



International Journal of Social Sciences

ISSN:2587-2591

DOI Number:<http://dx.doi.org/10.30830/tobider.sayi.24.8>

Volume 9/4

2025 p. 155-174

YENİ GÜVENLİK TEHDİTLERİ KARŞISINDA ULUSAL GÜVENLİK POLİTİKALARININ DÖNÜŞÜMÜ VE GÜVENLİKLEŞTİRME: SİBER GÜVENLİK, İKLİM KRİZİ VE PANDEMİ DENEYİMİ ÜZERİNE BİR DEĞERLENDİRME

TRANSFORMATION AND SECURITIZATION OF NATIONAL SECURITY POLICIES IN THE FACE OF NEW SECURITY THREATS: AN ASSESSMENT OF CYBERSECURITY, CLIMATE CRISIS, AND THE PANDEMIC EXPERIENCE

Abdullah ÇELİK*

ÖZ

Bu makale, siber güvenlik, iklim krizi ve pandemi gibi 21. yüzyılın yükselen yeni güvenlik tehditlerinin, ulusal güvenlik politikaları üzerindeki etkilerini derinlemesine analiz etmektedir. Geleneksel anlamda devlet merkezli ve askerî temelli güvenlik anlayışı, artık küresel ölçekte etkili olan ve çok aktörlü yapılarla şekillenen bu tehditleri kavramakta yetersiz kalmaktadır. Özellikle küreselleşme süreci, dijitalleşme, devlet dışı aktörlerin etkinliği ve karşılıklı bağımlılık ilişkileri, güvenlik kavramının yeniden tanımlanmasını zorunlu kılmıştır. Bu bağlamda çalışma, Kopenhag Okulu'nun güvenikleştirme kuramı çerçevesinde, yeni tehditlerin söylemsel ve kurumsal olarak nasıl inşa edildiğini ortaya koymaktadır. Siber güvenlik tehditleri, dijital altyapılar, bireysel mahremiyet, ifade özgürlüğü ve devletin egemenlik anlayışı üzerinde de ciddi etkiler yaratmaktadır. İklim krizi, su ve gıda kıtlığı, göç ve toplumsal istikrarsızlık gibi sonuçlar üzerinden güvenlik gündemine dâhil edilirken, pandemiler insan güvenliğinin ve toplumsal dirençliliğinin ne denli hayati olduğunu gözler önüne sermiştir. Makalede Türkiye örneği üzerinden yapılan değerlendirme, bu tehditlere karşı geliştirilen politikaların çoğunlukla tepkisel, sektörel ve parçalı kaldığını göstermektedir. Sonuç olarak, ulusal güvenlik anlayışının, bütüncül yönetim, dirençlilik odaklı planlama, insan güvenliğini önceleyen bir yaklaşım ve uluslararası iş birliği temelli stratejilerle yeniden tasarlanması gerekliliği vurgulanmaktadır. Bu dönüşüm, kavramsal bir değişimle beraber, kurumsal ve toplumsal zihniyet dönüşümünü de içermelidir.

Anahtar Kelimeler: *Harold Pinter, Doğum Günü Partisi, Louis Althusser, Çağırma, İdeolojik Devlet Aygıtları*

* Dr. Öğr. Üyesi, Polis Akademisi, İç Güvenlik Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, E-mail: clkabdullah@gmail.com, ORCID: 0000-0002-3912-3724, Ankara, Türkiye.

ABSTRACT

This article thoroughly analyzes the impact of the emerging new security threats of the 21st century, such as cybersecurity, the climate crisis, and pandemics, on national security policies. The traditional state-centric and military-based understanding of security is inadequate to grasp these threats, which are now impacting globally and shaped by multi-actor structures. In particular, the process of globalization, digitalization, the influence of non-state actors, and interdependence have necessitated a redefinition of the concept of security. In this context, the study reveals how new threats are constructed discursively and institutionally within the framework of the Copenhagen School's securitization theory. Cybersecurity threats also have significant impacts on digital infrastructures, individual privacy, freedom of expression, and the state's understanding of sovereignty. While the climate crisis is integrated into the security agenda through consequences such as water and food scarcity, migration, and social instability, pandemics have highlighted the vital importance of human security and societal resilience. The article's analysis, using the Turkish example, demonstrates that policies developed to address these threats remain largely reactive, sectoral, and fragmented. Consequently, it emphasizes the need to redesign the understanding of national security through holistic governance, resilience-focused planning, an approach prioritizing human security, and strategies based on international cooperation. This transformation must encompass not only a conceptual shift but also a transformation of institutional and societal mindsets.

Keywords: *National Security, Cybersecurity, Climate Crisis, Pandemic, Human Security*

Giriş

Güvenlik kavramı, uluslararası ilişkiler disiplininin teorik çerçevesinde ve devletlerin dış politika pratiklerinde merkezi bir konumda yer almaktadır. Soğuk Savaş'ın sona ermesiyle birlikte ise bu kavram hem teorik düzlemde hem de pratik uygulamalarda belirgin bir dönüşüm sürecine girmiştir. İki kutuplu sistemin askeri ve ideolojik kutuplaşması içerisinde şekillenen geleneksel güvenlik anlayışı, esasen devletin bekası ile toprak bütünlüğünün askerî tehditlere karşı korunmasını temel öncelik olarak benimsemişti (Walt, 1991; Kavıracı ve Demirbaş, 2020). Realist ve neorealist kuramsal yaklaşımlar çerçevesinde güvenlik; askerî kapasite, güç dengesi ve caydırıcılık gibi unsurlar üzerinden tanımlanmakta ve değerlendirilmektedir. Ancak 21. yüzyılın başından itibaren küreselleşme dinamiklerinin ivme kazanması, teknolojik ilerlemeler ve devlet dışı aktörlerin uluslararası alandaki etkinliğinin artması, bu dar ve devlet merkezli güvenlik yaklaşımının, çağdaş tehdit ortamının çok boyutlu yapısını kavramakta yetersiz kaldığını açık biçimde ortaya koymuştur (Buzan vd., 1998).

Çağdaş uluslararası güvenlik ortamı, geleneksel tehdit tanımlarının ötesine geçen, sınır aşan, çok aktörlü ve karmaşık dinamiklerle şekillenmektedir (Cavelty, 2007). Siber güvenlikten iklim krizine, pandemilerden küresel tedarik zincirlerindeki kırılmalara kadar uzanan yeni nesil tehditler, klasik güvenlik paradigmasının sınırları içinde

açıklanamayacak ölçüde çok boyutlu ve yayılımcı nitelikler taşımaktadır. Örneğin, kritik altyapılara yönelik siber saldırılar, bir devletin askerî kapasitesine, toplumsal işleyiş ve ekonomik bütünlüğe zarar verebilmekte; iklim değişikliği ise çevresel bir sorun olmaktan çıkarak siyasal ve sosyal sistemlerin istikrarını tehdit eden bir güvenlik meselesine dönüşmektedir (Homer-Dixon, 2010). Benzer şekilde, COVID-19 pandemisinde de görüldüğü üzere, küresel sağlık krizleri, ulusal sınırların ötesinde etkiler yaratarak toplumsal direnç kapasitesini ve yönetim mekanizmalarını ciddi biçimde sınamaktadır. Bu bağlamda, klasik caydırıcılık ve savunma stratejilerinin, kaynağı tanımlanması güç siber tehditler veya küresel nitelikli salgınlar karşısında büyük ölçüde yetersiz kaldığı açıkça görülmektedir. Bu tür krizlerin fiziksel, psikolojik ve toplumsal etkileri de dikkate değerdir. Özellikle bireylerde oluşan korku, sosyal ilişkilerin zayıflamasına, kamusal alanların terk edilmesine ve toplumsal dayanışmanın gerilemesine yol açabilmektedir. Bu durum, güvenliğe dair algının dönüşmesine de neden olmaktadır (bkz. Demirbaş, Çelik ve Akıncıoğlu, 2023).

Yeni nesil güvenlik tehditleri, karşılıklı etkileşim içinde olan ve birbirlerinin etkilerini pekiştiren bir “tehdit yakınsaması” dinamiği içinde ortaya çıkmaktadır (Kavsıracı, 2019). COVID-19 pandemisi, dijital altyapılara olan bağımlılığı dramatik biçimde artırarak hem bireysel kullanıcılar hem de kurumsal yapılar düzeyinde siber güvenlik açıklarının derinleşmesine ve potansiyel saldırı yüzeyinin genişlemesine neden olmuştur. Benzer şekilde, iklim değişikliğinin yol açtığı su ve gıda kıtlığı gibi kaynak temelli krizler, toplumsal huzursuzlukları derinleştirerek çatışma riskini artırmakta; bunun yanı sıra, kitlesel göç hareketleri ve yerinden edilme süreçleri aracılığıyla bulaşıcı hastalıkların yayılımı için elverişli zeminler yaratmaktadır (Demchak, 2015). Dahası, bir tehdit alanına yönelik geliştirilen pandemi sürecinde uygulanan karantina rejimleri ve uzaktan çalışma düzenlemeleri gibi politika müdahaleleri başka bir alanda, örneğin siber güvenlikte, öngörülmemiş kırılmalıklar yaratabilmektedir. Bu çok katmanlı ve karşılıklı etkileşimli tehdit ortamı, ulusal güvenlik politikalarının artık riskleri birbirinden izole olarak ele alamayacağını; aksine, bu tehditler arasındaki karmaşık bağlantıları ve kaskad etkileri dikkate alan bütüncül, sistemik ve entegre bir güvenlik yaklaşımını zorunlu kıldığını göstermektedir (Centeno, 2015).

Bu çalışma, siber güvenlik, iklim krizi ve pandemiler gibi yeni tehdit türlerinin, devletleri güvenlik gündemlerini genişletmeye ve güvenliğe ilişkin temel kavramsal çerçeveleri yeniden düşünmeye zorladığını ileri sürmektedir. Bu bağlamda, güvenliğin referans nesnesi devlet merkezli anlayıştan bireye ve topluma yönelmekte; tehdidin doğası ise askerî karakterini yitirerek çok boyutlu, yaygın ve karmaşık bir nitelik kazanmaktadır. Aynı şekilde, güvenliğe yönelik müdahale araçları da klasik askerî kapasitenin ötesine geçerek çok aktörlü, disiplinlerarası ve yönetim temelli stratejilere evrilmektedir. Bu dönüşüm süreci, özellikle Kopenhag Okulu’nun geliştirdiği güvenikleştirme kuramı çerçevesinde anlam kazanmaktadır. Güvenliğin toplumsal olarak inşa edilen ve söylemsel pratikler aracılığıyla şekillenen bir olgu olduğunu vurgulayan bu kuramsal yaklaşım, her bir yeni tehdit türünün farklı siyasal, toplumsal ve etik boyutlarda güvenikleştirilmesine olanak tanımakta; böylece güvenlik siyasetinin çok katmanlı doğasına dikkat çekmektedir.

Bu çalışmanın temel argümanını geliştirmek üzere, öncelikle güvenlik çalışmalarında yaşanan teorik dönüşüm ele alınacak ve özellikle Kopenhag Okulu'nun geliştirdiği güvenlikleştirme kuramı analitik bir çerçeve olarak sunulacaktır. Makale, Kopenhag Okulu'nun güvenlikleştirme kuramı çerçevesinde siber güvenlik, iklim krizi ve pandemi örnekleri üzerinden Türkiye'nin ulusal güvenlik politikalarını nasıl dönüştürdüğünü incelemektedir. Çalışma, güvenlikleştirme süreçlerinin aktörler ve söylemsel araçlarla nasıl meşrulaştırıldığını ve bu politikaların insan hakları ile toplumsal dayanıklılık üzerindeki etkilerini değerlendirmektedir. Hedef, güvenlikleştirme uygulamalarının normatif sınırlarını aşarak hak temelli politika önerileri sunmaktır.

Güvenlik Çalışmalarında Teorik Çerçeveler ve Güvenlikleştirme

Yeni güvenlik tehditlerinin ulusal güvenlik politikaları üzerindeki dönüştürücü etkisini sağlıklı biçimde analiz edebilmek, öncelikle güvenlik kavramının kuramsal temeller üzerinde nasıl evrildiğini ve tehditlerin toplumsal ve söylemsel düzeyde nasıl inşa edildiğini anlamayı gerektirir. Bu bölümde, güvenlik çalışmalarının tarihsel gelişimi çerçevesinde geleneksel realist yaklaşımlardan başlayarak, eleştirel güvenlik çalışmaları ve toplumsal inşacılığa dayanan perspektiflere kadar uzanan teorik evrim değerlendirilecektir. Bu kuramsal bağlam içerisinde, çalışmanın analitik temel kısmını oluşturan ve güvenliğin söylem aracılığıyla inşa edilen bir olgu olduğunu ileri süren Kopenhag Okulu'nun güvenlikleştirme (securitization) kuramı ele alınacaktır. Bu kuram, belirli bir konunun olağan siyasal tartışma alanının dışına çıkarılarak acil müdahale gerektiren bir güvenlik meselesi haline nasıl dönüştürüldüğünü açıklamak açısından çalışmanın temel teorik dayanağını oluşturmaktadır.

Güvenlik Çalışmaları disiplini, Soğuk Savaş dönemi boyunca büyük ölçüde realizm ve onun yapısalcı bir yorumu olan neorealizm'in entelektüel etkisi altında şekillenmiştir (Kavsıracı, 2020). Bu kuramsal yaklaşımlar, uluslararası sistemi anarşik bir yapı olarak kavramsallaştırmakta; devletleri ise bu anarşi ortamında varlıklarını sürdürebilmek amacıyla sürekli bir güç mücadelesi içinde olan rasyonel aktörler olarak tanımlamaktadır (Waltz, 1979). Bu çerçevede güvenlik, en temel anlamıyla, bir devletin dış askeri tehditlere karşı toprak bütünlüğünü ve siyasal bağımsızlığını koruma kapasitesi olarak ele alınmıştır. Söz konusu yaklaşımda güvenliğin referans nesnesi devlettir; tehdit ise büyük ölçüde diğer devletlerin sahip olduğu askeri güçten kaynaklanmaktadır. Bu dar ve devlet merkezli güvenlik anlayışı, güvenlik çalışmalarının temel gündemini nükleer caydırıcılık, stratejik denge, askerî ittifaklar ve güç dengesi gibi konular etrafında şekillendirmiştir (Walt, 1991). Bu bağlamda, Soğuk Savaş dönemi güvenlik düşüncesi, uluslararası ilişkiler disiplinde askeri tehditlere odaklanan, yapısal olarak statik ve referans nesnesi bakımından tek boyutlu bir paradigma ortaya koymuştur.

Soğuk Savaş'ın sona ermesi, güvenlik çalışmalarında uzun süre hâkim olan geleneksel ve devlet merkezli anlayışın ciddi biçimde sorgulanmasına yol açmıştır. İki kutuplu sistemin çöküşü, özellikle realist kuramların öngörülerini aşan bir gelişme olarak, uluslararası

sistemde köklü bir belirsizlik ortamı yaratmış; devletler arası büyük ölçekli savaşların yerini etnik çatışmalar, iç savaşlar, çevresel felaketler ve küresel ekonomik krizler gibi çok boyutlu istikrarsızlık kaynakları almıştır (Kaldor, 2013). Bu yeni uluslararası ortamda, akademik çevreler ve politika yapıcılar, güvenliğin askerî tehditlerle sınırlandırılmayacağını savunarak güvenlik kavramının hem kapsamının genişletilmesi hem de derinleştirilmesi gerektiğini ileri sürmüşlerdir. Kavramsal olarak “genişletme”, güvenliğin askerî, siyasal, ekonomik, toplumsal ve çevresel sektörlerdeki tehditleri kapsayacak biçimde ele alınmasını ifade ederken; “derinleştirme” ise güvenliğin referans nesnesini devletten bireylere, topluluklara ve nihayetinde tüm insanlığa doğru genişleten bir perspektifi içermektedir (Buzan vd., 1998). Bu iki yönlü kavramsal dönüşüm, güvenliğin içeriğini ve nesnesini dönüştürerek, disiplinin normatif ve analitik sınırlarını yeniden tanımlamıştır.

Eleştirel güvenlik literatürünün önemli dönüm noktalarından biri, Birleşmiş Milletler Kalkınma Programı’nın (UNDP) 1994 tarihli İnsani Kalkınma Raporu ile uluslararası gündeme taşınan “İnsani Güvenlik” (Human Security) kavramının ortaya çıkışıdır. Bu yaklaşım, güvenliğin referans nesnesini devletten bireye kaydırarak, güvenlik düşüncesinde köklü bir paradigmatik dönüşüm önermektedir. İnsani güvenlik anlayışı, askerî tehditlerin bertaraf edilmesiyle birlikte, bireylerin temel insani ihtiyaçlarının karşılanmasının da gerekli olduğunu, gerçek güvenliğin ise ancak bu biçimde sağlanabileceğini savunmaktadır. Bu doğrultuda, “korkudan özgürlük” ve “yoksunluktan özgürlük” ilkeleri, insani güvenliği normatif temelini oluşturmaktadır. UNDP, bu çerçevede insani güvenliği, ekonomik güvenlik, gıda güvenliği, sağlık güvenliği, çevre güvenliği, kişisel güvenlik, toplumsal güvenlik ve siyasal güvenlik olmak üzere yedi boyutta tanımlamıştır (UNDP, 1994). Bu yaklaşım, bir devletin sınırlarının ve askerî kapasitesinin korunmuş olması durumunda bile, yurttaşların yoksulluk, hastalık, açlık, çevresel felaketler veya siyasal baskılar altında yaşamasının ciddi bir güvensizlik hâli oluşturduğunu vurgulamaktadır. Dolayısıyla insani güvenlik, ulusal güvenlik politikalarının nihai hedefinin bireylerin refahı, onuru ve yaşam kalitesi olması gerektiğini ileri sürmektedir (Newman, 2001).

Kopenhag Okulu ve Güvenikleştirme Teorisi

Güvenlik gündeminin genişletilmesine ilişkin tartışmalar devam ederken, Barry Buzan, Ole Wæver ve Jaap de Wilde öncülüğünde şekillenen Kopenhag Okulu, güvenliğin mahiyetine ve inşa sürecine ilişkin post-yapısalcı ve toplumsal inşacı bir yaklaşım geliştirmiştir. Bu okulun temel argümanına göre güvenlik, nesnel gerçeklikte var olan bir tehdiye verilen doğrudan bir tepki değil; aksine, belirli aktörler tarafından bir konunun “varoluşsal bir tehdit” olarak temsil edilmesi ve bu temsilin hedef kitle tarafından meşru kabul edilmesi yoluyla inşa edilen söylemsel bir pratiktir. Bu sürece “güvenikleştirme” (securitization) adı verilmektedir (Buzan vd., 1998). Kopenhag Okulu’nun bu yaklaşımı,

güvenliği nesnel ve teknik bir mesele olmaktan çıkararak, siyasi ve söylemsel bir eylem biçimi olarak ele almaktadır. Bu çerçevede, bir meselenin güvenlik alanına dâhil edilmesi, onu olağan siyasal süreçlerin dışına taşıyarak, olağanüstü önlemlerle müdahale edilmesini mümkün ve meşru hale getirir. Bu yönüyle güvenlikleştirme hem bir durumu tanımlama biçimi hem de güçlü siyasi sonuçlar doğuran bir söz edimi olarak ifade edilebilir. Güvenlikleştirme süreci ise bir meselenin olağan siyasal tartışma alanından çıkarılarak “hayatta kalma” (survival) mantığı çerçevesinde ele alınmasını ve bu doğrultuda istisnai önlemlerin meşrulaştırılmasını sağlayan söylemsel bir pratiktir. Kopenhag Okulu’na göre bu süreç, üç temel unsurdan oluşur (Buzan vd., 1998). Bunlar;

- *Güvenlikleştirilen Aktör*: Genellikle hükümetler, siyasi liderler, üst düzey bürokratlar ya da güvenlik kurumları gibi siyasi otoriteye ve kamusal meşruiyete sahip aktörlerdir. Bu aktörler, belirli bir konuyu varoluşsal bir tehdit olarak çerçevlendirerek güvenlikleştirme girişiminde bulunurlar. Bu söylemsel hamle, bir konunun olağan siyasal zeminde çözülemeyecek kadar acil ve tehlikeli olduğunu iddia eder.
- *Referans Nesnesi*: Tehdit altında olduğu iddia edilen ve bu nedenle korunması gerektiği savunulan varlıktır. Geleneksel güvenlik anlayışında bu genellikle devletin toprak bütünlüğü veya siyasi egemenliği, çağdaş güvenlik söylemlerinde referans nesnesi olarak çevre, ekonomik düzen, insan hakları, toplumsal gruplar ya da kimlikler de öne çıkabilmektedir.
- *İzleyici/Kitle*: Güvenlikleştirme girişiminin başarılı olabilmesi, hem tehdidin tanımlanması hem de bu tehdidin varoluşsal olduğu yönündeki söylemin izleyici tarafından kabul edilmesiyle mümkündür. Bu izleyici; kamuoyu, medya, yasama organları veya uluslararası toplum gibi karar alma süreçlerine etkide bulunabilecek aktörler olabilir. Kitle tarafından verilen onay, güvenlikleştirme sürecine toplumsal ve siyasal meşruiyet kazandırır.

Kopenhag Okulu, bir meselenin güvenlik alanına nasıl dâhil edildiğini anlamak amacıyla konuları “politize olmamış, politize olmuş ve güvenlikleştirilmiş” olmak üzere üç temel kategoriye ayırmaktadır (Buzan vd., 1998).

Politize olmamış bir mesele, ne devletin doğrudan müdahalesine konu olur ne de kamuoyu gündeminde yer alır; dolayısıyla siyasal karar alma süreçlerinin dışında kalır. Politize olmuş konular ise kamu politikasının parçası haline gelmiştir; hükümetin karar alma süreçlerine, kaynak tahsisine ve düzenleyici müdahalelerine konu olur ve demokratik tartışmalar çerçevesinde ele alınır. Buna karşılık, güvenlikleştirilmiş bir mesele, ilgili aktörler tarafından “varoluşsal bir tehdit” olarak çerçevlendirilerek olağan siyasal süreçlerin dışına çıkarılır. Bu durumda, güvenlikleştirilen aktör, tehditle mücadele gerekçesiyle olağanüstü önlemler talep eder ve bu talepler çoğu zaman demokratik denetim mekanizmalarının dışında işlemeye başlar. Güvenlikleştirme bu yönüyle, siyasal bir

meselenin güvenlik söylemi aracılığıyla istisna rejimi içerisine alınması anlamına gelir ve bu durumun ciddi siyasal, hukuksal ve etik sonuçları olabilir.

Söz konusu çerçeve, güvenlik alanında normatif, kuramsal ve analitik tartışmaları dönüştüren öncü bir yaklaşım haline gelmiştir. Güvenikleştirme teorisi, güvenlik olgusunun sosyal olarak inşa edilen yönünü ortaya koyarak literatüre öneli bir kuramsal katkı sunmuştur. Ancak bu teori, beraberinde çeşitli eleştirileri de gündeme getirmiştir. Eleştirilenler, Kopenhag Okulu'nun teorik çerçevesinin "söz edimi" kavramına fazlasıyla odaklanarak, tehditlerin maddi/nesnel boyutlarını yeterince dikkate almadığını savunmaktadır. Bu eleştiriye göre, bazı durumlarda belirli bir tehdidin gerçekten var olup olmadığı ya da ne ölçüde tehlike arz ettiği, somut materyal koşullarla da ilişkilidir. Buna ek olarak, teorinin normatif çerçevesinin daha çok demokratik rejimlerdeki siyasal süreçlere uygun şekilde tasarlandığı ileri sürülmektedir. Otoriter veya totaliter rejimlerde ise normal siyaset ile istisnai siyaset arasındaki sınırların bulanık olduğu ve bu bağlamda güvenikleştirmenin analitik olarak nasıl işleyeceğinin net biçimde açıklanmadığı belirtilmiştir (Vuori, 2008).

Ayrıca, teoride kitlenin rolü büyük ölçüde pasif bir kabul ya da ret ikiliğine indirgenmekte; böylece izleyici aktörlerin güvenlik söyleminin oluşumundaki aktif katkısı ve direniş potansiyeli göz ardı edilmektedir. Son olarak, güvenikleştirmenin çoğunlukla olumsuz, demokratik süreçleri tahrip eden ve bu nedenle kaçınılması gereken bir pratik olarak sunulması da kuramsal bir indirgeme eleştirisiyle karşı karşıyadır. Oysa bazı durumlarda güvenikleştirme, örneğin iklim krizi ya da pandemiler gibi ciddi tehditlerin kamu gündemine taşınmasında işlevsel bir araç da olabilir.

Kopenhag Okulu'nun güvenikleştirme teorisine yöneltilen eleştiriler karşısında geliştirilen en dikkat çekici yanıtlarından biri, Rita Floyd'un ortaya koyduğu Adil Güvenikleştirme Teorisi'dir (Just Securitization Theory). Bu yaklaşım, klasik savaş etiği literatüründe köklü bir yere sahip olan "Adil Savaş Teorisi" ilham alınarak, güvenikleştirmenin nasıl işlediğini ve ne zaman ahlaki olarak meşru kabul edilebileceğini sorgulayan normatif bir çerçeve sunar (Floyd, 2010). Floyd'un teorisi, güvenikleştirme süreçlerini etik bir değerlendirmeye tabi tutmak üzere üç aşamalı bir kriter seti öne sürmektedir. Bunlar, adil başlangıç, adil yürütme ve adil sonlandırma olarak ifade edilmektedir (Floyd, 2019).

Adil Başlangıç aşamasında, güvenikleştirilen tehdidin nesnel olarak varoluşsal nitelikte olması gerekir. Bunun yanı sıra, güvenliğin referans nesnesi insan toplulukları veya temel haklar gibi meşru bir varlık olmalıdır. Güvenikleştirme hamlesinin samimi niyetlerle gerçekleştirilmiş olması ve müdahalenin potansiyel faydalarının, doğuracağı zararlardan açık biçimde daha fazla olması beklenir. Adil Yürütme aşamasında ise, alınan güvenlik önlemlerinin orantılı olması, tehdit karşısında etkililik göstermesi ve sürecin temel insan haklarına saygılı bir biçimde yürütülmesi esastır (Floyd, 2019). Adil Sonlandırma (just termination), bir güvenikleştirme sürecinin etik olarak meşru kabul edilebilmesi için sürecin nasıl başlatıldığı, nasıl yürütüldüğü, ne zaman ve nasıl sona erdirildiği sorusunu da

dikkate almayı gerektirir. Floyd'a göre, bir güvenlik politikası ne kadar haklı gerekçelerle başlamış ve ne kadar orantılı önlemlerle yürütülmüş olursa olsun, süresiz olarak devam ettirilmesi durumunda etik meşruiyetini yitirebilir (Floyd, 2019). Bu nedenle, güvenlikleştirmenin belirli koşullar altında ve zamanında sonlandırılması, adil bir güvenlik siyasetinin vazgeçilmez bir unsurudur. Bu kuramsal yaklaşım, güvenlikleştirmenin her durumda olumsuz ve kaçınılması gereken bir süreç olmadığına işaret ederken, onu etik bir değerlendirme süzgecinden geçirerek, bazı durumlarda meşru ve hatta gerekli bir müdahale biçimi olarak yeniden düşünmeye imkân tanımaktadır.

Rita Floyd'un adil güvenlikleştirme teorisinin ampirik geçerliliğini test etmeye yönelik çalışmalarından biri, Yunanistan'ın COVID-19 pandemisine verdiği tepkiyi inceleyen Dimari ve Papadakis'in (2023) analizidir. Bu çalışma, pandeminin nesnel olarak varoluşsal bir tehdit oluşturduğu, güvenliğin referans nesnesi olarak tanımlanan Yunan halkının meşru bir varlık olduğu ve hükümetin uyguladığı karantina gibi önlemlerin orantılı ve etkili olduğu tespitlerine dayanarak, sürecin etik açıdan meşru bir güvenlikleştirme örneği teşkil ettiğini ileri sürmektedir.

Yazarlar, güvenlikleştirmenin üç aşamasını da değerlendirmeye tabi tutarak, ilk olarak tehdidin epidemiyolojik verilerle desteklenen nesnelliğine, ikinci olarak uygulanan politikaların halk sağlığı üzerindeki somut etkilerine, son olarak ise hükümetin olağanüstü yetkilere başvurmasına rağmen zaman içinde bu yetkileri sınırlı ve geçici olarak kullanmasına dikkat çekmektedir. Bu bağlamda çalışma, Yunanistan'ın COVID-19 krizine verdiği yanıtın Adil Güvenlikleştirme Teorisi kapsamında başarılı ve normatif açıdan meşru bir örnek sunduğu sonucuna ulaşmaktadır.

Güvenlikleştirme, bir yönüyle güvenlik tehdidine verilen söylemsel bir yanıt oluştururken diğer taraftan siyasi aktörler tarafından olağanüstü yetkiler elde etmek, kamusal kaynakları yeniden yönlendirmek ve muhalefeti baskı altına almak amacıyla araçsallaştırılabilecek güçlü bir siyasal mekanizma olarak da işlev görebilmektedir. Bir meselenin ulusal güvenlik sorunu olarak çerçeveselendirilmesi, genellikle demokratik denetim süreçlerinin askıya alınmasına ve yürütmenin geniş, denetlenmemiş yetkilerle hareket etmesine zemin hazırlayabilmektedir. Bu durum, özellikle sivil özgürlükler açısından riskler barındırmaktadır. Örneğin, "siber terörizm" söylemi, kapsamlı internet gözetimi, veri toplama ve ifade özgürlüğünü sınırlandıran yasal düzenlemeleri meşrulaştırmak amacıyla kullanılabilirken; "biyogüvenlik" çerçevesinde yapılan güvenlikleştirme hamleleri, toplanma özgürlüğü ve seyahat hakkı gibi temel hakları süresiz biçimde askıya alan olağanüstü kararları mümkün kılabilir (Hansen ve Nissenbaum, 2009).

Bu bağlamda, bir tehdidin nesnel olarak gerçek olup olmadığı ve güvenlikleştirme sürecine öncülük eden aktörlerin niyetleri, uygulanan önlemlerin orantılılığı ve alınan kararların temel hak ve özgürlükler üzerindeki etkisi de eleştirel bir değerlendirmeye tabi tutulmalıdır. İşte bu noktada, Rita Floyd'un ortaya koyduğu Adil Güvenlikleştirme Teorisi,

güvenlikleştirmenin gerekli olup olmadığını ve aynı zamanda güvenlikleştirmenin olabilmesi için gerekli hâllerin de etik bir çerçevede analiz edilmesini mümkün kılar. Bu yaklaşım, güvenlik siyasetinin normatif boyutunu görünür kılarak, güvenlikleştirmenin hem demokratik denge hem de insan hakları açısından ne tür sonuçlar doğurduğunu sorgulamayı zorunlu kılar.

Dijital Çağın Ulusal Güvenlik Paradoksu: Siber Güvenlik

Dijital çağ, ekonomik ve toplumsal yapıların yanı sıra ulusal güvenlik anlayışlarını da köklü biçimde dönüştürmüştür. Bu dönüşüm sürecinde ortaya çıkan siber uzay, modern devletler için giderek daha merkezi bir güvenlik alanı hâline gelmiştir. Ekonomik işlemlerden siyasi iletişime, askerî komuta kontrol sistemlerinden bireylerin gündelik yaşam pratiklerine kadar hemen her alanın dijital altyapılara bağımlılığı arttıkça, devletler ve toplumlar, geleneksel tehdit tanımlarının ötesine geçen yeni ve karmaşık risk biçimlerine karşı daha kırılgan hâle gelmiştir. Bu bağlamda siber tehditler; fiziksel sınırları aşan, kaynağı belirsiz ve hem kamu hem özel sektör altyapılarını hedef alabilen çok boyutlu bir güvenlik sorunu olarak değerlendirilmekte; bu nedenle de hızla güvenlikleştirme pratiklerinin konusu hâline gelmektedir.

Siber tehditler hem yapısal olarak hem de failerin motivasyonları açısından son derece geniş ve dinamik bir yelpazeye sahiptir. Bu tehditlerin özgünlüğü, teknolojik araçlara dayanması ve devlet-dışı aktörlerin de etkin biçimde bu alanda faaliyet gösterebilmesinden kaynaklanmaktadır. Singer ve Friedman'a (2014) göre, siber uzaydaki tehdit üreticileri dört temel kategori altında sınıflandırılabilir. Bunlar;

- *Devletler ve Devlet Destekli Aktörler:* Bu gruba dâhil olan aktörler, genellikle ulusal çıkarları gözeterek stratejik hedeflerle hareket ederler. Siber casusluk yoluyla hassas siyasi, askerî veya ekonomik bilgilerin elde edilmesi; kritik altyapılara yönelik sabotaj girişimleri, kamuoyunu yönlendirmeye yönelik dezenformasyon kampanyaları gibi faaliyetler bu kategorinin temel eylem planını oluştururlar.
- *Siber Suç Örgütleri:* Finansal kazanç amacı güden bu aktörler, fidye yazılımları, oltalama saldırıları ve kişisel ya da kurumsal veri hırsızlığı gibi yöntemlerle dijital ekonomik sistemler üzerinde ciddi tehditler oluştururlar.
- *Terörist Yapılar:* Terör örgütleri, dijital mecraları propaganda yaymak, yeni üyeler kazanmak, finansal kaynak yaratmak ya da fiziksel saldırılarla senkronize biçimde dijital altyapıları hedef almak için kullanılmaktadır. Siber uzay, bu yapılar için hem bir operasyonel alan hem de ideolojik bir mobilizasyon aracı işlevi görmektedir.
- *Hackivist Gruplar:* Politik ya da toplumsal motivasyonla hareket eden bu gruplar, belirli ideolojik hedefleri desteklemek adına siber saldırılar gerçekleştirmektedir. Web sitelerinin tahrif edilmesi, hizmet dışı bırakma (DDoS) saldırıları gibi yöntemler, dijital protesto biçimleri olarak öne çıkar.

Bu çok aktörlü yapı, siber güvenlik alanında tehdidin teknik, politik, etik ve yönetsimsel bir sorun hâline geldiğini göstermektedir. Farklı aktörlerin karmaşık motivasyonları, devletlerin siber tehditleri nasıl tanımladığı ve bu tehditleri nasıl güvenlikleştirdiği sorusunu daha da kritik hale getirmektedir.

Siber saldırıların ulusal güvenlik açısından en kaygı verici yönlerinden biri, kritik altyapılara yönelik gerçekleştirilen müdahalelerin hem dijital sistemlerde hem de fiziksel dünyada da yıkıcı etkiler doğurabilmesidir. Enerji santralleri, su arıtma tesisleri, ulaşım sistemleri, finansal piyasalar ve sağlık hizmetleri gibi toplumun sürekliliği açısından hayati öneme sahip olan bu altyapılar, siber saldırılar sonucunda kitlesel panik, ekonomik istikrarsızlık ve hatta can kayıplarına yol açabilecek ölçüde zarar görebilir. Bu durum, siber güvenlik ile fiziksel güvenlik arasındaki geleneksel ayrımın giderek geçersizleştiğini göstermektedir.

Siber tehditlerin sahip olduğu yıkıcı potansiyel, devletler tarafından hızla bir “varoluşsal tehdit” olarak tanımlanmasına yol açmış; bu doğrultuda siber güvenlik, ulusal güvenlik stratejilerinin merkezî unsurlarından biri hâline gelmiştir. Bu güvenlikleştirme süreci, söylemsel, kurumsal ve toplumsal düzeylerde çok katmanlı biçimlerde gerçekleşmektedir. Lene Hansen ve Helen Nissenbaum (2009), bu süreci üç temel biçimde kavramsallaştırarak, siber güvenliğin nasıl toplumsal anlam kazandığını analiz etmişlerdir:

- *Hiper-güvenlikleştirme*: Bu yaklaşımda siber tehditler, dramatize edilmiş felaket senaryoları üzerinden çerçevelenir. “Dijital Pearl Harbor” veya “Siber 9/11” gibi kavramlar aracılığıyla, siber saldırıların ani ve topyekûn toplumsal çöküşe yol açabileceği ima edilir. Genellikle askerî ve istihbarat kurumları tarafından üretilen bu söylem, geniş kapsamlı olağanüstü yetkilerin, yasal düzenlemelerin ve bütçelerin meşrulaştırılması amacıyla kullanılır.
- *Gündelik Güvenlik Pratikleri*: Bu çerçevede siber güvenlik, devlet kurumları, özel kurum ve kuruluşlar ile bireylerin gündelik yaşamlarının ortak konusudur. Özellikle virüsler, kimlik hırsızlığı, dolandırıcılık gibi yaygın tehdit türlerine karşı bireylerin bilinçli hareket etmesi gerektiği vurgulanır. Siber hijyen kampanyaları ve güvenli internet kullanımı gibi uygulamalarla güvenlik sorumluluğu devletten bireye doğru kaydırılır; böylece güvenlik söylemi gündelik pratikler aracılığıyla toplumsallaştırılır.
- *Teknifikasyon*: Bu süreçte siber güvenlik, yüksek düzeyde teknik bilgi gerektiren, uzmanların anlayabileceği karmaşık bir mesele olarak sunulur. Böylelikle konu, siyasi ve toplumsal tartışmanın dışına taşınır ve teknokratik elitlerin yönettiği dar uzman çevrelerinin tekelinde çözülmesi gereken bir alan hâline gelir.

Hansen ve Nissenbaum’un bu üçlü kavramsal ayrımı hem siber tehditlerin nasıl sunulduğunu hem de güvenlikleştirmenin toplumsal inşa süreçlerinde nasıl işlediğini de gözler önüne sermektedir. Bu çerçeve, Türkiye gibi gelişmekte olan dijital altyapılara sahip

ülkelerde güvenlik söyleminin hangi biçimlerde kurumsallaştığını analiz etmek için de önemli bir analitik araç sunmaktadır.

Siber güvenliğin ulusal güvenlik stratejilerinde merkezi bir konuma yerleşmesi, devletlerin siber uzay üzerinde egemenlik kurma çabalarını da beraberinde getirmiştir. Bu bağlamda birçok devlet, dijital ortam üzerindeki kontrolünü artırmak amacıyla “dijital egemenlik” arayışına yönelmiştir. Dijital egemenlik, bir devletin kendi sınırları içerisindeki dijital altyapı, veri trafiği ve bilgi akışı üzerinde bağımsız ve mutlak denetim kurma kapasitesine sahip olma iddiasını ifade eder. Bu çerçevede, veri yerelleştirme (data localization) politikaları, yabancı teknoloji şirketlerine yönelik regülasyonlar, ulusal internet altyapılarının küresel ağdan izole edilebilmesine imkân tanıyan teknik uygulamalar ve içerik denetimi gibi araçlar ön plana çıkmaktadır. Ancak bu gelişmeler, dijital güvenlikle bireysel özgürlükler arasında giderek derinleşen bir ikilemi de gündeme getirmektedir. Ulusal güvenliğin sağlanması gerekçesiyle artırılan gözetim, denetim ve sansür mekanizmaları; bireylerin mahremiyet hakkı, ifade özgürlüğü ve diğer temel hak ve özgürlükler açısından ciddi riskler doğurmaktadır (DeNardis, 2014).

Devletlerin “ulusal güvenliği koruma” söylemi altında yürüttüğü kitlesel veri toplama, algoritmik izleme, içerik filtreleme gibi uygulamalar, siber güvenliğin dış kaynaklı siber tehditlerle sınırlı bir mesele olmadığını; iç güvenlik, rejim istikrarı ve hatta otoriterleşme eğilimleri ile doğrudan ilişkili hâle gelebildiğini de göstermektedir. Bu bağlamda, siber güvenliğe ilişkin politikaların değerlendirilmesi teknik yeterlilik ve caydırıcılık düzeyiyle sınırlı kalmamalı, bu politikaların demokratik normlara, hukuk devleti ilkelerine ve adil güvenlikleştirme ölçütlerine ne ölçüde uyduğuna da dikkat edilmelidir.

Benzer şekilde, ulusal güvenlik gündemini dönüştüren bir diğer kritik alan da çevresel boyut olup, özellikle iklim değişikliği günümüzde geleneksel güvenlik anlayışlarını zorlayan başat tehditlerden biri olarak öne çıkmaktadır. İklim değişikliği, geleneksel güvenlik analizlerinin uzun süre göz ardı ettiği bir mesele olmakla birlikte günümüzde giderek daha fazla sayıda devlet ve uluslararası kuruluş tarafından uzun vadeli, yapısal ve çok boyutlu bir güvenlik tehdidi olarak tanımlanmaktadır. Bu durum, çevresel sorunların kalkınma, sürdürülebilirlik, uluslararası barış ve istikrar açısından kritik bir öneme sahip olduğu anlayışına dayanmaktadır. İklim krizi, doğrudan bir savaş nedeni olmaktan ziyade; su kıtlığı, gıda güvensizliği, kitlesel göç, sağlık krizleri ve ekonomik çöküş gibi mevcut kırılganlıkları derinleştirerek çatışma risklerini artıran bir “tehdit çarpanı” olarak kavramsallaştırılmaktadır (Overhaus, 2014). Bu nedenle, iklim değişikliği ile güvenlik arasındaki yapısal ilişki farklı düzlemlerde ele alınmayı gerektirmektedir.

İklim değişikliğinin güvenlik üzerindeki etkileri çok boyutlu bir tehdit yapısı ortaya koymaktadır. Artan sıcaklıklar, düzensiz yağış rejimleri ve şiddetlenen kuraklıklar, özellikle tarıma dayalı ekonomilerde su ve gıda güvenliğini tehdit ederek geçim kaynaklarını ortadan kaldırmakta, topluluklar arasında gerilimi artırmakta ve devlet otoritesini zayıflatmaktadır. Bu bağlamda, Suriye İç Savaşı öncesinde yaşanan uzun süreli

kuraklık, kırsal bölgelerden kentlere göçleri tetiklemiş, sosyo-ekonomik baskıları ağırlaştırmış ve toplumsal huzursuzluğu körüklemiştir (Gleick, 2014). Benzer şekilde deniz seviyesinin yükselmesi, özellikle alçak kıyı bölgelerinde yaşayan milyonlarca insan için varoluşsal bir tehdit oluşturmaktadır. Bangladeş ve Pasifik adaları gibi bölgelerde kara parçalarının sular altında kalma riski, kalıcı yerinden edilmeleri gündeme getirmekte; kasırgalar, seller ve çölleşme gibi aşırı hava olayları milyonlarca insanı iklim mülteci haline getirmektedir. Bu tür nüfus hareketleri, ev sahibi topluluklarla göçmenler arasında sosyopolitik gerilimler yaratarak güvenlik açısından ciddi istikrarsızlıklara yol açmaktadır (Boas vd., 2019).

İklim krizinin etkileri toplumsal ve demografik düzeylerde olduğu gibi altyapısal ve askerî güvenliği de doğrudan etkilemektedir. Askerî üsler, limanlar, enerji tesisleri ve iletişim altyapıları çoğunlukla kıyı bölgelerinde konumlandıkları için deniz seviyesinin yükselmesi ve fırtına kabarmaları karşısında kırılgan hale gelmektedir. Bu durum ülkelerin savunma kapasitelerinde fiziksel zafiyetler yaratırken, aşırı iklim koşulları ve sıcak hava dalgaları askerî personelin sağlığını olumsuz etkilemekte, tatbikatları sekteye uğratmakta ve teçhizatın etkinliğini azaltabilmektedir (Such, 2022). Ayrıca Arktik bölgesinde buzulların erimesi, Kuzeydoğu ve Kuzeybatı geçitlerinin açılmasına yol açmakta; enerji ve mineral kaynaklarının erişilebilirliğinin artması, ABD, Rusya ve Çin arasında stratejik bir rekabeti tetiklemektedir (Osthagen, 2020). Dolayısıyla iklim değişikliği, çevresel bir sorun olmanın ötesinde jeopolitik ve altyapısal güvenlik boyutlarıyla da ele alınmalıdır.

Bununla birlikte iklim değişikliğinin güvenlikleştirilmesi süreci, literatürde sıklıkla “iki ucu keskin kılıç” olarak tanımlanmaktadır. Bir yandan güvenlikleştirme, iklim krizine ilişkin siyasal aciliyet duygusunu artırmakta, politika yapıcılarını harekete geçmeye zorlamakta, kaynak tahsisini hızlandırmakta ve uluslararası iş birliğini teşvik etmektedir. Ulusal güvenlik tehdidi olarak tanımlanması, çevre sorunlarını geleneksel çevre politikalarının yavaş işleyen süreçlerinden çıkararak yüksek siyasetin alanına taşımaktadır. Trombetta'nın (2008) da vurguladığı üzere, iklim değişikliğini bütüncül bir güvenlik tehdidi olarak yeniden çerçevelemek, hem siyasi elitlerin dikkatini çekmek hem de toplumun farklı kesimlerinde daha geniş farkındalık yaratmak açısından stratejik bir işlev görmektedir.

Öte yandan, iklim krizinin güvenlikleştirilmesi süreci önemli normatif ve pratik sakıncalar da barındırmaktadır. Güvenlikleştirme söylemi kimi zaman demokratik süreçleri zayıflatabilir, otoriter eğilimleri güçlendirebilir ve kırılgan toplulukların marjinalleşmesine zemin hazırlayabilir. Bu nedenle, iklim güvenliği söyleminin ne zaman, nasıl ve kimin tarafından üretildiği, hangi amaçlara hizmet ettiği ve hangi kesimler üzerinde ne tür sonuçlar doğurduğu dikkatle sorgulanmalıdır. Eleştirel güvenlik literatürünün işaret ettiği üzere, güvenlikleştirme hem uygulama düzeyinde hem de ahlaki ve siyasal sonuçları bakımından da titizlikle değerlendirilmesi gereken bir süreçtir (Buzan vd., 1998).

Sonuç itibarıyla iklim krizi, çevresel, toplumsal, ekonomik, jeopolitik ve altyapısal boyutlarıyla çok katmanlı bir güvenlik tehdidi olarak ulusal ve uluslararası gündemin merkezinde yer almaktadır. Bu bağlamda iklim değişikliğinin güvenlik politikalarıyla bütünleşik biçimde ele alınması çevresel sürdürülebilirlik, siyasal istikrar, toplumsal barış ve uluslararası güvenlik açısından zorunluluk arz etmektedir.

Pandemi Deneyimi: Biyogüvenlik ve İnsan Güvenliğinin Sınava

2019 yılı sonunda ortaya çıkan ve kısa sürede küresel ölçekte etkisini gösteren COVID-19 pandemisi, 21. yüzyılın en kapsamlı ve çok boyutlu krizlerinden biri olarak tarihe geçmiştir. İlk bakışta bir halk sağlığı krizi olarak ortaya çıkmakla birlikte, pandemi kısa sürede sağlık sistemleri başta olmak üzere küresel ekonomi, toplumsal yapılar ve siyasal düzenler üzerinde derin sarsıntılara yol açmıştır. Bu süreç, özellikle küreselleşmiş dünyanın kırılma noktalarını ve devletlerin en temel yükümlülüklerinden biri olan vatandaşlarının yaşam ve güvenliğini koruma kapasitelerinin sınırlarını açık biçimde gözler önüne sermiştir (Greer vd., 2020).

Pandeminin yol açtığı bu sarsıcı deneyim, ulusal güvenlik anlayışının sadece askerî ve dış kaynaklı tehditlere dayandırılmasının yetersizliğini ortaya koyarak, biyogüvenlik ve insani güvenlik gibi daha kapsamlı ve birey merkezli güvenlik yaklaşımlarını ön plana çıkarmıştır. Aynı zamanda, salgının yönetiminde yaşanan zorluklar, devletlerin kriz yönetimi kapasiteleri, kurumsal koordinasyon düzeyleri ve toplumsal dayanıklılık stratejileri açısından yeniden değerlendirilmesini zorunlu kılmıştır. Bu bağlamda pandemi, her ne kadar bir sağlık krizi olsa ortaya çıkardığı zincirleme risk ve tehditler göz önünde bulundurulduğunda ulusal güvenlik paradigmasının yeniden düşünülmesini gerekli kılan yapısal bir dönüm noktası işlevi görmüştür.

COVID-19 pandemisi, modern toplumların karşılıklı bağımlılık temelinde yapılandığını ve bu karmaşık sistemlerin tek bir küresel şok karşısında nasıl hızla işlevsizleşebileceğini dramatik biçimde ortaya koymuştur. Bu süreç, ulusal güvenliğin tek başına dışsal tehditlere karşı askerî kapasiteyle sağlanamayacağını, aksine iç sistemik dayanıklılığın stratejik bir güvenlik unsuru haline geldiğini göstermiştir. Pandeminin yarattığı başlıca güvenlik zafiyetleri şu şekilde özetlenebilir:

- *Tedarik Zincirlerinin Kırılabilirliği:* Salgının ilk evrelerinde başta maske, ventilatör, test kitleri gibi tıbbi malzemeler ve bazı temel gıda ürünleri olmak üzere çeşitli kalemlerde yaşanan tedarik sıkıntıları, küresel ölçekte uygulanan “tam zamanında üretim” modelinin ne denli kırılabilir olduğunu ortaya koymuştur. Bu durum, stratejik ürünlerde ulusal üretim kapasitesini güçlendirme, stok politikalarını yeniden yapılandırma ve tedarik güvenliği kavramını ulusal güvenlik stratejilerine entegre etme yönünde ciddi bir paradigma kaymasına yol açmıştır (Gereffi, 2020).

- *Sağlık Altyapısının Yetersizliği:* Pandemi, en gelişmiş sağlık sistemlerine sahip devletlerde dahi yoğun bakım kapasitesinin yetersizliği, personel açığı ve tıbbi ekipman eksikliği gibi sorunları görünür kılmıştır. Bu durum, kamu sağlığının salt sosyal politika değil, aynı zamanda ulusal güvenliğin kritik bir bileşeni olarak değerlendirilmesi gerektiğini ortaya koymuştur (Burwell, 2021).
- *Dezenformasyon ve Sosyal Kutuplaşma:* Belirsizlik dönemlerinde bilgi eksikliği ve korku, yanlış bilgilendirme ve kasıtlı dezenformasyonun hızla yayılmasına uygun bir zemin yaratmaktadır. COVID-19 bağlamında, virüsün kaynağı, yayılım biçimleri ve tedavi yöntemleri hakkında dolaşıma sokulan komplo teorileri ve yanlış bilgiler, halk sağlığı önlemlerine olan güveni sarsmış, aşılama kampanyalarını zayıflatmış ve toplumda siyasi kutuplaşmayı derinleştirmiştir (Cinelli vd., 2020).
- *Ekonomik ve Sosyal İstikrarsızlık:* Pandemiyle mücadele kapsamında uygulanan karantina önlemleri ve hareket kısıtlamaları, küresel ekonomide İkinci Dünya Savaşı'ndan bu yana en ciddi daralmalardan birine yol açmıştır. İşsizlik oranlarındaki artış, yoksulluğun derinleşmesi ve gelir dağılımındaki eşitsizliklerin belirginleşmesi, toplumsal istikrar ve siyasi meşruiyet açısından da ciddi tehditler doğurmuştur (Ahmed vd., 2020).

Bu kapsamlı güvenlik zafiyetleri, pandeminin salt bir sağlık krizi değil, bir bütün olarak sistemsel güvenliğe yönelik çok boyutlu bir tehdit olduğunu ve ulusal güvenlik anlayışının yapısal olarak yeniden tanımlanmasını zorunlu kıldığını ortaya koymaktadır. COVID-19 pandemisinin ortaya çıkardığı çok boyutlu kırılmalıklar, ulusal güvenlik anlayışında insan güvenliği perspektifinin gerekliliğini bir kez daha güçlü biçimde gündeme getirmiştir. Salgın süreci, bir devletin askerî kapasitesi ne denli büyük olursa olsun, eğer vatandaşlarının sağlığını, refahını ve temel yaşam koşullarını koruyamıyorsa, gerçek anlamda güvenli bir yapıdan söz edilemeyeceğini açıkça ortaya koymuştur. Bu durum, güvenliğin dış tehditlere ve sınır savunmasına indirgenemeyeceğini, aksine birey temelli bir anlayışın ulusal güvenliğin önkoşulu olduğunu göstermiştir.

Pandemi, bireysel güvenlik ile toplumsal ve devlet güvenliği arasındaki karşılıklı bağımlılık ilişkisini somutlaştırarak, insan güvenliği yaklaşımının teorik bir iddiadan ibaret olmadığını, aksine pratik ve hayati bir zorunluluk olduğunu kanıtlamıştır. Bireyin sağlığı ve yaşam koşullarının tehdit altında olduğu bir ortamda, toplumsal istikrarın ve siyasi meşruiyetin sürdürülebilirliği de büyük ölçüde riske girmektedir. Bu bağlamda, COVID-19 pandemisi bir sağlık krizi olmanın ötesinde ulusal güvenliğin birey merkezli yeniden tanımlanması açısından da tarihsel bir kırılma noktası olarak değerlendirilmelidir.

COVID-19 pandemisi, dünya genelinde en hızlı ve en kapsamlı güvenikleştirme süreçlerinden birine sahne olmuştur. Pandemiyle mücadelede siyasi liderler, virüsü sıklıkla görünmez bir düşman olarak nitelendirmiş ve salgını bir savaş metaforu üzerinden çerçevelemişlerdir. Bu militarize edilmiş söylem, devletlere normal koşullarda kabul

edilmesi güç olan istisnai önlemleri alma ve uygulama yönünde güçlü bir meşruiyet zemini sağlamıştır (Daoudi, 2020). Halk sağlığını koruma amacıyla gerçekleştirilen bu güvenikleştirme sürecinde, temel sivil özgürlüklerin aşağıda maddeler halinde sunulan biçimlerde kısıtlandığı görülmektedir.

- *Hareket Özgürlüğünün Kısıtlanması:* Pandeminin en kritik dönemlerinde uygulanan sokağa çıkma yasakları, şehirlerarası ve uluslararası seyahat kısıtlamaları ve zorunlu karantina tedbirleri, bireylerin en temel haklarından biri olan serbest dolaşım hakkını fiilen askıya almıştır (Parmet ve Sinha, 2020).
- *Toplanma ve İfade Özgürlüğünün Sınırlanması:* Kamusal alanlarda toplanma yasakları, protesto gösterilerinin önlenmesine yol açarken; bazı ülkelerde kriz yönetimine yönelik eleştirel sesler, yanlış bilgi yayma suçlamalarıyla baskı altına alınmış ve ifade özgürlüğü ciddi şekilde daraltılmıştır (Chiozza ve King, 2022).
- *Mahremiyetin İhlali ve Dijital Gözetim:* Temas takip (contact tracing) uygulamaları, virüsün yayılımını izlemek ve bulaş zincirlerini kırmak için etkili bir araç olarak sunulmuş; ancak bu teknolojiler, devletlerin vatandaşlarının konum verilerini, sosyal ağlarını ve kişisel sağlık bilgilerini toplu şekilde izlemelerine imkân tanımıştır. Bu durum, gizlilik ve veri güvenliği alanında ciddi etik ve hukuki tartışmaları beraberinde getirmiştir (Morley vd., 2020).

Pandemi sürecinde uygulanan istisnai önlemler, halk sağlığının korunması ile sivil özgürlüklerin gözetilmesi arasındaki kırılğan dengeyi bir kez daha görünür kılmıştır. Bu noktada, Rita Floyd'un geliştirdiği "Adil Güvenikleştirme Teorisi", güvenikleştirme süreçlerinin varoluşsal tehdide dayalı olup olmadığını ve bu süreçlerin etik ve normatif meşruiyetini sorgulama imkânı sunan analitik bir çerçeve sağlamaktadır. Pandeminin nesnel olarak varoluşsal bir tehdit teşkil ettiği ve referans nesnesi olarak insan yaşamının meşru bir güvenlik değeri taşıdığı konusunda genel bir mutabakat mevcuttur. Ancak Floyd'a göre bu, alınan tüm önlemlerin kendiliğinden adil kabul edilmesini garanti etmez. Aksine, güvenikleştirme sürecinin orantılılık, etkililik ve temel insan haklarına saygı gibi ölçütler çerçevesinde her bir vaka özelinde titizlikle değerlendirilmesi gerekir (Floyd, 2011).

Bu çerçevede yapılan bir saha araştırması, örneğin Afrika'da sokağa çıkma yasaklarının polis şiddetiyle uygulanmasına yönelik halk tepkilerini analiz etmiş ve bireylerin, zorlayıcı güvenlik önlemleri yerine sosyal mesafe, hijyen uygulamaları ve halk sağlığı bilgilendirmesi gibi sağlık temelli yaklaşımları daha meşru ve gerekli bulduklarını ortaya koymuştur (Kanyako, 2024). Bu bulgu, adil güvenikleştirme sürecinde karar vericilerin niyetlerinin, toplumun algısının, rızasının ve tepkilerinin de meşruiyetini belirleyici bir parçası olduğunu göstermektedir. Kitlenin pasif bir onay nesnesi değil, güvenikleştirme sürecinin aktif bir etik sınıyıcısı olduğu yönündeki görüş, bu bağlamda daha da önem kazanmaktadır.

Sonuç

Yeni güvenlik tehditlerinin doğası, ulusal güvenlik anlayışının hem kavramsal çerçevesinde hem de pratik uygulamalarında köklü bir dönüşümü zorunlu kılmaktadır. Siber güvenlik, iklim krizi ve pandemi gibi tehditler, klasik anlamda devlet merkezli, askerî odaklı ve sınır temelli güvenlik yaklaşımlarının artık yetersiz kaldığını açıkça göstermektedir. Bu tehditler sosyal, ekonomik, çevresel ve bireysel güvenliği de kapsayan çok boyutlu yapılarıyla, ulusal güvenlik politikalarının yeniden tanımlanmasını ve bütüncül bir perspektifle ele alınmasını gerektirmektedir.

Siber saldırılar kritik altyapıları hedef alarak devletlerin bilgi sistemlerini, kamu hizmetlerini ve hatta demokratik süreçlerini tehdit ederken; iklim değişikliği su, enerji ve gıda gibi yaşamsal kaynaklar üzerinde baskı oluşturarak toplumsal huzursuzluklara, göç hareketlerine ve jeopolitik gerilimlere yol açmaktadır. Pandemiler ise başta sağlık sistemleri olmak üzere ekonomi, eğitim, iş gücü ve sosyal düzeni doğrudan etkileyerek güvenliğin kapsamını biyopolitik düzeye taşımaktadır. Bu bağlamda yeni tehdit ortamında, güvenliğin düşmanla mücadele etmekten ibaret olmadığını, bu nedenle de sistemlerin krizlere karşı dirençli hale getirilmesini, bireylerin temel haklarının korunmasını ve toplumsal bütünlüğün sağlanmasını da içeren çok katmanlı bir yaklaşımı gerekli kılmaktadır.

Bu çerçevede, ulusal güvenlik mimarisinin yeniden inşasında dört temel unsur öne çıkmaktadır: bütüncüllük, dayanıklılık, insan güvenliği ve çok taraflılık. Ancak bu ilkeler birbirinden bağımsız değil; aksine bir güvenlik sisteminin parçaları olarak birbirini tamamlayıcı niteliktedir. Bütüncül yaklaşım, güvenliğin askerî ya da diplomatik alan da dahil olmak üzere sağlık, çevre, tarım ve dijital altyapı gibi çok sayıda sektörde eş zamanlı olarak ele alınmasını ve kurumlar arası koordinasyonun artırılmasını gerektirmektedir.

İnsani güvenlik ise güvenlik kavramının merkezine bireyi yerleştirerek, temel hak ve özgürlüklerin, yaşam koşullarının ve insan onurunun korunmasını esas almaktadır. Devletin güvenlik politikaları bireylerin haklarını zayıflatmamalı; aksine onları güçlendirecek biçimde kurgulanmalıdır. Bu nedenle siber güvenlik yasalarının ifade özgürlüğünü kısıtlamaması, iklim politikalarının yoksul toplulukları dışlamaması ve pandemiye karşı alınan önlemlerin toplumsal eşitliği gözetmesi gerekmektedir. Bu yeni tehditler küresel ölçekte etkiler yarattığından, uluslararası iş birliği, norm geliştirme, kolektif bilgi üretimi ve çok taraflı mekanizmalarla birlikte ele alınması gereken bir alan haline gelmiştir.

Türkiye örneği üzerinden değerlendirildiğinde, mevcut ulusal güvenlik stratejilerinin bu yeni tehdit ortamına uyum sağlama konusunda bazı yapısal eksiklikler taşıdığı görülmektedir. Siber güvenlik alanında teknik altyapı kadar hukuki ve kurumsal çerçevenin de geliştirilmesi gerekmektedir. İklim krizinin güvenlik politikalarına entegrasyonu ise

henüz yeni sayılabilir. Pandemi sonrası sağlık sisteminin dayanıklılığını artırmaya yönelik yapılan düzenlemeler olumlu bir adım olmakla birlikte, bu süreçte kırılğan grupların özel ihtiyaçlarına dönük sosyal politika araçlarının yeterince güçlü olmadığı da dikkat çekmektedir. Ayrıca, Türkiye'nin bölgesel ve uluslararası güvenlik forumlarına daha aktif katılımı, hem bilgi ve kapasite paylaşımı açısından hem de bölgesel istikrarın sağlanmasında kritik bir rol oynayabilir.

Sonuç olarak, 21. yüzyılın güvenlik anlayışı, sınırları korumak ya da düşmanı caydırmakla sınırlı değildir. Bu nedenle ulusal güvenlik, çok aktörlü, çok katmanlı ve çok disiplinli bir anlayışla yeniden ele alınmalıdır. Tehditlerin doğasına uygun olarak tasarlanmış, kırılğanlıkları azaltmayı, dayanıklılığı artırmayı ve bireylerin haklarını korumayı amaçlayan bir güvenlik vizyonu, günümüzün karmaşık krizleriyle başa çıkabilmek için gereklidir. Bu dönüşüm, siyasal kararlılığın gerekliliğine ek olarak toplumsal farkındalık, bilimsel katkı ve uluslararası dayanışma ile gerçekleştirilebilir. Türkiye gibi yükselen bölgesel aktörler açısından, bu yönde atılacak her adım, iç güvenliğe katkı sunduğu gibi küresel düzeyde de güvenliğe katkı sağlayacak stratejik bir yatırım anlamına gelecektir.

Kaynaklar

- Ahmed, F., Ahmed, N. E., Pissarides, C., ve Stiglitz, J. (2020). Why inequality could spread COVID-19. *The Lancet Public Health*, 5(5), e240.
- Boas, I., Farbotko, C., Adams, H., Sterly, H., Bush, S., Van der Geest, K., ... ve Hulme, M. (2019). Climate migration myths. *Nature Climate Change*, 9(12), 901-903.
- Burwell, S. M. (2021). *Improving pandemic preparedness: lessons from COVID-19*. Council on Foreign Relations.
- Buzan, B., Wæver, O., ve De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.
- Cavelty, M. D. (2007). *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.
- Centeno, M. A., Nag, M., Patterson, T. S., Shaver, A., ve Windawi, A. J. (2015). The emergence of global systemic risk. *Annual Review of Sociology*, 41(1), 65-85. Waltz
- Chiozza, G., ve King, J. (2022). The state of human rights in a (post) COVID-19 world. *Journal of Human Rights*, 21(3), 246-262.

Cinelli, M., Quattrociochi, W., Galeazzi, A., Valensise, C. M., Brugnoli, E., Schmidt, A. L., ... ve Scala, A. (2020). The COVID-19 social media infodemic. *Scientific reports*, 10(1), 16598.

Daoudi, S. (2020). The war on covid-19: the 9/11 of health security. *Policy Paper*, (20-06).

Demchak, C., Kerben, J., McArdle, J., ve Spidalieri, F. (2015). Cyber readiness index 2.0. *Potomac Institute for Policy Studies*.

Demirbaş, M., Çelik, A. ve Akıncıoğlu, N. U. (2023). Suç korkusuna teorik bir yaklaşım. *Külliyeye Uluslararası Sosyal Bilimler Dergisi*, 4(2), 224–241. <https://doi.org/10.48139/aybukulliyeye.1339633>

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Dimari, G., ve Papadakis, N. (2023). The securitization of the Covid-19 pandemic in Greece: a just or unjust securitization?. *Quality ve Quantity*, 57(Suppl 1), 77-97.

Floyd, R. (2010). *Security and the environment: Securitisation theory and US environmental security policy*. Cambridge University Press.

Floyd, R. (2011). Can securitization theory be used in normative analysis? Towards a just securitization theory. *Security Dialogue*, 42(4-5), 427-439.

Floyd, R. (2019). *The morality of security: A theory of just securitization*. Cambridge University Press.

Gereffi, G. (2020). What does the COVID-19 pandemic teach us about global value chains? The case of medical supplies. *Journal of International Business Policy*, 3(3), 287.

Gleick, P. H. (2014). Water, drought, climate change, and conflict in Syria. *Weather, climate, and society*, 6(3), 331-340.

Greer, S. L., King, E. J., da Fonseca, E. M., ve Peralta-Santos, A. (2020). The comparative politics of COVID-19: The need to understand government responses. *Global public health*, 15(9), 1413-1416.

Hansen, L., ve Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, 53(4), 1155-1175.

Homer-Dixon, T. F. (2010). *Environment, scarcity, and violence*. Princeton University Press.

- Kaldor, M. (2013). *New and old wars: Organised violence in a global era*. John Wiley ve Sons.
- Kanyako, V. (2024). *Civil Society and Peacebuilding in Sierra Leone: Donors, Government, and Human Security*. Routledge.
- Kavsıracı, O. (2019). Türkiye'nin iç güvenlik algısı ve politikaları (1980-1990). *OPUS—Uluslararası Toplum Araştırmaları Dergisi*, 14(20), 2074-2097. DOI: 10.26466/opus.605112.
- Kavsıracı, O. (2020). Klasik Realizm-Güvenlik İlişkisi Çerçevesinde Türkiye'nin İç Güvenlik Politikaları (1923-1960). *Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, 18(Armağan Sayısı), 117-128.
- Kavsıracı, O., ve Demirbaş, M. (2020). İstihbarat Faaliyetlerinin Devlet Güvenliği Açısından İncelenmesi. *Anadolu Strateji Dergisi*, 2(1), 49-64.
- Morley, J., Cowls, J., Taddeo, M., ve Floridi, L. (2020). Ethical guidelines for COVID-19 tracing apps. *Nature*, 582(7810), 29-31.
- Newman, E. (2001). Human security and constructivism. *International studies perspectives*, 2(3), 239-251.
- Osthagen, A. (2020). *Coast guards and ocean politics in the Arctic*. Singapore: Palgrave Macmillan.
- Overhaus, M. (2014). *Quadrennial Defense Review 2014: Entwicklungstrends US-amerikanischer Verteidigungspolitik und Konsequenzen für die Nato*.
- Parmet, W. E., ve Sinha, M. S. (2020). Covid-19—the law and limits of quarantine. *New England Journal of Medicine*, 382(15), e28.
- Singer, P. W., ve Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
- Such, L. (2022). *CLIMATE CHANGE IN THE DEPARTMENT OF DEFENSE (Doctoral dissertation)*.
- Trombetta, M. J. (2008). Environmental security and climate change: analysing the discourse. *Cambridge review of international affairs*, 21(4), 585-602.
- UNDP, U. (1994). *Human development report 1994: New dimensions of human security*. *New York*. Retrieved December, 12, 2022.

Vuori, J. A. (2008). Illocutionary logic and strands of securitization: Applying the theory of securitization to the study of non-democratic political orders. *European journal of international relations*, 14(1), 65-99.

Walt, S. M. (1991). The renaissance of security studies. *International studies quarterly*, 35(2), 211-239.

Waltz, K. (1979). Theory of international relations (pp. 111–114). *Reading, MA: Addison-Webley*.