Zekâ Destekli Erken Uyarı Sistemleri	Algoritmik tehdit tespiti ve otomatik saldırı izleme sistemlerinin yaygınlaştırılması	AI tabanlı istihbarat sistemlerinin entegrasyonu, tehdit senaryolarına göre veri analiz altyapısı kurulması
Kritik Altyapıların Güvenlik Standartları	Enerji, finans, sağlık gibi sektörlerdeki sistemlerin güvenlik denetimi	Sektörlere özel siber güvenlik rehberleri ve zorunlu güvenlik testleri
Bireysel Dijital Farkındalık ve Siber Okuryazarlık	Bireylerin dijital tehditlere karşı bilgilendirilmesi, davranışsal direncin arttırılması	Okullarda ve kamu spotlarında siber hijyen eğitimi, medya okuryazarlığı kampanyaları

Polis Odaklı Suçla Mücadele Stratejisi (2022)

Almanya Federal Kriminal Dairesi tarafından 2022 yılında yayımlanan belge, *suçla mücadele konusunda* toplumsal direnci artıran, teknolojiye dayalı ve önleyici yöntemlerin gerekliliğini vurgulamaktadır. Bu kapsamda analiz edilen belgede dört ana kod öne çıkmaktadır. Bu kodları "organize suça karşı ulusal ve uluslararası istihbarat koordinasyonu", "siber suçlarla mücadelede teknik kapasitenin artırılması", "finansal suçlarla mücadelede şeffaflık ve izleme sistemlerinin güçlendirilmesi" ve "suç önleme politikalarında toplum temelli iş birliklerinin teşvik edilmesi" şeklinde sıralamak mümkündür (Almanya Federal Kriminal Dairesi, 2022:8–14).

Organize suçla mücadelede öncelik, çok aktörlü veri paylaşım platformlarının kurulması ve sınır ötesi suç şebekelerine karşı Avrupa merkezli iş

birliklerinin artırılması olarak tanımlanmıştır (2022:9). Siber suçlara karşı ise yapay zekâ temelli analiz araçları ve dijital kanıt toplama kapasitesinin geliştirilmesi ön plandadır (mümkündür (Almanya Federal Kriminal Dairesi,2022:11). Finansal suçlarla mücadelede ise şüpheli para hareketlerinin tespiti için finansal istihbarat birimlerinin güçlendirilmesi önerilmektedir (2022:13). Son olarak suç önleme politikalarında, yerel yönetimlerin, STK'ların ve eğitim kurumlarının güvenlik süreçlerine katılımı desteklenmiştir (2022:14). Belge, suçla mücadelede toplumsal direncin artırılması ve risklerin erken aşamada tespiti ilkelerini esas almaktadır.

Tablo 4. Kodların Polis Odaklı Suçla Mücadele Stratejisi'ndeki Görünürlüğü

Kod	Açıklama	Öne Çıkan Politikalar
Organize Suçlara Karşı İstihbarat Koordinasyonu	Ulusal ve uluslararası düzeyde suç ağlarına karşı bilgi paylaşımı ve birlikte operasyon	Europol ve Interpol iş birlikleri, sınır ötesi veri analiz platformlarının kurulması
Siber Suçlarla Mücadelede Teknik Kapasite	Polis teşkilatının dijital tehditlere karşı teknolojik donanım ve personel altyapısının güçlendirilmesi	Yapay zekâ tabanlı analiz, siber adli tıp laboratuvarları, darknet gözlem araçları
Finansal Suçlarla Mücadelede Şeffaflık	Kara para aklama ve finansal dolandırıcılıklara karşı izleme ve raporlama sistemlerinin güçlendirilmesi	Finansal İstihbarat Birimi (FIU) reformu, dijital para takibi, AML direktiflerine uyum
Toplum Temelli Suç Önleme Yaklaşımı	Yerel düzeyde halkın, belediyelerin ve STK'ların suç önleme süreçlerine dahil edilmesi	Mahalle güvenlik projeleri, okul temelli farkındalık çalışmaları

Afetlere Karşı Dayanıklılığın Güçlendirilmesine İlişkin Strateji Belgesi (2022)

Almanya' da Federal Hükümet, 13 Temmuz 2022 tarihinde Federal İçişleri Bakanlığı tarafından sunulan "Afetlere Karşı Dayanıklılığın Güçlendirilmesine İlişkin Strateji"sini kabul etmiştir. Bu stratejinin genel olarak odak noktası sürdürülebilirlik, iklim koruma ve uyum, kentsel gelişim, dijitalleşme vb. gibi ilgili politika alanlarındaki uygulamaların aynı zamanda risk önlemeyi iyileştirmek noktasında nasıl kullanılabileceğidir. Bu doğrultuda federal hükümetin geniş yelpazedeki tehditlerin etkilerine zamanında ve etkili bir şekilde direnebilmesi, bunları karşılayabilmesi, uyum sağlayabilmesi ve bunlardan kurtulabilmesi için bazı önlemler formüle edilmiştir (Federal İçişleri Bakanlığı, 2022).

Belgede "dayanıklılık" kavramı tehlikelere maruz kalan bir sistemin, risk yönetimi yoluyla temel işlevlerini koruyup eski haline getirerek, zamanında ve etkin bir şekilde tehlikenin etkilerine direnme, uyum sağlama, dönüştürme ve toparlanma yeteneğini olarak tanımlanmıştır (Federal İçişleri Bakanlığı, 2022:5). Bu doğrultuda stratejinin genel amacı toplumun mevcut ve gelecekteki riskler konusunda bilgilendirilmesine yardımcı olmak olarak belirlenmiştir. Dayanıklılık stratejisi federal hükümete, yetkililere ve diğer federal hükümet kurumlarına yönelik tedbirleri içermektedir. Aynı zamanda özel kişilerden eyalet, belediye, sivil toplum, iş dünyası, bilim ve medya temsilcilerine kadar her kesimi sorumluluk altına almıştır.

Belgeye yönelik gerçekleştirilen analizde dört ana kod tespit edilmiştir. Söz konusu kodları "çok düzeyli yönetişimde dayanıklılık odaklı reformlar", "kamu kurumları için risk tabanlı hazırlık sistemleri", "kriz sonrası toparlanma için kurumsal öğrenme süreçleri" ve "toplumsal kapasite geliştirme yoluyla bireysel sorumluluğun artırılması" şeklinde sıralamak mümkündür.

Çok düzeyli yönetişim vurgusu, federal yapı ile eyaletler ve yerel yönetimler arasındaki eşgüdümün kriz anlarında sürdürülebilir dayanıklılık açısından belirleyici olduğunu ortaya koymaktadır (Federal İçişleri Bakanlığı, 2023:9). Bu yapı sayesinde yerel düzeydeki aktörlerin krizlere etkin biçimde müdahale edebilmesi amaçlanmıştır. Nitekim yerel kapasitenin güçlendirilmesi, yerel aktörlerin etkinliğini artıracaktır. Bu bağlamda yerel yönetimlerin karar alma süreçlerine daha fazla entegre edilmesi, tepki sürelerini kısaltmakta ve müdahale kalitesini yükseltmektedir. Ayrıca, yönetişim mekanizmalarında süreklilik sağlayan kurumsal hafıza, kriz tepkilerinde tutarlılık açısından kritik bir rol oynamaktadır. Kurumsal hazırlık sistemleri kapsamında ise risk senaryolarına göre özelleştirilmiş erken uyarı sistemleri, müdahale kapasitesi ve hizmet sürekliliği analizleri talep edilmektedirn(Federal İçişleri Bakanlığı, 2023:14). Söz konusu analizler insan kaynağı ve organizasyonel esnekliği de kapsamaktadır. Ayrıca, kurumlar arası bilgi paylaşımının hızlı ve şeffaf biçimde sağlanması, erken uyarı sistemlerinin etkinliğini artırmaktadır. Kurumların kriz sonrası dönemde öğrenme süreçlerine ağırlık vererek yeniden yapılanmaları teşvik edilmektedir (Federal İçişleri Bakanlığı, 2023:17). Toplumsal kapasite geliştirme konusunda ise halkın afet bilinci, öz yardım becerileri ve katılım mekanizmalarına erişiminin teşvik edildiğini söylemek mümkündür (Federal İçişleri Bakanlığı, 2023:21). Genel anlamda belgede yer alan kodları şu şekilde tablolaştırmak mümkündür:

Tablo 5. Kodların Afetlere Karşı Dayanıklılığın Güçlendirilmesine İlişkin Strateji Belgesi'ndeki Görünürlülüğü

Kod	Açıklama	Öne Çıkan Politikalar
Dayanıklılık Odaklı Yönetişim Reformları	Federal ve eyalet kurumları arasında risk tabanlı eşgüdüm sistemlerinin oluşturulması	Çok düzeyli koordinasyon mekanizmaları, merkezi-dayanıklı planlama süreçleri
Kurumlar İçin Risk Tabanlı Hazırlık Sistemleri	Kamusal hizmetlerin kesintisiz sürmesi için özelleştirilmiş erken uyarı ve senaryo sistemleri	Kamu kurumlarında hizmet sürekliliği planları, kriz bazlı risk analizleri
Kurumsal Öğrenme ve Yeniden Yapılanma	Kriz sonrası dönemde kamu yönetiminde öğrenme temelli reflektif dönüşüm	Performans değerlendirme raporları, iyileştirme odaklı yönetişim döngüsü
Toplumsal Kapasite Geliştirme ve Öz Yardım	Bireylerin kriz anlarında bilinçli ve hazırlıklı hareket edebilmesi	Afet bilinci kampanyaları, gönüllülük eğitimi, toplumsal dayanıklılık merkezleri

Kritik Altyapıların Korunmasına İlişkin Çatı Strateji Belgesi (2023)

Almanya Federal İçişleri Bakanlığı tarafından 2023 yılında yayımlanan "Kritik Altyapıların Korunmasına İlişkin Çatı Stratejisi" devletin ve toplumun işleyişi için hayati öneme sahip altyapı sistemlerini korumayı amaçlayan bütüncül bir güvenlik çerçevesi sunmaktadır. Kritik altyapılar kamu sektörü açısından hayati öneme sahip, arızalanması durumunda kamu güvenliğinde önemli aksamalara yol açabilecek kuruluşlar veya tesislerdir. Enerji ve su temini, ulaşım ve trafik, bilgi teknolojileri ve telekomünikasyon kritik altyapılar arasında yer almaktadır. Analiz kapsamında dört özgül kod tespit edilmiştir: Bu kodları "kritik altyapılar için minimum güvenlik standartlarının belirlenmesi", "sektörler arası bağımlılıkların değerlendirilmesi", "özel sektör ile kamu arasında risk temelli iş birliği mekanizmalarının güçlendirilmesi" ve son olarak "acil durum hazırlık planlarının kurumsallaştırılması" şeklinde sıralamak mümkündür. Söz konusu strateji, "önleme, hazırlık, müdahale ve iyileştirme" döngüsünü merkeze alarak sadece kriz anını değil, kriz öncesi ve sonrası süreçleri de kapsamaktadır (Federal İçişleri Bakanlığı, 2023:5).

Belgede ilk olarak, altyapı operatörleri için zorunlu ve ölçülebilir güvenlik kriterleri geliştirilmesi gerektiği vurgulanmıştır. Bu kapsamda siber güvenlik, fiziksel erişim kontrolü ve kriz iletişimi gibi alanlarda kurumlara yönelik asgari uygulama standartları belirlenmiştir (Federal İçişleri Bakanlığı, 2023:12). Söz konusu standartlar, farklı sektörlerde faaliyet gösteren kurum-

ların eşgüdüm içinde hareket etmesini kolaylaştırmakta ve güvenlik açıklarının sistematik şekilde ele alınmasına olanak tanımaktadır. Ayrıca, güvenlik kriterlerinin ölçülebilir hâle getirilmesi, izleme ve denetim mekanizmalarının işlerliğini artırmaktadır. Sektörler arası bağımlılıklar kodu kapsamında, enerji, sağlık, ulaşım ve bilgi sistemleri arasında ortaya çıkabilecek zincirleme etkilerin modellenmesi gerektiği ifade edilmiştir (Federal İçişleri Bakanlığı, 2023:15). Kamu-özel iş birliği ise kriz yönetiminde risk paylaşımı ve veri akışı konusunda kilit bir unsur olarak öne çıkmakta; özellikle özel sektörün güvenlik planlarına entegrasyonu teşvik edilmektedir (Federal İçişleri Bakanlığı, 2023:18). Son olarak, acil durum senaryolarına hazırlık bağlamında tatbikat zorunlulukları, alternatif hizmet senaryoları ve hizmet sürekliliği planlarının geliştirilmesi önerilmektedir (Federal İçişleri Bakanlığı, 2023:22). Bu strateji, Almanya'nın güvenlik paradigmasında dayanıklılığı kurumsal bir hedef olarak konumlandırmaktadır. Belgede yer alan söz konusu kodları şu şekilde tablolaştırmak mümkündür:

Tablo 6. Kodların Kritik Altyapıların Korunmasına İlişkin Çatı Strateji Belgesi'ndeki Görünürlüğü Tablosu

Kod	**Açıklama**	**Öne Çıkan Politikalar**
Minimum Güvenlik Standartlarının Belirlenmesi	Kritik altyapı işletmeleri için zorunlu kriterlerinin oluşturulması	Siber güvenlik, fiziksel koruma, iletişim güvenliği gibi alanlarda asgari uygulama kılavuzlarının geliştirilmesi
Sektörler Arası Bağımlılık Analizi	Bir sektördeki aksamanın diğer sistemler üzerindeki etkilerinin değerlendirilmesi	Enerji, sağlık ve iletişim gibi alanlar arasında senaryo bazlı kırılganlık modellemeleri yapılması
Kamu-Özel İş Birliği ile Risk Paylaşımı	Devlet ve özel sektör arasında karşılıklı sorumluluk, bilgi akışı ve güvenlik planlaması	Özel sektörün stratejik karar süreçlerine dahil edilmesi, ortak kriz senaryoları hazırlanması
Acil Durum Hazırlık Planlarının Kurumsallaşması	Altyapı sağlayıcılarının afet, siber saldırı ve kesinti senaryolarına hazır hâle getirilmesi	Tatbikat zorunlulukları, yedek altyapı sistemleri, süreklilik ve toparlanma planlarının hayata geçirilmesi

Anayasayı Koruma Raporu (2023)

Bu rapor Almanya Federal Anayasayı Koruma Teşkilatı tarafından her yıl yayımlanan ve anayasal düzene yönelik tehditleri değerlendiren resmî bir güvenlik raporudur. Belge aşırı sağ ve aşırı sol hareketler, dini gerekçeli aşırıcılık, terör örgütlerinin faaliyetleri, yabancı istihbarat servislerinin Al-

manya'daki etkileri, siber tehditler ve dezenformasyon kampanyaları gibi çok boyutlu tehdit alanlarını kapsamlı bir biçimde ele almaktadır. Raporda, hem tehditlerin nitelikleri hem de bu tehditlere karşı alınan önleyici güvenlik önlemleri ayrıntılı şekilde sunulmaktadır. Aynı zamanda anayasal düzenin korunmasına yönelik iç güvenlik politikalarının şekillenmesinde önemli bir referans kaynağı işlevi görmektedir. Kamuoyunu bilgilendirme amacının yanı sıra, demokratik kurumların sürekliliğini sağlamak ve devletin güvenlik vizyonunu yansıtmak açısından da stratejik öneme sahiptir.

2023 yılında yayınlanan rapora göre dört tematik kodun ön plana çıktığı görülmektedir. Bunları "aşırı sağcı ideolojilere karşı önleyici istihbarat faaliyetleri, "dijital dezenformasyonun anayasal düzene etkisi", "dini gerekçeli aşırıcılık ve toplumsal kutuplaşma riskleri", "yabancı istihbarat faaliyetlerinin demokrasiyi hedef alması" şeklinde sıralamak mümkündür (Anayasayı Koruma Teşkilatı, 2023:37). Bu yaklaşım, kamu güvenliğini sadece fiziksel tehditlere karşı değil, aynı zamanda anayasal değerleri zedeleyen sosyo-psikolojik ve dijital tehditlere karşı da korumayı hedeflemektedir.

Raporda aşırı sağ tehdidi hem örgütlü gruplar hem de bireysel radikalleşme süreçleri üzerinden analiz edilmiştir. Bu doğrultuda özellikle genç bireylerin dijital platformlarda radikal içeriklerle karşılaşma oranlarının arttığı vurgulanmıştır (Anayasayı Koruma Teşkilatı,2023:15). Dijital dezenformasyon kampanyalarının Almanya'da seçim süreçleri, toplumsal huzur ve kamu kurumlarına güven üzerinde aşındırıcı etkileri olduğuna dikkat çekilmiş ve bu bağlamda dezenformasyonun sistematik bir tehdit haline geldiği belirtilmiştir (Anayasayı Koruma Teşkilatı,2023:22). Dini gerekçeli aşırıcılıkta ise özellikle Selefi hareketlerin genç Müslümanları etkileme kapasitesine vurgu yapılmıştır (Anayasayı Koruma Teşkilatı, 2023:30). Son olarak, Rusya ve Çin gibi aktörlerin Almanya içindeki siyasi, akademik ve teknolojik kurumlara sızma girişimleri "demokratik düzene dönük dış kaynaklı tehdit" olarak sınıflandırılmıştır (Anayasayı Koruma Teşkilatı,2023:37). Bu belge, anayasa temelli bir kamu güvenliği anlayışının nasıl ulusal ve uluslararası tehditler karşısında yeniden tanımlandığını göstermektedir. Kodları şu şekilde tablolaştırmak mümkündür:

Tablo 7. Kodların Anayasayı Koruma Raporu'ndaki Görünürlüğü

Kodlar	Açıklama	Öne Çıkan Politikalar
Aşırı Sağ Tehdidine Karşı Önleyici İstihbarat	Genç bireylerin radikalleşmesini önlemek ve örgütlü aşırı sağ grupların etkisini azaltmak	Online izleme faaliyetleri, aşırı sağ içeriklerin tespiti, propaganda ile mücadele
Dijital Dezenformasyon ve Demokratik Erozyon	Yabancı aktörlerin sistematik bilgi manipülasyonu yoluyla kamuoyunu etkilemesi	Sosyal medya gözetimi, dezenformasyon ağlarının takibi, kamuoyunu bilinçlendirme stratejileri
Dini Gerekçeli Aşırıcılıkla Mücadele	Selefilik ve diğer radikal grupların genç bireyleri etkilemesinin önlenmesi	Toplumsal katılım projeleri, dini eğitimin denetimi
Yabancı İstihbarat Faaliyetleri ve Demokratik Tehdit	Almanya'daki akademik, siyasi ve teknolojik kurumlara karşı yürütülen casusluk faaliyetleri	Çin ve Rusya kaynaklı sızma faaliyetlerinin takibi, hassas bilgilerin korunmasına yönelik teknik kapasite artırımı

Ulusal Güvenlik Strateji Belgesi (2023)

Almanya Federal Hükûmeti tarafından Haziran 2023'te yayımlanan "Ulusal Güvenlik Stratejisi", hibrit tehditler, siber saldırılar, dezenformasyon, kriz yönetimi ve toplumsal dayanıklılık gibi çok boyutlu konuları içeren bütüncül bir güvenlik yaklaşımını ortaya koymuştur (Almanya Federal Hükûmeti, 2023:8-11). Belgenin içeriğine bakıldığında dört temel kodun öne çıktığı görülmektedir. Bunları "demokratik düzenin korunması", "siber güvenlik ve dijital direnç, " toplumsal dayanıklılık ve krizlere hazırlık", "uluslararası güvenlik iş birlikleri" şekline sıralamak mümkündür.

İlk olarak otoriter rejimlerin etkisine karşı demokrasinin içeride ve dışarıda güçlendirilmesi hedeflenmiştir. Diğer yandan siber güvenlik başlığı altında, dijital altyapıların korunması, kamu kurumlarının dirençli hâle getirilmesi ve özel sektörle iş birliği vurgulanmaktadır. Toplumsal dayanıklılık kodu ise kriz anlarında halkın katılımının sağlanması, eğitim vasıtasıyla toplumsal bilinçlendirme kampanyaları gibi unsurları içermektedir. Uluslararası güvenlik iş birlikleri kodu çerçevesinde ise Almanya'nın NATO ve Avrupa Birliği ile ortak hareket etme kararlılığı açıkça ifade edilmiştir (Almanya Federal Hükûmeti, 2023:11,34,39,49). Belgedeki kodları şu şekilde tablolaştırmak mümkündür:

Tablo 8. Kodların Ulusal Güvenlik Stratejisindeki Görünürlüğü Tablosu

Kod	Açıklama	Öne Çıkan Politikalar
Demokratik Düzenin Korunması	Otoriter etkilere yönelik demokratik kurumların ve değerlerin güçlendirilmesi	Demokrasiye dirençli toplumlar oluşturma, dış etkilerden korunma
Siber Güvenlik ve Dijital Direnç	Dijital altyapıların korunması ve siber tehditlere karşı hazırlıklı olma	Kamu-özel sektör iş birliği, dijital kamu hizmetlerinin güvenli hâle getirilmesi
Toplumsal Dayanıklılık ve Krizlere Hazırlık	Kriz anlarında toplumun dayanıklılığını artırmaya yönelik stratejiler	Sivil savunma planları, afet senaryoları için tatbikatlar, birey odaklı bilinçlendirme
Uluslararası Güvenlik İş Birlikleri	NATO, AB ve diğer kurumlarla güvenlik alanında koordinasyon	Avrupa savunma kapasitesinin güçlendirilmesi

Aşırılıkla Mücadele ve Demokrasi Güçlendirme Stratejisi Belgesi (2024)

Almanya Federal Hükûmeti, 2024 yılında yayımladığı bu belge ile en temelde çoğulcu bir toplumda yaşama hakkını ön plana çıkarmıştır. Bu anlamda her bireyin, siyasi yönlendirmeden uzak, ayrımcılıktan arınmış ve kendi kaderini tayin edebileceği bir yaşam sürme özgürlüğüne sahip olması gerektiği vurgulanmıştır. Bu özgürlük, bireylerin yaşamlarını kendi fikirlerine göre şekillendirme fırsatını da beraberinde getireceğinden, doğal biçimde gelişen çeşitlilik toplumunun ortaya çıkması hedeflenmiştir. Analiz çerçevesinde belgede öne çıkan beş spesifik kod belirlenmiştir: Bu kodları sırasıyla "çocuk ve gençlere yönelik demokratik bilinçlendirme" "radikalleşme riskinin erken tespiti için çok aktörlü izleme sistemleri", "sivil toplum kuruluşlarının desteklenmesi", "dijital aşırılıkla mücadele", "ayrımcılığa uğrayan gruplar için destek mekanizmaları" şeklinde sıralamak mümkündür.

Belge, çocukluk çağından itibaren demokratik değerlerin öğretilmesini radikalleşme ile mücadelede birincil öncelik olarak vurgulamaktadır (Almanya Federal Hükûmeti, 2024:9). Diğer yandan radikalleşmenin erken tespiti için geliştirilen çok aktörlü sistemlerde okul, güvenlik birimleri ve sosyal hizmet uzmanları arasında iş birliği yapılması teşvik edilmektedir (Almanya Federal Hükûmeti, 2024, s. 14). Sivil toplum aktörlerinin güçlendirilmesi ise belgeye göre, toplumsal dayanıklılığı artırmak ve yerel düzeyde demokratik farkındalık yaratmak açısından kritik bir öneme sahiptir (Almanya Federal Hükûmeti, 2024:20). Aşırıcı söylemler genellikle dijital ortamlarda yayılmaktadır. Dijital mecralardaki söz konusu bu söylemlere yönelik medya okuryazarlığı eğitim-

leri ve dijital içerik takibi öne çıkan stratejiler arasında yer almaktadır (Almanya Federal Hükûmeti, 2024:25). Son olarak, belgede yerel danışma merkezlerinden bahsedilmiştir. Bu merkezlerin ayrımcılığa maruz kalan bireylerin desteklenmesi noktasında hukuki yardım ve psiko-sosyal destek hizmeti hedeflenmiştir (Almanya Federal Hükûmeti, 2024:30). Belgede, Almanya'nın güvenlik stratejisinde toplumsal bütünlüğü koruma ve demokratik değerleri güçlendirme konularının merkeze alındığı görülmektedir. Ayrıca bu konuların önleyici güvenlik politikalarıyla bütünleştirildiği de görülmektedir. Belgede yer alan söz konusu kodları şu şekilde tablolaştırmak mümkündür:

Tablo 9. Kodların Aşırılıkla Mücadele ve Demokrasi Güçlendirme Stratejisi Belgesi'ndeki Görünürlüğü

Kod	Açıklama	Öne Çıkan Politikalar
Demokratik Değerlerin Erken Yaşta Aşılanması	GGençler için demokrasi eğitimi ve eleştirel düşünme becerilerinin kazandırılması	Okullarda vatandaşlık eğitimi, eleştirel medya okuryazarlığı
Radikalleşmenin Erken Tespiti İçin Çok Aktörlü Sistemler	Eğitim, güvenlik ve sosyal hizmet aktörleri arasında veri ve bilgi paylaşımı	Gençlik merkezleri, okullar ve yerel kolluk birimleri arasında ortak erken uyarı mekanizmaları kurulması
Sivil Toplumun Güçlendirilmesi	STK'ların desteklenmesi, demokratik katılım projelerinin finanse edilmesi	Hibe programları, yerel demokrasi platformları, gönüllülük temelli toplumsal katılım projeleri
Dijital Aşırılıkla Mücadele	Online platformlarda aşırıcı içeriklerin izlenmesi, dezenformasyona karşı eğitim	Sosyal medya izleme yazılımları, dijital vatandaşlık eğitimi, çevrimiçi nefret söylemiyle mücadele mekanizmaları
Ayrımcılığa Maruz Kalan Gruplar İçin Destek	Etnik, dini ya da sosyal nedenlerle dışlanan bireylerin güçlendirilmesi	Danışma hatları, hukuki yardım ofisleri, psikososyal destek programları

Bulgular

İlk olarak "Demokratik Güvenlik ve Katılımcı Yönetişim" teması, demokrasinin kurumsal olarak korunmasını ve toplumsal katılımın güvenlik yönetişimine entegre edilmesini önceliklendirdiğini ortaya koymaktadır. "Ulusal Güvenlik Stratejisi (2023)", otoriter rejimlere yönelik olarak demokrasiyi güçlendirmeyi hedeflemiştir. Diğer yandan "Koalisyon Anlaşması (2021)"nda ise polis teşkilatının demokratik reformlara tabi tutulması ve dijital gözetim uygulamalarının yasal denetimle kontrol altına alınması

başlıkları vurgulanmıştır. "Aşırılıkla Mücadele Stratejisi ve Anayasayı Koruma Raporu (2024)"nda sivil toplumun güçlendirilmesi ve yapısal ırkçılıkla mücadele gibi önleyici yaklaşımlar ön plana çıkarılarak bu temanın normatif boyutu pekiştirilmiştir. Bu çerçevede "demokratik değerlerin erken yaşta aşılanması", "polis reformları", "toplumsal meşruiyetin güçlendirilmesi" ve "sivil toplumun desteklenmesi" gibi kodlar, temanın kurucu unsurları olarak öne çıkmaktadır.

İkinci olarak "Dijital Güvenlik ve Teknolojik Kapasite" teması Almanya'nın güvenlik belgelerinde dijitalleşme ile gelen tehditlerin çok boyutlu bir şekilde incelendiği görülmektedir. Bu tema genel olarak dijital altyapıların korunması, siber saldırılar ve yapay zekâ destekli erken uyarı sistemleri gibi konuları içermektedir. 2021 tarihli "Siber Güvenlik Strateji Belgesi (2021)", kamu kurumlarında dijital direnç kapasitesinin artırılması ve bireylerin dijital okuryazarlığının yükseltilmesi gibi yapısal hedefler belirlemiştir. "Koalisyon Anlaşması (2021)"nda dijital gözetimin hukuki çerçevede sınırlandırılması, bireysel hak ve özgürlüklerin korunmasına yönelik önemli bir önlem olarak yer almıştır. "Anayasayı Koruma Raporu (2023)"nda dijital dezenformasyonun anayasal düzene etkileri ayrıntılı biçimde değerlendirilmiştir. Bu doğrultuda "kamu kurumlarında dijital direnç", "bireysel dijital farkındalık", "yapay zekâ destekli erken uyarı" ve "dijital gözetimin hukuki sınırlandırılması" gibi kodlar, temanın ana eksenlerini oluşturmuştur.

Üçüncü olarak "Kapsayıcı Dayanıklılık ve Çok Düzeyli Kriz Yönetişimi" temasında federal yapıdaki yönetişim aktörlerinin kriz anlarında nasıl eşgüdüm içinde çalışması gerektiği ele alınmıştır. Bu doğrultuda toplumun krizlere karşı nasıl hazır hâle getirileceği tasarlanmıştır. "Afetlere Karşı Dayanıklılığın Güçlendirilmesine İlişkin Strateji Belgesi (2022)" kriz durumlarının yanına ek olarak, kriz öncesi hazırlık ve kriz sonrası toparlanma süreçlerine dair kapsamlı bir yaklaşım sunmaktadır. Bu belgede yönetişim reformları, kurumsal öğrenme süreçleri ve birey temelli kapasite geliştirme konularının ön plana çıkarıldığı görülmektedir. "Kritik Altyapılar Strateji Belgesi (2023)" ise altyapı hizmetlerinin sürekliliği için minimum güvenlik standartları ve kamu-özel iş birliği modelleri önermektedir. Bu bağlamda "dayanıklılık odaklı yönetişim reformları", "kurumlar için risk tabanlı hazırlık sistemleri", "kurumsal öğrenme ve yeniden yapılanma" ve "toplumsal kapasite geliştirme" kodları bu temanın içeriğini tanımlamaktadır.

Dördüncü olarak "**Önleyici** Güvenlik ve Aşırılıkla Mücadele" teması, aşırılıkla mücadele konusunu erken uyarı mekanizmalarıyla bütüncül olarak ele almaktadır. "Aşırılıkla Mücadele ve Demokrasi Güçlendirme Stratejisi (2024)",

özellikle çocuklar ve gençler için demokratik bilinçlendirme faaliyetlerine öncelik vererek, radikalleşmenin temeline inen bir yaklaşım geliştirmiştir. "Anayasayı Koruma Raporu (2023)" ise sağ tehditlere karşı istihbarat odaklı önleyici güvenlik tedbirlerinin önemine vurgu yapmıştır. Bu temanın temel yapı taşlarını çok aktörlü izleme sistemlerinin kurulması, dijital aşırılıkla mücadele ve ayrımcılığa maruz kalan grupların desteklenmesi gibi konuların oluşturduğunu ifade etmek mümkündür. Bu kapsamda "radikalleşmenin erken tespiti için çok aktörlü sistemler", "dijital aşırılıkla mücadele", "ayrımcılığa uğrayan gruplar için destek" gibi kodlar ön plana çıkmıştır.

Son olarak "Bütünleşik Suçla Mücadele ve İstihbarat İş Birliği" teması Almanya'nın organize suçlar, siber suçlar ve finansal suçlara karşı geliştirdiği istihbarat temelli güvenlik stratejilerini içermektedir. 2022 tarihli "Polis Odaklı Suçla Mücadele Stratejisi (2022)", klasik kolluk yöntemlerinin ötesine geçerek yeni nesil güvenlik uygulamalarını önermektedir. Özellikle organize suçlara karşı uluslararası istihbarat iş birliklerinin artırılması ve Avrupa merkezli güvenlik yapılarıyla entegrasyonu ön plana çıkarmaktadır. "Anayasayı Koruma Raporu (2023)"nda ise yabancı istihbarat faaliyetlerinin demokratik düzene dönük tehdit olarak değerlendirildiği görülmektedir. Bu doğrultuda "organize suçlara karşı istihbarat koordinasyonu", "siber suçlarla mücadelede teknik kapasite", "finansal suçlarla mücadelede şeffaflık" ve "toplum temelli suç önleme" kodları temayı biçimlendirmiştir.

Araştırmanın söz konusu bulgularını şu şekilde tablolaştırmak mümkündür:

Tablo 10. Tematik Bulgular Tablosu

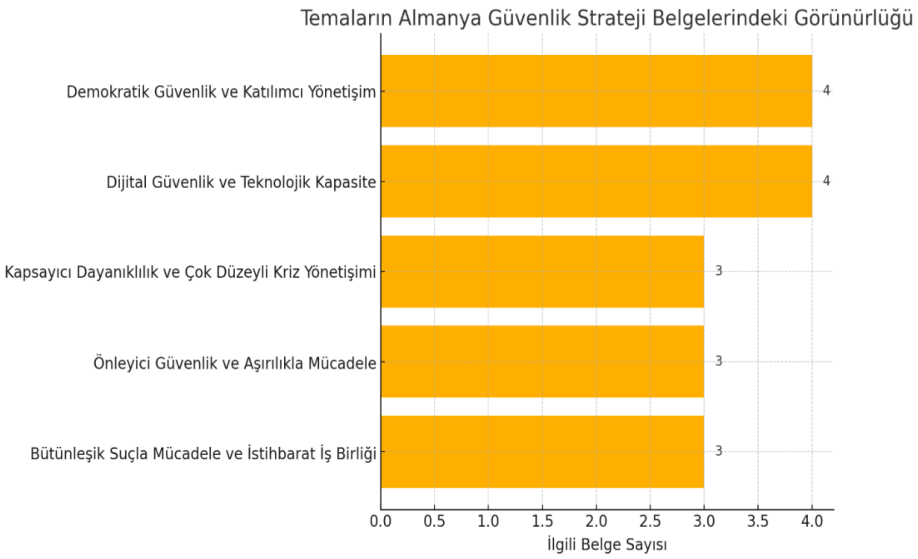
Tema	**Genel Eğilim**	**İlgili Belgeler**
1. Demokratik Güvenlik ve Katılımcı Yönetişim	Demokratik düzenin korunması, polis reformları, yapısal ırkçılıkla mücadele ve sivil toplumun güçlendirilmesi	Ulusal Güvenlik Strateji Belgesi (2023), Aşırılıkla Mücadele Stratejisi (2021), Koalisyonun Ayrılması (2021–2025), Anayasayı Koruma Raporu (2023)
2. Dijital Güvenlik ve Teknolojik Kapasite	Dijital tehditlere karşı kamu kurumlarının dirençli hale getirilmesi, bireysel farkındalığın artırılması ve dijital gözetimin hukuki çerçevede sınırlandırılması öne çıkmaktadır.	Siber Güvenlik Stratejisi (2021), Koalisyon Anlaşması (2021–2025), Anayasayı Koruma Raporu (2023), Ulusal Güvenlik Strateji Belgesi (2023)

3. Kapsayıcı Dayanıklılık ve Çok Düzeyli Kriz Yönetişimi	Federal ve yerel düzeyde kurumsal hazırlık, kriz sonrası öğrenme, halkın afet farkındalığı ve yönetime katılımının artırılması	Ulusal Dayanıklılık Strateji Belgesi (2023), Ulusal Güvenlik Strateji Belgesi (2023), Kritik Altyapılar Stratejisi (2023)
4.Önleyici Güvenlik ve Aşırılıkla Mücadele	Radikalleşmenin önlenmesi, çok aktörlü izleme sistemleri, toplumsal kutuplaşmanın azaltılması politikaları vurgulanmaktadır.	Aşırılıkla Mücadele ve Demokrasi Güçlendirme Stratejisi (2021), Anayasayı Koruma Raporu (2023), Ulusal Suçla Mücadele Belgeleri
5. Bütünleşik Suçla Mücadele ve İstihbarat İş Birliği	Organize suçlar, siber suçlar, finansal suçlar ve uluslararası suç ağlarıyla mücadelede istihbarat paylaşımı, teknik kapasite artırımı ve toplumsal toplam önleme yaklaşımı	Polis Odaklı Suçla Mücadele Stratejisi (2022), Anayasayı Koruma Raporu (2023), Siber Güvenlik Stratejisi (2021)

Sonuç

Bu çalışma, Almanya'nın kamu güvenliği politikalarının strateji belgeleri aracılığıyla sistematik biçimde analiz edilmesi bakımından Türkçe literatürde yer alan sınırlı sayıdaki nitel araştırmalardan biri olma niteliğini taşımaktadır. Bu yönüyle çalışma, güvenlik politikalarının politika belgeleri üzerinden nasıl şekillendiğini gösteren ampirik bir zemin sunmaktadır. Ayrıca, Almanya örneği üzerinden geliştirilen tematik analiz çerçevesi, yalnızca ilgili ülkenin güvenlik stratejilerini kavramaya katkı sağlamakla kalmayıp, aynı zamanda karşılaştırmalı kamu politikası analizlerine dayalı akademik çalışmalara ve çok aktörlü yönetişim yaklaşımlarına dayanan güvenlik kuramlarının ampirik olarak beslenmesine de önemli bir katkı sunmaktadır.

Çalışma, Almanya'nın güvenlik stratejilerinde kendini gösteren yaklaşımları tematik bir analizle ortaya koymuştur. Bu yaklaşımların çok boyutlu, katılımcı ve teknoloji odaklı olduğu görülmektedir. İncelenen sekiz strateji belgesi üzerinden yapılan kodlama çalışması sonucunda ulaşılan beş ana tema **"**Demokratik Güvenlik ve Katılımcı Yönetişim, Dijital Güvenlik ve Teknolojik Kapasite, Kapsayıcı Dayanıklılık ve Çok Düzeyli Kriz Yönetişimi, Önleyici Güvenlik ve Aşırılıkla Mücadele ile Bütünleşik Suçla Mücadele ve İstihbarat İş Birliği" şeklindedir. Genel olarak Almanya'nın güvenlik politikalarına bakıldığında normatif değerlerin korunması, sosyal kırılganlıkların azaltılması ve dijital çağın getirdiği yeni risklerin yönetilmesi konuları en az klasik tehdit algıları kadar önem arz etmektedir.



Şekil 1. Temaların Almanya Güvenlik Strateji Belgelerindeki Görünürlüğü

Yukarıdaki grafik, çalışmada tespit edilen beş ana temanın Almanya'nın güvenlik strateji belgelerindeki görünürlüğünü göstermektedir. Her bir tema en az üç temel politika belgesinde kendisine yer bulmuştur. Bu veriden hareketle güvenlik politikalarının bütüncül ve çok boyutlu bir yapıda geliştirildiğini ifade etmek mümkündür. Özellikle "Demokratik Güvenlik ve Katılımcı Yönetişim" ile "Dijital Güvenlik ve Teknolojik Kapasite" temalarının dört belgeyle temsil ediliyor oluşu, Almanya'nın normatif değerlerle dijital risk yönetimini eş zamanlı olarak güvenlik çerçevesine entegre ettiğini göstermektedir.

21. yüzyılda güvenlik anlayışındaki gelişmeler toplumsal, dijital ve psikolojik alanlardaki tehditlere karşı proaktif müdahaleyi içeren çok katmanlı bir yapıya ihtiyaç duyulduğunu göstermiştir. Böylelikle "önleyici güvenlik" kavramı kamu güvenliği politikalarının merkezine taşınmıştır. Almanya'da özellikle 2021–2024 yılları arasında yayımlanan strateji belgeleri incelendiğinde, güvenlik mimarisinin risklere karşı "öngörü temelli" refleksler geliştirdiği gözlemlenmektedir. Bu bağlamda Lucia Zedner'in suç öncesi müdahale kavramsallaştırması, Alman güvenlik paradigmasının önleyici yönünü anlamak açısından açıklayıcı niteliktedir. Nitekim Zedner çağdaş güvenlik politikalarının gerçekleşme ihtimali olan risklere karşı da müdahaleyi meşrulaştırdığını ifade etmiştir (Zedner, 2007, s. 262). Almanya'nın "radikalleşmenin erken tespiti", "çok aktörlü erken uyarı sistemleri" ve "aşırı sağ tehdidine karşı ön-

leyici istihbarat" gibi kodlarla örneklenen stratejik tercihleri, bu yaklaşımın somut yansımaları olarak değerlendirilebilir.

Diğer yandan, Almanya'nın strateji belgelerinde, teknikleşme ve yönetişim söylemi yoluyla oluşan depolitizasyon iklimini görmek mümkündür. Didier Bigo'nun "güvenliğin profesyonelleri" ve "uzman dilinin siyaseti susturması" şeklinde özetlediği yaklaşım, bu süreci eleştirel biçimde analiz etmeyi mümkün kılar. Bigo'ya göre, güvenlik giderek daha fazla "olağanüstü durum", "acil tehdit" ya da "uzman gerektiren teknik mesele" olarak çerçevelendiğinde, siyasal denetim alanı daralmaktadır. Bu durum güvenliğe dair alınan kararların teknokratik bir zemine kaymasına neden olmaktadır (Bigo, 2002, s. 65). Bu duruma Almanya özelinde bakıldığında, kritik altyapıların korunmasından dijital gözetim teknolojilerine kadar uzanan geniş bir yelpazede düzenlendiği görülmektedir. Almanya'nın güvenlik politikalarını kurumsal uzmanlık temelli bir ağ aracılığıyla yönetmesi, Bigo'nun yönetişimsel güvenlik eleştirisinin çağdaş bir örneği olarak okunabilir.

Strateji belgelerinden elde edilen bulgular, Almanya'nın güvenlik paradigmasında **önleyici, direnç odaklı ve çok aktörlü bir yönetişim anlayışını** benimsediğini ortaya koymuştur. Bu yönelimin en belirgin özelliği, güvenliği yalnızca devletin tekelinde bir işlev olarak değil; bireylerin, kurumların, sivil toplumun ve uluslararası aktörlerin ortak sorumluluğu olarak tanımlamasıdır. Ayrıca güvenlik politikalarının, demokratik normlar, insan hakları, toplumsal meşruiyet ve hukukun üstünlüğü ilkeleriyle uyumlu biçimde kurgulanması, Almanya'nın güvenlik vizyonunu liberal-demokratik bir çerçevede yeniden yapılandırdığını da ortaya koymaktadır. Sonuç olarak, Almanya'nın strateji belgeleri hem normatif değerlerle güvenlik arasında denge kurmayı hem de krizlere karşı sistematik bir toplumsal dayanıklılık inşa etmeyi hedefleyen ileri düzey bir yönetişim modelini temsil etmektedir.

Kaynakça

Agafonova, O. (2024). "Change of Epochs" in German security and defense policy. Izvestiya of Saratov University. Sociology. Politology. https://doi.org/10.18500/1818-9601-2024-24-2-229-235.

Ahmadi, A. (2021). The French Security and Defence Issue: How Does Strategic Culture Help Explain French Views on Common Security and Defence Cooperation? (Bachelor's thesis, Lund University).

Almanya Federal Anayasayı Koruma Teşkilatı (2023). *Anayasayı Koruma Raporu* https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2024-06-18-verfassungsschutzbericht-2023.pdf?__blob=publicationFile&v=17 E.T. 03.06.2025

Almanya Federal Hükûmeti. (2023). *Ulusal Güvenlik Stratejisi* https://www.bmvg.de/en/national-security-policy E.T. 29.10.2024

Almanya Federal Hükûmeti. (2024). *Aşırılıkla Mücadele ve Demokrasi Güçlendirme Stratejisi* https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/ministerium/BMI24021.pdf?__blob=publicationFile&v=8 E.T. 02.03.2025

Almanya Federal İçişleri Bakanlığı. (2021). *Siber Güvenlik Stratejisi.* https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1 E.T.02.02.2025

Almanya Federal İçişleri Bakanlığı. (2022). *Afetlere Karşı Dayanıklılığın Güçlendirilmesine İlişkin Strateji* https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/resilienzstrategie/resilienzstrategie-node.html E.T. 03.03.2025

Almanya Federal İçişleri Bakanlığı. (2023). *Kritik Altyapıların Korunmasına İlişkin Çatı Strateji* https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cybersicherheitspolitik/cybersicherheitspolitik-node.html E.T.02.02.2025

Almanya Federal Kriminal Dairesi (2022). *Polis Odaklı Suçla Mücadele Stratejisi* https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2022/Strategie-OK.pdf?__blob=publicationFile&v=7 E.T. 03.12.2025

Arends, J. (2015). *Güvenliğin Genişlemesi ve Derinleşmesi*. Globacademy.

Arslan, A. C. (2024). Hukuk Devleti ve Kamu Düzeni İlişkisinde Güvenlik Politikalarının Oluşumu. *Liberal Düşünce Dergisi*, (116), 51-74. https://doi.org/10.36484/liberal.1400587

Aslan, M. (2022). Türkiye'de Güvenlik Algısının Kavramsal ve Pragmatik Dönüşümü: Modern Dönemlerin Karşılaştırılması. *Gaziantep Üniversitesi Sosyal Bilimler Dergisi, 21(3), 293–310.*

Aytekin, A. (2015). Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi (Yüksek lisans tezi, Gazi Üniversitesi).

Banasik, M. (2018). Dilemmas of security perception. Scientific Journal of the Military University of Land Forces. https://doi.org/10.5604/01.3001.0012.6222.

Beck, U. (1992). *Risk society: Towards a new modernity* (M. Ritter, Trans.). Sage Publications.

Berenskoetter, F. (2005). Mapping the Mind Gap: A Comparison of US and German Security Cultures. *World Affairs*, 168(2), 83–95.

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. Alternatives: *Global, Local, Political*, 27(1_suppl), 63–92. https://doi.org/10.1177/03043754020270S105

Bigo, D. (2014). The (in)securitization practices of the three universes of EU border control: Military/navy – Border guards/police – Database analysts. Security Dialogue, 45(3), 209–225. https://doi.org/10.1177/0967010614530459

Bigo, D., & Guild, E. (2021). *Security above the law? Exceptionalism and border controls in the time of COVID-19. Movements Journal*, 9(1).

Bigo, D., & Guild, E. (Eds.). (2005). Controlling frontiers: Free movement into and within Europe. Ashgate Publishing.

Bigo, D., & Tsoukala, A. (Eds.). (2008). Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11. Routledge.

Bigo, D., Brouwer, E., Jeandesboz, J., & Hayes, B. (2013). *Mass surveillance of personal data by EU member states and its compatibility with EU law*. Centre for European Policy Studies (CEPS). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2360473

Bigo, D., Carrera, S., Guild, E., & Walker, R. (2008). *Mapping the field of the EU internal security agencies*. Centre for European Policy Studies (CEPS). https://didierbigo.com/wp-content/uploads/2016/03/Mapping.pdf

Bilgin, P. (2006). Uluslararası İlişkilerde Güvenlik Kavramı: Kuramsal Bir Çerçeve. *Uluslararası İlişkiler Dergisi*, 3(11), 3–25.

Birdişli, F. (2017). *Teori ve Pratikte Uluslararası Güvenlik*. Seçkin Yayıncılık.

Buzan, B., Wæver, O., de Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Cassedy, C. P. (2013). National Security Strategies of the US and the UK: An Expansion of "Security" Over Time (Master's thesis). University of North Carolina at Chapel Hill.

Çıdam, E. V. (2025). Post-Ulusal Kimlik ve Geçmişle Yüzleşme Siyaseti: Almanya Örneği. *Liberal Düşünce Dergisi*, (117), 167-183. https://doi.org/10.36484/liberal.1584867 E.T. 05.15.2025

Çifçi, O. (2024). Güvenlik Paradigmasının Dönüşümü ve 21. Yüzyılda Uluslararası Güvenliğin Yeni Gündemi. *Liberal Düşünce Dergisi*, (113), 143-170. https://doi.org/10.36484/liberal.1335666

Dilbirliği, M. (2017). Avrupa aşırı sağının görünüş şekilleri: Almanya örneği. *Liberal Düşünce Dergisi*, (86), 145-168. https://dergipark.org.tr/tr/pub/liberal/issue/48149/609149

Ettinger, A. (2017). U.S. National Security Strategies: Patterns of Continuity and Change, 1987–2015. Comparative Strategy, 36(1), 25–40.

Ettinger, A. (2018). Trump's National Security Strategy: "America First" Meets the Establishment. International Journal, 73(1), 119–132.

Frank A. Stengel, *The Politics of Military Force: Antimilitarism, Ideational Change, and Post-Cold War German Security Discourse* (Ann Arbor: University of Michigan Press, 2020

Gebremeskel, B., Jonathan, G., ve Yalew, S. (2022). Information Security Challenges During Digital Transformation. , 44-51. https://doi.org/10.1016/j.procs.2023.01.262.

Goedecke, M. (2012). The Modernization of the Bundeswehr: A New Trend in Germany's Security Policy.

Gözen, R. (2015). Uluslararası Güvenlik Yaklaşımlarının Tarihsel Gelişimi. *Stratejik Araştırmalar Dergisi*, 2(1), 65–81.

Hammerstad, A., & Boas, I. (2015). National Security Risks? Uncertainty, Austerity and Other Logics of Risk in the UK Government's National Security Strategy. Cooperation and Conflict, 50(4), 454–472.

Kaldor, M. (2007). *New and Old Wars: Organized Violence in a Global Era*. Stanford University Press.

Köker, A. E. (2022). Ulusal Siber Güvenlik Stratejisi: Fransa. Uluslararası Politika Akademisi (UPA).

Layton, P. (2015). The 2015 National Security Strategy and Strategic Defence and Security Review choices: grand strategy, risk management or opportunism?. *Defence Studies*, *15*(1), 28-45.

Mathews, J. T. (1989). Redefining Security. *Foreign Affairs*, 68(2), 162–177.

Miller, R. (2012). Balancing Security and Liberty in Germany. .

Mirković, V. (2024). Germany's Security Management In The Lıght Of The Integrated Security – Current State and Prospect. Scıence International Journal. https://doi.org/10.35120/sciencej0301089m.

Mutlu, B. (2020). Güvenliğin Dönüşen Anlamı: Yeni Tehditler ve Güvenlik Paradigması. *Güvenlik Stratejileri Dergisi*, 16(33), 39–60.

Nye, J. S. (2010). *The Future of Power*. PublicAffairs.

Rhodes, R. A. (2000). Governance and public administration. *Debating governance*, *54*, 90.

Sankot, O. (2016). German foreign and security policy, development and changes in the context of the Islamic State. , 2016, 91-108.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Sokolov, A. (2024). The Concept Of Security In German Foreign Policy. Scientific and Analytical Herald of IE RAS. https://doi.org/10.15211/vestnikieran42024715.

Song, M., Kim, D. H., Bae, S., & Kim, S.-J. (2021). Comparative Analysis of National Cyber Security Strategies using Topic Modelling. International Journal of Advanced Computer Science and Applications, 12(6), 6–13.

Sozialdemokratische Partei Deutschlands [SPD], Bündnis 90/Die Grünen & Freie Demokratische Partei [FDP]. (2021). *2021–2025 Koalisyon Anlaşması:* https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf E.T. 03.03.2025

Stewart, H. (2022). Digital Transformation Security Challenges. Journal of Computer Information Systems, 63, 919 - 936. https://doi.org/10.1080/08874417.2022.2115953.

Taran, Y. (2021). Transforming the Concepts of “State Security” and “National Security” in the System of Public Administration. Scientific Journal the Academy of National Security. https://doi.org/10.53305/2523-4927.2021.30.01.

UNDP. (1994). *Human Development Report*. United Nations Development Programme.

Walt, S. M. (1991). The Renaissance of Security Studies. *International Studies Quarterly*, 35(2), 211–239.

Zedner, L. (2003). The concept of security: An agenda for comparative analysis. Legal Studies, 23(1), 153–176. https://doi.org/10.1111/j.1748-121X.2003.tb00209.x

Zedner, L. (2012). Risiko, Sicherheit und Terrorismus: Drei Konzepte auf der Suche nach einer akademischen Disziplin. Kriminologisches Journal, 10. Beiheft, 30–46.

Zedner, L.(2007). Pre-crime and post-criminology? *Theoretical Criminology*, 11(2), 261–281. https://doi.org/10.1177/1362480607075851

Zedner, L., & Ashworth, A. (2014). Preventive justice. Oxford University Press.