YENİ YÜZYIL'DA İLETİŞİM ÇALIŞMALARI DERGİSİ

OCAK 2026
JANUARY 2026

Cilt/*Volume:* 4
Sayı/*Issue:* 13
ISSN: 2757-7007
SS: 171-186

https://dx.doi.org/10.66009/0.2026.10

SPLINTERNET: SİBER EGEMENLİK ÇAĞINDA DİJİTAL PARÇALANMANIN JEOPOLİTİĞİ

SPLINTERNET: THE GEOPOLITICS OF DIGITAL FRAGMENTATION IN THE AGE OF CYBER SOVEREIGNTY

Dr. Seda KARAGÖZ
Bağımsız Araştırmacı
ORCID ID: 0000-0003-3929-861X, karagoezseda@hotmail.com

ÖZ
Bu çalışma, dijital çağın yeni siyasal stratejileri ve jeopolitiğini şekillendiren merkezî kavramlardan biri hâline gelen splinternet olgusunu, siber egemenlik ekseninde ele almaktadır. 1990'lı yıllarda dijital müşterekler ve internete erişim hakkı gibi ilkeler temelinde idealize edilen internet, bugün otoriter ve sağ popülist iktidarlar tarafından ulusal çıkarlar doğrultusunda parçalanmaya başlamıştır. Özellikle COVID-19 sonrası ivme kazanan dijital dönüşüm süreciyle birlikte devletler, siber uzam üzerindeki teknik ve siyasal kontrol kapasitelerini artırmış; internetin küresel ve bütünlüklü niteliği aşınarak yerini ulusal çıkarların belirlediği parçalı bir mimariye bırakmıştır. "Yeni devletçilik" olarak adlandırılan bu süreçte siyasal alanda ulusal güvenlik odaklı uygulamalar güç kazanırken, dijital uzam, sansür ve algoritmik kontrol mekanizmalarının belirlediği panoptik bir niteliğe bürünmüştür. Çin ve Rusya gibi devletler ileri düzeyde izolasyona dayalı splinternet pratiklerine yönelirken, ABD, Türkiye ve Hindistan gibi devletler kısmî plâtform kontrolüne dayalı siber egemenlik politikalarını benimsemiş; Avrupa Birliği ise regülasyon yasalarıyla dijital alana normatif bir boyut kazandırmıştır. Son olarak Rusya-Ukrayna ve İsrail-Filistin savaşları splinternet olgusunu jeopolitik düzleme taşıyarak onu hegemonik bir araca dönüştürmüş; dijital plâtformlar ise taraflar açısından çatışmaların etkin bir bileşeni hâline gelmiştir. Sonuç olarak, splinternet, yalnızca teknik bir parçalanma değil; dijital egemenliğin yeniden tesis edildiği farklı bir siber düzenin habercisi olarak karşımıza çıkmaktadır.

Anahtar kelimeler: Splinternet, Siber egemenlik, Yeni devletçilik

ABSTRACT
This study examines the phenomenon of the splinternet -which has become one of the central concepts shaping the new political strategies and geopolitics of the digital age- through the lens of cyber sovereignty. The internet, idealized in the 1990s on the basis of principles such as digital commons and the right to internet access, has today begun to fragment along national interests by authoritarian and right-wing populist regimes. With the acceleration of digital transformation processes particularly after COVID-19, states have strengthened their technical and political control capacities over cyberspace; as a result, the global and unified nature of the internet has eroded, giving way to a fragmented architecture defined by national priorities. In this process, described as "neo-statism", national-security-oriented political practices have gained prominence, while digital space has taken on a panoptic character shaped by mechanisms of censorship and algorithmic control. While states such as China and Russia have turned to splinternet practices based on advanced levels of isolation, states such as the US, Turkey, and India have adopted cyber sovereignty policies based on partial platform control; the European Union, on the other hand, has introduced a normative dimension to the digital realm through regulatory laws. Finally, the Russia-Ukraine and Israel-Palestine wars have carried the splinternet phenomenon into the geopolitical arena, transforming it into a hegemonic tool, while digital platforms have become an active component of the conflicts for all parties evolved. In conclusion, the splinternet represents not merely a technical fragmentation, but a harbinger of a different cyber order in which digital sovereignty is being reconstituted.

Keywords: Splinternet, Cyber sovereignty, Neo-statism

GİRİŞ

Neredeyse yarılamış olduğumuz 2020'li yıllar, siber-ütopyacıların büyük bir şevkle savunduğu dijital demokrasi ideallerini kökten sarsacak türden gelişmelere sahne oldu: 2020 yılı Mart ayında pandemiye dönüşen COVID-19, İspanyol gribinden sonra görülen en geniş çaplı ve ölümcül hastalık olarak kayıtlara geçti. Hükümetler ise hayatın hemen her alanında krizlere yol açan bu hastalığı kendi iç gözetim kapasitelerini genişletmek ve internet özgürlüğünü sınırlandırmak için bir fırsat olarak değerlendirmeyi tercih etti. Devamında Rusya'nın Ukrayna'ya, İsrail'in Filistin'e yönelik saldırıları, Avrupa'da sağ partilerin başa gelmesi/güçlenmesi ve Amerika Birleşik Devletleri'nde (ABD) Trump'ın geri dönüşüyle birlikte internet, devletlerin egemenlik, güvenlik, ekonomi ve ideoloji temelli çıkarlarını şekillendirdiği yeni bir dijital-jeopolitik cepheye dönüşmeye başladı.

Yakın bir geçmişe kadar internetin demokratik katılımı teşvik eden ve hatta doğrudan demokrasiyi yeniden tesis edebilecek bir dijital kamusal alan olarak yüceltildiği, özellikle de Arap coğrafyasındaki isyanlarla birlikte toplumsal hareketlerin önemli bir itici gücü olarak görüldüğü iyimser anlayış akademide güçlü bir şekilde savunulurken, bugün ibre tersine dönmektedir. Bahsi geçen gelişmelere paralel olarak internet, ulus devletler ve teknoloji devlerinin gitgide yükselen duvarları arasında sıkışık ve parçalı bir görünüme bürünmektedir. Bu parçalı yapı, alanyazında 2000'li yılların başlarından itibaren "splinternet" kavramıyla ele alınmakta; ilgili kavram, siber alanın başlangıçtaki küresel birlik ve açıklık idealinin yerini ulusal sınırlar, bölgesel regülasyonlar ve farklı politik rejimlerin müdahaleleriyle çok merkezli bir düzene bırakmasını ifade etmektedir. Splinternet tartışmaları ayrıca siber egemenlik ve jeopolitik kuramsal çerçevelerle ilişkilendirilmekte; bu doğrultuda siber dünyada güncel gelişmeleri anlamlandırmak için önemli bir teorik altyapı sunmaktadır.

Bu çalışma nitel doküman analizi yöntemiyle yürütülmüş betimleyici bir araştırmadır. Konusunu literatürde "splinternet" kavramıyla ifade edilen bu dijital parçalanma ve sınırlandırma olgusu oluşturmakta; özellikle pandemi sonrası dönemde özgür, açık, evrensel ve müştereklere dayalı bir internet tahayyülünden nasıl giderek uzaklaşıldığı gerçeği, belli başlı ülkelerden örneklerle anlatmaktadır. İnceleme kapsamında ulusal ve uluslararası alanyazın, resmî kurum raporları ile güncel haber kaynakları incelenmiş; kaynaklar konuya ilişkin güncellik, erişilebilirlik ve splinternet pratiklerine dair somut veri sunma kriterleri esas alınarak seçilmiştir. Analiz sürecinde nitel dokümanlar, siber egemenlik, devlet-merkezli regülasyon, internete erişim hakkı gibi temalar altında çözümlenmiştir. Bu çerçevede farklı ülkelerin izlediği yöntemler hem benzerlikleri hem de ayrışan yönleri bakımından değerlendirilmiştir. Çalışma, kapsamı gereği splinternet olgusuna yönelik kavramsal ve betimleyici bir giriş mahiyetindedir. Söz konusu olgulara yönelik tartışmaların Türkçe literatürde henüz kurumsallaşmamış olması, çalışmaya özgün bir nitelik kazandırmaktadır. Bu bağlamda makale, siber egemenliğin güncel yönelimlerini kavramsal bir tartışma zemininde ele almakta ve splinternet olgusunun teknik parçalanmanın ötesinde, yeni bir jeopolitik düzenin göstergesi olduğunu ileri sürmektedir.

1. SİBER EGEMENLİK KUŞATMASI ALTINDA SİYASALLAŞAN KÜRESEL AĞLAR

Son yıllarda, özellikle hukuk literatürü başta olmak üzere akademik çalışmalarda, "internet özgürlüğü" tabirinden ziyade ağırlıklı olarak kamusal bir hakkı ifade eden "internete erişim hakkı" tabiri tercih edilmektedir. Zira internet kullanımının herhangi bir engelleme veya kısıtlamaya maruz kalmadan gerçekleşebilmesi, öncelikle internet erişiminin devletler tarafından eşit bir kamusal hak olarak tanınmasına bağlıdır. Bu noktada teknik altyapının güçlendirilmesi, internete erişimi mümkün kılan teknolojik araçların yaygınlaşması ve satın alma gücü yetersiz yurttaşlara bu araçların ücretsiz verilmesi internete erişim hakkının asli bileşenleri olarak kabul edilmektedir. Bağlantı hızının yeterliliği ile sansür ve gözetimden arındırılmış bir çevrim içi iletişimin güvence altına alınması da aynı hak kapsamına dahil edilmekte ve tüm bu düzenlemeler devletlerin sorumluluk alanı içinde değerlendirilmektedir (Demir, 2025).

Ancak 1990'lı yıllarda internetin küresel çapta kullanıma açılması ve yaygınlaşması, internete erişim hakkı üzerinde Demokles'in kılıcı gibi sallanacak siber

egemenlik[1] tartışmalarını da beraberinde getirmiştir. Özellikle 2009 yılı sonunda Arap coğrafyasında başlayan isyanlar, devletlerin internete yönelik müdahaleleri ile kitlesel çevrim içi gözetim pratiklerinin görünür hâle geldiği bir dönemin işaret fişeği olmuştur. Arap isyanları ve devamında pek çok ülkede patlak veren ayaklanmalarda, web 2.0 teknolojileriyle hayatımıza giren sosyal medya plâtformları yadsınamaz bir rol oynamıştır. Bu durum, siber egemenlik-demokrasi ikilemini daha da derinleştirmiştir.

Esasen web 2.0 teknolojisi, internetin kullanım şekli ve işlevini kökten değiştirerek yeniden tanımlanmasına neden olacak türden gelişmeleri ortaya çıkarmıştır. İlk nesilden farklı olarak web 2.0'da kullanıcıların içerik üretebilmesi, birbirleriyle etkileşime girebilmesi ve bu yollarla topluluklar oluşturabilmesi internete sosyal bir ekosistem olma niteliği kazandırmıştır. Bu durum medya ve demokrasi arasında uzun yıllardır tartışılagelen simbiyotik ilişkinin dijital düzleme taşınmasında etkili olmuştur. İnternetin katılıma olanak veren yapısı, farklı seslerin duyurulması ve böylece gerçek anlamda bir demokrasi kültürünün geliştirilmesi için önemli bir fırsat sunmuştur. Zira modern iletişim teknolojileri, merkezî kontrol mekanizmaları ile bürokratik hiyerarşi üzerinden şekillenen geleneksel güç anlayışını sarsarak gücün daha dağıtık, iktidar ilişkilerinin ise daha dinamik ve akışkan hâle gelmesine olanak sağlamıştır. Bilgiye erişimin ve paylaşımın hızlanması, birey ve grupların toplumsal güç ilişkilerinde daha etkin bir özne olarak rol alabilmesini mümkün kılmıştır. Bu durum, toplumsal katılımı güçlendirerek demokratik süreçlerin genişlemesine katkı sunmuştur (Castells, 2016).

Ancak tıpkı toplumlar gibi onların dijital uzantılarında da toplumsal güç ilişkilerinden bağımsız "Heliopolis[2]"lerin kurulamayacağı kısa sürede anlaşılmıştır. Morozov'un (2019) deyimiyle -"siber ütopyacıların" ileri sürdüğü argümanların aksine- yeni iletişim teknolojilerinin demokratikleşmeye katkı sunan "nötr araçlar" olduğu miti, Batılı liberal demokrasiler de dahil tüm rejimlerde paramparça olmuştur. Örneğin, 2013 yılında ABD'de bizzat "içeriden" birinin, Edward Snowden'ın ifşaatları NSA[3]'in Google, Microsoft, Facebook, YouTube, Yahoo vb. büyük teknoloji şirketlerinin sunucularına doğrudan erişim sağladığını ve bu yolla dünya genelinde milyonlarca insanı hukuka aykırı bir şekilde izlediğini ortaya koymuştur. Devamında 2016 yılı başkanlık seçimleri öncesinde Cambridge Analytica adlı veri analiz şirketi, milyonlarca vatandaşın verilerine haberleri olmadan erişmiş ve mikro-hedefleme yoluyla özellikle kararsız seçmenleri manipülatif içeriklerle yönlendirmiştir (Hoffmann vd., 2020).

Bahsi geçen "kabul edilemez" vakalar ayyuka çıktığında, devletlerin yasal düzenlemelerle kurumsallaştırdığı denetim-sansür mekanizmaları ile küresel dijital eşitsizliğin yarattığı bilgiye erişim ve katılım adaletsizliklerinin varlığı, çoktan beridir zaten bilinmekteydi. Buna ek olarak, manipülatif, sansasyonel veya kutuplaştırıcı içeriklerin öne çıkarılması, kullanıcı verileri ve üretken katılımla edinilen sermaye birikimi ile algoritmik sessizleştirme gibi pratikler de dijital ortamın demokrasi açısından taşıdığı risklerin boyutunu daha fazla görünür kılmaktaydı. Bu noktada devletler, -örneğin başta 11 Eylül öncesi ABD- gözetim ve sansür uygulamalarını genellikle gizli yürütmeyi ya da en azından afişe etmemeyi tercih ederken pandemi süreciyle birlikte dijital baskı mekanizmalarının "toplum sağlığı", "kamusal güvenlik" gibi gerekçelerle açıkça meşrulaştırıldığı ve yasal zemine oturtulduğu yeni bir evreye geçilmiştir. Dolayısıyla COVID-19 pandemisi, internette gözetim ve denetim pratiklerinin önce geçici, ardından kalıcı ve yasal hâle gelmesinde bir katalizör işlevi görmüştür. Ardı ardına birçok devlet, ulusal güvenlik, dezenformasyonla mücadele, çocukların korunması gibi "toplumsal" gerekçeleri ileri sürerek dijital mecralara yönelik yasal düzenlemelere gitmiştir (Racine, 2023).

1.1. Pandemi Sonrası Yeni Devletçilik ve Sağ Popülizmin Yükselişi

2021'de pandemi kısıtlamalarının kademeli olarak kaldırılmaya başlanmasıyla küresel gerginlik tırmanışa

[1] Siber egemenlik, ulusal egemenliğin siber uzaydaki uzantısıdır. Bir devletin ulusal egemenliği temelinde, kendi topraklarındaki siber altyapı, varlıklar, davranışlar ile ilgili veri ve bilgiler üzerinde sahip olduğu iç üstünlük ve dış bağımsızlık olarak tanımlanmaktadır (World Internet Conference, 2024).

[2] Heliopolis: Anadolu'nun bilinen ilk devrimcilerinden Aristonikos'un M.Ö. 133'te Roma Cumhuriyeti'ne karşı önderlik ettiği isyanda "Köleliğin olmadığı; herkesin eşit hakka sahip olduğu bir ülke: Güneş Ülkesi" vaadidir (Türk, 2024).

[3] Ulusal Güvenlik Ajansı: ABD'nin yabancı ülkelerin iletişim faaliyetleri hakkında bilgi toplayan istihbarat kurumudur (Brittanica, 2025).

geçmiş; önce Doğu Avrupa'da, ardından Ortadoğu'da büyük can kaybı ve yıkımların yaşandığı geniş çaplı savaşlar başlamıştır. Enerji ve gıda fiyatlarındaki yükseliş, küresel çapta enflasyon artışına neden olmuştur. Birçok ülkede esnek ve güvencesiz çalışma biçimleri kalıcı hâle gelmiş, genç işsizlik oranları yükselmiş, varlıklı sınıflar ile emekçi kesimler arasındaki ekonomik uçurum derinleşmiştir. Ayrıca, kamu borçları rekor seviyelere ulaşmıştır. Küresel iklim değişikliği nedeniyle başta aşırı sıcak hava dalgaları olmak üzere hava anomalileri artmış, kuraklık hem içme suyuna erişim hem de tarım için önemli bir tehdit hâline gelmeye başlamış, Kanada'da ve Akdeniz ülkelerinde yaz aylarında geniş ölçekli orman yangınları yaşanmıştır (IMF World Economic Outlook October, 2021; OECD Employment Outlook, 2021).

Bu süreçte özellikle alt ve orta sınıfların yüksek işsizlik, enflasyon ve ekonomik durgunluk nedeniyle yaşadığı güvensizlik duygusu, başta Avrupa kıtası olmak üzere dünya genelinde sağ popülist partilerin "ekonomik korumacılık", "yerlilik" "ulusal kimlik" ve "millî çıkarlar" gibi temalar üzerinden söylem oluşturmasında etkili olmuştur. Buna son yıllarda büyüyen göçmen-mülteci dalgası da eklendiğinde, pek çok ülkede bu tip partiler iktidara taşınmıştır (Baritci, 2024; Çetin, 2020). Milliyetçilik ve ekonomik kalkınmacılığın bir sentezi olarak nitelendirilebilecek olan sağ popülizm, diğer sağ ideolojilerden farklı olarak etnik köken, yerlilik, kültürel içe kapanma ve hatta zaman zaman doğrudan yabancı sermayeye karşıtlık gibi vurgular üzerinden şekillenmektedir (İyiekici, 2024). Schmitt'in (2012) dost-düşman ayrımını esas alan bu ideolojide, siyaset bir nevi "hayatta kalma" meselesi olarak görülmektedir. Popülist liderler, tehdit olarak gördükleri kesim ve kurumları (göçmenler/mülteciler, LGBTİ+ bireyler, muhalif medya, küreselciler, Avrupa Birliği gibi devletler üstü örgütler, bürokrasi vb.) düşmanlaştırmaktadır.

Gerbaudo'nun (2022) kurumsallaşmasını "yeni devletçilik[4]" kavramıyla incelediği sağ popülist yönetimler, -neoliberalizmin aksine- devletin toplumu koruyabilmesi için ekonomiye daha güçlü bir şekilde müdahale etmesi gerektiğini savunmaktadır. 1970'lerden itibaren neoliberalizmin temel mantığı, refah devletini zayıflatmak uğruna devletin oyun kurucu ve müdahaleci rolünü reddetmeye dayanırken pandemi sonrası güçlenen popülist yönelimler, devletleri bir yandan oldukça güçlü ancak diğer yandan daha parçalı, çelişkili ve güvenlik odaklı birer aktör hâline getirmiştir (Akçay, 2025). Sonuç olarak, giderek daha katı, merkeziyetçi, korumacı ve doğal olarak buna eşlik eden otoriterleşme eğilimleri ile karakterize edilen yeni devletçi siyaset anlayışı, dijital düzlemde ise kendisini splinternet pratikleri ile göstermeye başlamıştır.

2. SPLINTERNET: DİJİTAL SINIRLARLA ÇİZİLEN SİYASAL HARİTALAR

Sovyetler'in çöküşünü -büyük ölçüde- bir zafer anlatısı şeklinde yorumlayan küreselleşme yazını, 1990'lı yıllarda "özgürlük" ve "değişim" merkezli retoriğini teknolojik düzlemde internet ve onun "bilginin serbest dolaşımını mümkün kılan" yapısı üzerine inşa etmiştir. İnternetin "ağların ağı" olması, bu yapının anlık etkileşime ve paylaşım kültürünün gelişimine olanak vermesi, siyasal açıdan evrensel, katılımcı ve özgürlükçü bir mecra olarak karakterize edilmesini mümkün hâle getirmiştir. Ancak son yıllarda internet, küresel ve sınır tanımayan bir ağ olma özelliğini giderek kaybetmeye başlamıştır. Birçok devlet, siber altyapıyı kendi güvenlik stratejileri ve ulusal çıkarları doğrultusunda şekillendirmekte; internete erişim hakkı ve bilgi akışını regüle etme yoluna gitmektedir (Deibert, 2013).

Bu durum internetin yekpare bir alan olmaktan uzaklaşarak teknik ve normatif yönden farklı sınırlar ve bölgesel yapılar etrafında şekillenmeye başladığını göstermektedir. Özellikle siber egemenlik, veri güvenliği ve bilgi güvenliği gibi kavramlar, internetin evrensel ölçekteki serbest dolaşımına dair liberal yaklaşımları sorgulamaya açmıştır. 2000'li yıllardan itibaren Çin'in başlattığı ilk büyük dijital ölçekli bölgesel sınırlamalar, interneti kısa sürede yeniden tanımlayan ve tayin eden bir egemenlik stratejisine dönüşürken, onun doğasına dair özgürlükçü tahayyülleri de sarsmaya başlamıştır (Mhalla, 2023). Devamında başka ülkelerin de Çin'i izlemesiyle, başlangıçta küresel çapta bir kamusal alan oluşturabileceği varsayılan internet, zamanla "içten dışa doğru örülen dijital duvarlar"la

[4] Sosyolog ve siyaset kuramcısı Paolo Gerbaudo'nun "yeni devletçilik" kavramı, özellikle pandemi sonrasında devletlerin kriz söylemiyle meşrulaştırma çabası içine girdiği otoriterleşme eğilimlerini ifade etmektedir. Bu yaklaşım, piyasa mekanizmalarının sınırlanması, karar alma süreçlerinin merkezileşmesi ve ulusal çıkar söyleminin güçlenmesi gibi dinamiklerle karakterizedir (Gerbaudo, 2022).

çevrili; normatif açıdan parçalı-çok katmanlı bir yapıya evrilmiştir.

İngilizce'de "parçalanmak" anlamına gelen *splinter* kelimesi ile *internet* sözcüklerinin birleşiminden oluşan "splinternet" kavramı, ilk kez 2001 yılında Clyde Wayne Crews tarafından internetin siyasi, ideolojik ve ticarî gerekçelerle parçalanarak birbirinden kopuk ağ yapılarına dönüşmesini ifade etmek için kullanılmıştır (Nocetti, 2024). Siyasal düzlemde splinternet, internetin mikro ve izole parçalara (ağlara) bölünmesi anlamına gelmektedir. Bu bölünme, hükümetlerin kendi ülkelerindeki kullanıcıların erişim ve paylaşımlarını kontrol altına almak için bölgesel intranetler kurma çabalarıyla gerçekleşmektedir (Ananthaswamy, 2011). Birbirlerine bağlı otonom ağlardan oluşan küresel bir sistem olan internet, tanımı ve doğası gereği bütünleşik bir siber evren olsa da (pandemi sonrası giderek artan bir hızla) yapısal olarak çeşitli segmentlere bölünmeye başlamıştır. Bu noktada parçalanma, internetin bir kısmının bütünden koparılarak izole edilmesi biçiminde teknik bir boyut taşımasının yanında internet kullanıcılarının çevrim içi içeriğe erişirken yaşadıkları farklı deneyimleri de (içerik parçalanması) kapsamaktadır. Dolayısıyla parçalanma süreci hem altyapısal (teknik) internete hem de evrensel bir siber kamusal alan olan internete (siyasal) uygulanmaktadır. Bu durum esasen bir bütünü ifade eden "ağ"lar için paradoksal bir nitelik taşımaktadır (Perarnaud vd., 2022).

2.1. Ağ Parçalanması Tipleri

Ağ parçalanmaları teknik boyutuyla iki biçimde ortaya çıkmaktadır: Kısmî izolasyon ve tam izolasyon. Kısmî izolasyon bir ağın, küresel internetin belirli kısımlarına erişebilirken geri kalanına erişememesi durumunu ifade etmektedir. Bu tip parçalanmalar, genellikle bölgesel/coğrafi sansür uygulamaları ya da uzun süreli siber güvenlik duvarları ile ortaya çıkmaktadır. Literatürde bu tip izolasyonlar "yarımada" (peninsula) benzetmesiyle nitelenmekte; ağ, bütünden koparılmamış olsa da küresel dijital alana sınırlı şekilde bağlanabilmektedir. Tam izolasyon ise, bir ağın kendi içinde sistematik bir bağlantıya sahip olmasına karşın internetin bütünden tamamıyla koparılması anlamına gelmektedir. Bu tip izolasyonlar ise, "ada" (island) benzetmesiyle nitelenmekte ve genelde devletlerin ulusal düzeyde yürüttüğü kapsamlı filtreleme, dijital güvenlik gerekçeli bağlantı kesintileri ya da siyasal izolasyon stratejilerini ifade etmektedir (Baltra ve Heidemann, 2021). Özetle, splinternet olgusu temelde iki teknik düzeyde ele alınmaktadır. Kısmî izolasyon, küresel internetin aşamalı olarak zayıflatıldığı bir durumu anlatırken tam izolasyon ise, coğrafî (genellikle ulusal) sınırlar temelinde küresel internetten ayrışmış, bu doğrultuda yeniden yapılandırılmış/regüle edilmiş siber alanların oluşumuna işaret etmektedir. Bununla birlikte tam izolasyon, literatürde yalnızca teorik bir eşik durumu olarak yer almakta; uygulamada ise ağların genelde küresel altyapıyla çok sınırlı ve kontrollü de olsa etkileşimi (uluslararası finans, ticaret sistemi, tedarik zincirleri ve diplomasi yoluyla) devam etmektedir. Dolayısıyla literatürde "tam izolasyon" olarak nitelenen bu uç durum, pratikte ileri/yüksek izolasyon[5] olarak karşımıza çıkmaktadır.

Siyasal boyutuyla ele alındığında splinternet, bugün çoğunlukla dünyada son yıllarda sağ popülist partilerin güçlenişi ve yeni devletçilik olarak kavramsallaştırılan ulusal egemenlik merkezli politik rasyonalite ile ilişkilendirilse de olgunun tarihsel kökeni bu gelişmelerden daha eskiye dayanmaktadır. 2000'li yılların başlarından itibaren (tarihi savunma duvarına atfen) "Dijital Güvenlik Seddi[6]" ile anılan Çin başta olmak üzere Rusya, İran gibi devletlerin öncülüğünde başlayan bu eğilimler, 2010'lardaki Arap İsyanları ile Orta Doğu'daki rejimlere doğru genişlemiştir. Bu tip rejimler, teknolojik gelişmelere paralel olarak interneti denetim almaya girişmiş; bu yolla devletin meşru otorite tekelini dijital uzamda tesis etmeye çalışmıştır. "Otoriter" olarak nitelendirilebilecek bu devletler, interneti Batı merkezli ve dış tehditlere açık, ideolojik bir araç olarak görmüş; böylece savunmacı bir egemenlik mantığına dayalı olarak çoğunlukla ileri/yüksek izolasyona dayalı, yeniden yapılandırılmış ulusal siber ekosistemler inşa etmeye başlamıştır (Gerbaudo, 2022; Litvinenko, 2021; Tai ve Yi Zhu, 2022).

[5] İleri/Yüksek İzolasyon: İleri/yüksek izolasyon, literatürde tam izolasyon olarak tanımlanan durumun pratikteki karşılığıdır ve ulusal internetin küresel ağdan teknik olarak bütünüyle ayrılmasa da fiilen kapalı devreye yakın işlediği denetim modelidir. Bu modelde devlet hem içerik akışını daraltmakta hem de uluslararası veri geçişini katı şekilde regüle etmektedir. Böylece devlet merkezli bir siber sınır rejimi yaratılmaktadır (Baltra ve Heidemann, 2021).

[6] Dijital Güvenlik Seddi (Great Firewall of China): Dijital Güvenlik Seddi, Çin devletinin uluslararası internet trafiğini denetlemek, filtrelemek ve yeniden yönlendirmek üzere geliştirdiği geniş ölçekli kontrol ve sansür sistemini ifade etmektedir. Bu yapı sadece içerikleri engellemekle kalmamakta; aynı zamanda devletin siber alan üzerindeki ideolojik kontrolünü pekiştiren bir egemenlik mimarisi işlevi görmektedir (Deibert, 2013).

Ancak interneti parçalama pratikleri, son yıllarda Batılı demokratik devletler ile Avrupa Birliği gibi yine liberal değerler üzerine inşa edilen devletler üstü yapılarda da karşımıza çıkmaktadır. Özellikle pandemi dönemi sonrasında ABD ve pek çok Avrupa ülkesinde iktidara gelen sağ popülist partiler, yurttaş haklarını ve ekonomik özerkliği koruma retoriğiyle splinternet pratiklerini meşrulaştırma çabası içine girmektedir. Böylece otoriter rejimlerdeki internet parçalama uygulamalarının ulusal güvenlik mantığı, Batı demokrasilerinde yasadışı faaliyetlerle (terör, çocuk pornosu vb.) mücadele, mahremiyet, özgürlük ve etik bir teknoloji ilkelerine dayandırılarak haklılaştırılmaya çalışılmaktadır (Merrill ve Komaitis, 2020). Ağ parçalanması tiplerinden kısmî izolasyon çerçevesinde değerlendirilebilecek bu uygulamalar, paradoksal biçimde Avrupa Birliği'nde de görülmektedir. "Açıklık içinde kontrol" olarak nitelendirilebilecek, normatif bir dijital model yaratma çabası içinde olan Avrupa Birliği'nin interneti parçalamak gibi tanımlanmış bir hedefi olmasa da son yıllarda ileri sürdüğü "Avrupa dijital egemenliği" kavramı ve yürürlüğe koyduğu yasalar fiiliyatta bir bölünme dinamiği yaratmaktadır (European Commission, 2020; Mueller, 2020).

Tanımlamalardan hareketle, tıpkı fizikî sınırlar gibi dijital egemenlik sınırlarını belirleyen aslî aktörler devletler ve devletler üstü yapılar olsa da aslında splinternet olgusu, dünyanın neredeyse tamamında hâkim olan kapitalist sistemin mantığından bütünüyle ayrı bir düzlemde gelişmemektedir. Zira büyük verinin dijital plâtformlar tarafından anlık olarak toplanıp ekonomik değere dönüştürüldüğü bir çağda, altyapı gücünün kullanımı sadece devletlerin "bölgesel olarak belirlenmiş" fiziksel sınırlarıyla şekillenmemektedir. Dijital yığın, özel internet sermayesinin algoritmik süreçlerle oluşturduğu verileri eşzamanlı olarak biriktirip pazarlaması yoluyla gerçekleşmektedir (Kelton vd., 2022). Ancak bu makalede, konuyu sınırlandırmak adına splinternet'in ağırlıklı olarak siyasal boyutuna odaklanılmakta; başta teknoloji devleri olmak üzere şirketlerin ticarî çıkarları (ticarî splinternet), inceleme dışında tutulmaktadır.

Bu doğrultuda uygulayıcısı olan siyasal aktörler çerçevesinde incelendiğinde splinternet, aşağıdaki başlıklar altında ele alınmaktadır:

2.2. Ulusal Egemenlik Temelli Splinternet: Splinternet, internetin monolitik yapısını kırmakta; dijital alan devletlerin çıkarları doğrultusunda, genellikle ulusal sınırlar temelinde bölünmektedir (Hoffmann vd., 2020). Bugün artık devletler internetin işleyiş ve standartlarına giderek daha stratejik biçimde yaklaşmaktadır. Bu eğilim devletlerin siber egemenlik kapasitesini genişletirken kullanıcıların küresel dijital alana serbestçe erişimini zayıflatmaktadır. Devletlerin küreselden büyük oranda kopuk ve ulusal çerçevede yeniden yapılandırılmış parçalı dijital altyapılar inşa etmesi, vatandaşların internete erişim hakkını sınırlayarak onları sanal duvarlar içine hapsetmektedir (Perarnaud vd., 2022).

Buna göre örneğin Çin, Rusya, İran, Suudi Arabistan gibi devletler -farklı yoğunluklarda olmakla beraber- interneti ulusal güvenlik, resmî ideoloji, stratejik rekabet ve veri koruma gibi gerekçelerle ileri/yüksek veya kısmen kontrollü bir alana dönüştürme eğilimi gösteren devletler arasındadır (Freedom House, 2019). Bu çabalar, küresel dijital akışın ileri/yüksek düzeyde veya kısmen sınırlandırılması ve devletlerin ulusal dijital ekosistemlerini yönetme kapasitelerini güçlendirilmesi amacı doğrultusunda ortaya çıkmaktadır. Ulusal egemenlik temelli splinternet, yalnızca teknik altyapıyı denetim altına almayı değil; aynı zamanda içerik kontrolü, dijital güvenlik politikaları, veri saklama politikaları ve ticarî veri akışının yönetimini de kapsamaktadır. Sonuç olarak, uluslararası internet mimarisinde hem teknik hem de hukuksal boyutuyla yeni bir egemenlik ile segmentli bir düzenleme anlayışı yaratılmaktadır (Pohle ve Thiel, 2020).

2.3. Devletler üstü Regülasyon Temelli Splinternet:

Kimi devletlerin ileri/yüksek izolasyon uygulamalarının aksine, bir devletlerüstü yapı olarak Avrupa Birliği, dijital evreni katı bir biçimde izole etmeye yönelmemekte; fakat birtakım etik ve hukuki ilkeler üzerinden işleyen normatif bir siber egemenlik düzeni kurmayı tercih etmektedir. Birlik, önce 2018 yılında Genel Veri Koruma Tüzüğü (GDPR) ve 2022 yılında Dijital Hizmetler Yasası ile kapsamlı yasal standartlar belirlemiştir. Bu standartlar, kişisel verilerin korunması, dijital plâtformların sorumlulukları ve içerik denetimi gibi konuları kapsamaktadır. Böylece kullanıcı verilerinin büyük bir bölümünün izlenebilir hâle getirilmesinin önü açılmıştır (De Hert vd., 2018).

Son olarak 2024 yılında yürürlüğe giren Yapay Zekâ

Yasası (AI Act) ile ise algoritmik karar süreçlerinde insan kontrolünü esas alan gözetim temelli sistemlerin sınırlandırılması amaçlanmıştır (Floridi, 2023). Ancak bahsi geçen çok katmanlı regülasyon yapıları, her ne kadar teknik bakımdan açık bir çerçeve sunsa da fiiliyatta bölgesel standartlar oluşturarak normatif farklılaşmalar yaratmaktadır. Bu durum, internetin bütünlüklü doğasının kısmen de olsa parçalanmasına neden olmaktadır. Dolayısıyla bu yasalar, devletler üstü bir yapı olarak Avrupa Birliği'nin dijital egemenliğini pekiştirdiği ve internetin evrensel teknik altyapısını zayıflattığı gerekçesiyle eleştirilmektedir.

3. TEKNOLOJİ, SİYASET VE KONTROL: DEVLET VE DEVLETLER ÜSTÜ YAPI ÖRNEKLERİYLE SPLINTERNET PRATİKLERİ

Bugün dünya çapında her türden siyasal rejime sahip devlet, veri yerelleştirmesini zorunlu hâle getirmeye çalışmakta; bu verileri denetim altında tutmaya, çıkarları doğrultusunda içerikleri kısıtlamaya veya bazı plâtformları tamamen yasaklamaya yönelmektedir (Fick ve Miscik, 2022). Örneğin Çin, otuz yılı aşkın süredir sosyal, ekonomik ve siyasi yaşamın tüm alanlarında dijital teknolojilerin benimsenmesini ve yaygınlaşmasını desteklerken aynı zamanda dünyanın en gelişmiş sansür ve kontrol sistemlerinden birini kurmuştur. Bu sistem belirli anahtar kelimeleri tespit etmek için web (HTTP) trafiğini izlemekte; Çin hükümetinin resmî ideolojiye aykırı gördüğü siyasi görüşler, yasakladığı gruplar ve tartışılmasını istemediği tarihi olaylara ilişkin içerikleri filtrelemektedir (Clayton vd., 2006; Creemers, 2020). Çin Kamu Güvenliği Bakanlığı 1998'de ulusal çapta dijital bir kontrol ve gözetim mekanizması olan "Altın Kalkan Projesi"ni devreye sokmuştur. Günümüzde de devamlı genişletilerek uygulanmaya devam eden proje kapsamında 2009 yılında YouTube, Twitter, Facebook, Instagram gibi uluslararası çapta popüler olan sosyal medya plâtformları Komünist Parti'nin anlatısına karşıt olduğu gerekçesiyle yasaklanmıştır. Bunların yerine Youku, Baidu, QQ gibi yerli ağlar kurulmuştur (Washington Post, 2016). Çin'in dijital engelleri elbette sadece siyasi kontrol araçları olarak değil; aynı zamanda yerli işletmeleri koruyan ve uluslararası rakiplerinin etkinliğini zayıflatan ticarî bir strateji olarak da işlev görmektedir. Hükümet, yabancı sosyal medya ağlarını, arama motorlarını ve diğer pek çok internet hizmetini sınırlandırarak ya da engelleyerek yerli alternatiflerinin (Alibaba gibi) büyümesine zemin hazırlamaktadır. Ülkede ideolojik kontrol ile birlikte yerli bir dijital sanayiyi geliştirme stratejileri iç içe geçmiştir (Foote ve Atkinson, 2020).

Konunun ironik yönü, Çin'in önderlik ettiği siyasi ve ticarî dijital parçalama stratejilerine yönelik olarak verilen tepkilerin de benzer pratikler ile gerçekleşmesidir. Bu noktada ABD, 11 Eylül Saldırılarından beri sürdürdüğü "ulusal güvenlik" stratejisini dijital alana taşımış ve özellikle Trump Dönemi'nden itibaren Çin'e karşı hamlelerde bulunmaya başlamıştır. Ülkede ilk kez 2020 yılında kullanıcı verilerinin güvenliğinin sağlanmadığı gerekçesiyle gündeme gelen Çinli TikTok plâtformunu yasaklama girişimleri (her ne kadar ertelense de) güncelliğini korumaktadır (T24, 2025). ABD ile Çin arasındaki dijital hesaplaşmanın en görünür öznelerinden biri hâline gelen TikTok, şimdilik yalnızca hükümete ve askeriyeye ait birimlerde yasaklanmış olsa da İkinci Trump Hükümeti plâtformun ya yasaklanması ya da ABD'li bir şirkete satılması konusunda ısrarcı görünmektedir (BirGün, 2025).

Telekomünikasyon, fiber optik kablolar ve uydu ağlarından oluşan geniş bir matris olan internet, hâlihazırda büyük ölçüde ABD'nin bir eseri olarak ortaya çıkmıştır. İnternetin temelini oluşturan teknolojiler federal araştırma projeleriyle doğmuş ve Amerikan şirketleri bu teknolojiyi geliştirmiş, ticarileştirmiş ve küreselleştirmiştir. Başlangıçta ABD'nin stratejik, ekonomik ve dış politika çıkarları "evrensel ve açık bir ağ" ideali ile uyumlu iken bugün jeopolitik güç ve rekabetin aslî kaynaklarından biri hâline gelmiştir (Fick ve Miscik, 2022). Ancak bugün internet doğduğu topraklarda dahi eyaletler düzeyinde, başka bir deyişle giderek daha mikro ölçeklerde parçalanmaktadır. Buna göre Amerikan Anayasası'nın en temel maddelerinden biri olan "ifade özgürlüğü" hakkı, dijital plâtformlar düzeyinde gitgide daha tartışmalı hâle gelmektedir. Örneğin Teksas eyaleti, sosyal medya şirketlerinin kullanıcı içeriklerini kaldırma ve engelleme yetkilerinin sınırlandırılması gerektiğini savunan yasayı geçerli bulmuştur; devamında Florida eyaleti de benzer bir yasa çıkarmış olsa da ilgili yasa plâtformlara cezai yaptırım öngördüğü için mahkeme tarafından ifade özgürlüğüne aykırı bulunmuş ve askıya alınmıştır. İçerik denetimi ve ifade özgürlüğüne ilişkin mahkeme

kararlarının farklı oluşu, sosyal medya kontrolüne ilişkin hukukî mücadeleleri eyaletler düzeyinde dahi kızıştırmaktadır (The Economic Times, 2024). Özetle, internetin yapısına yönelik tartışmalar, ABD'nin kendi hukuk sistemi içinde ifade özgürlüğünün dahi sınırlarını yeniden tanımlamayı gerektirmektedir.

Dolayısıyla çevrim içi dünyayı kontrol altına almaya çalışan yegâne aktörler, demokrasi endekslerinde "otoriter" olarak sınıflandırılan rejimlere sahip devletler değildir. Örneğin, Almanya'da sosyal medya plâtformlarında dezenformasyon, nefret söylemi, şiddet içerikli paylaşımların artışıyla birlikte "NetzDG[7]" (Ağ Yürütme Yasası) çıkarılmıştır. İlgili yasa "açıkça suç teşkil eden" içeriklerin 24 saat hâlinde kaldırılmaması hâlinde 50 milyon avroya kadar para cezası uygulanmasını öngörmektedir (Fick ve Miscik, 2022). Esasen filtreleme ve sansür gibi splinternet pratikleri üzerine yapılan araştırmalar, tipik olarak otoriter rejimlere odaklansa da başta ifade özgürlüğü olmak üzere temel haklara uzun yıllardır bağlılık gösteren Batılı liberal demokrasiler de bu uygulamalara giderek daha sık başvurmaktadır. Bu durum, devletlerin yetkilerini anti-demokratik amaçlarla kullanma ihtimâlini ve filtrelemeleri düzenleme noktasında piyasa güçlerine güvenmelerinin meşruiyetini sorgulatmaktadır (Wright ve Breindl, 2013). Ayrıca Almanya, her ne kadar dış (devletler üstü) düzeyde Avrupa Birliği üyesi olarak, birliğin ortak siber regülasyon politikalarına tabi olsa da iç hukuk çerçevesinde NetzDG gibi yasalarla ulusal düzeyde kendi splinternet pratiklerini ortaya koymaktadır. Bu noktada Avrupa Birliği'nin siber alan düzenlemelerinin normatif bütünlük ve kullanıcı hakları odaklı biçimlendiği; Almanya'nın ise kamu düzeni ve güvenlik gibi gerekçelerle daha katı ve sınırlayıcı pratiklere başvurduğu gözlemlenmektedir (Gorwa, 2024). İlgili farklılık, birlik ile birliğe üye bir devletin siber egemenlik ve ifade özgürlüğü anlayışları arasındaki gerilimi yansıtmaktadır.

İnterneti kontrollü bir alana dönüştürme uygulamaları, yasalarla kalıcı hâle getirilebildiği gibi zaman zaman yavaşlatma ya da geçici olarak kapatma biçiminde de gerçekleşebilmektedir. Örneğin, 2015-2022 yılları arasında 60'tan fazla ülkenin interneti yüzden fazla kez kesintiye uğratılmıştır. Dünyanın en büyük nüfusunu barındıran Hindistan'da devlet, 2019 ve 2020 yıllarında interneti 13 bin saati aşkın bir süre boyunca askıya almıştır. Yine son birkaç yılda Etiyopya, Nijer, Nijerya ve Uganda da kimi zaman bilgi akışını kontrol etmek ve seçim sonuçlarını etkilemek için interneti geçici olarak kapatma yoluna gitmiştir (Fick ve Miscik, 2022). Bahsi geçen ülkeler Çin ve Rusya gibi ileri/yüksek izole bir internet kontrol sistemi ya da ulusal bir sosyal medya ekosistemine sahip değildir. Ancak kimi zaman erişim engellemeleri, veri yerelleştirme zorunlulukları ile regülasyon baskıları gibi yöntemlerle kısmî splinternet uygulamalarına yönelmektedir.

Benzer durum Türkiye için de geçerlidir. Freedom House'un 2024 yılı raporuna göre, mobil hızlardaki artışa rağmen sosyal medya paylaşımları nedeniyle verilen cezalar, erişim engelleri, içerik kaldırma emirleri ve dezenformasyon yasası gibi uygulamalar nedeniyle Türkiye, "internetin özgür olmadığı ülkeler" kategorisinde yer almaktadır. Çevrim içi kontrol ağları, hükümet yanlısı dezenformasyonu artırmakta; gazeteciler, sosyal medya kullanıcıları ve aktivistler paylaşımları nedeniyle suçlamalarla karşı karşıya kalmaktadır (Freedom House, 2024). Ayrıca son yıllarda Cumhurbaşkanı Erdoğan'a yakın isimler her ne kadar Batı'ya karşı rekabetçi ulusal sosyal medya plâtformlarının geliştirilmesi gerektiğini vurgulasa da ülkede henüz yabancı teknoloji devlerine alternatif oluşturabilecek ağlar kurulamamıştır (Krzyzanowska, 2025). Bu doğrultuda Türkiye, yarı kontrollü internet/kısmî splinternet pratikleri yürüten devletler arasında değerlendirilebilir.

İlgili ülke örnekleri beraber değerlendirildiğinde, splinternet pratiklerinin ulusal egemenlik temelli daha katı stratejiler ile devletler üstü regülasyon odaklı kısmî müdahaleler arasında farklı yoğunluklarda çeşitlendiği görülmektedir. Çin ve Rusya gibi ileri/yüksek izolasyon örnekleri, ulusal egemenliği siber alanda yeniden kuran kapsamlı filtreleme rejimleri ve katı ağ mimarileri üretirken; ABD, Almanya gibi devletler ve devletler üstü bir örgüt olarak Avrupa Birliği, içerik denetimi, güvenlik ve rekabet temelli müdahalelerle daha seçici bir izolasyon biçimi oluşturmaktadır. Türkiye, Hindistan ve Afrika'daki kimi ülkelerde görülen kesintiler, erişim engelleri

[7] NetzDG (Ağ Yürütme Yasası): Almanya'da 2017 yılında yürürlüğe giren ve iki milyonun üzerinde kayıtlı kullanıcısı bulunan sosyal ağ sağlayıcılarını kapsayan bir düzenlemedir. İlgili yasa, plâtformlara kullanıcı şikâyeti üzerine "açıkça suç teşkil eden" içerikleri 24 saat; suç niteliği tartışmalı olan içerikleri ise en fazla 7 gün içerisinde kaldırma ya da erişimi engelleme yükümlülüğü getirmiştir. Ayrıca sosyal ağ sağlayıcılarının temsilci ataması ve yılda iki defa şeffaflık raporu yayımlaması da zorunlu kılınmıştır (Ekici ve Erdem, 2024).

ve baskıcı düzenlemeler ise siyasi konjonktüre ve teknik kapasiteye bağlı olarak dalgalı bir izolasyona işaret etmektedir. Bu farklılaşmalar, splinternet'in rejim tiplerinin ötesinde, jeopolitik konum, kurumsal denetim kapasitesi ve siyasi kriz dönemlerinde benimsenen düzenleme anlayışlarına göre farklı ölçeklerde şekillenen çok boyutlu bir olgu niteliği taşıdığını göstermektedir (Nocetti, 2024).

4. SİBER EGEMENLİĞİN DIŞSALLAŞMASI: KÜRESEL GÜÇ MÜCADELELERİNDE CEPHELEŞEN DİJİTAL PLÂTFORMLAR

Dijital ağların sınırsızlığına karşın devletler ve devletler üstü örgütlerin siber egemenlik politikaları doğrultusunda örmeye çalıştığı sınırları ifade eden splinternet olgusu, 2020'li yıllardan itibaren hegemonik bir yapıya bürünerek aynı zamanda dışsal/uluslararası bir nitelik kazanmaya başlamıştır. Splinternet'in dışsallaşması, siber egemenliğin Westphalian egemenlik anlayışındaki içsel yetki alanından çıkarak uluslararası güç ilişkilerinin bir unsuru hâline gelmesini ifade etmektedir. Devletler kendi vatandaşlarının bilgi akışını yönetmekle kalmamakta; aynı zamanda düşman veya rakip devlet ve aktörlerin dijital görünürlüğünü, iletişim kapasitesini ve uluslararası meşruiyetini sınırlandırmaya veya biçimlendirmeye yönelmektedir (Pierucci, 2025). Bu noktada Rusya ile Ukrayna ve İsrail ile Filistin arasında yaşanan savaşlar, splinternet'in iç politikada bir egemenlik aracı olmanın ötesine geçerek devletler arasında bir çatışma ve güç projeksiyonu mekanizmasına dönüşebildiğini göstermektedir. Fidler'a göre (2025) bu yeni ve daha da genişleyen parçalanma biçimi, interneti devlet ya da devletler üstü yapı düzeyinde bir intranetten ziyade siber-Balkanlaştırılmış ağların sınır karakollarına dönüştürmektedir.

Rusya-Ukrayna Savaşı, dijital plâtformların devletlerarası askerî bir çatışma bağlamında, Schmittçi bir anlayışla "dost" ya da "düşman" olarak konumlandırıldığı ve plâtformların da buna göre belirgin bir şekilde taraf hâline geldiği ilk savaşlardan biri olarak tarihe geçmiştir. 2022 yılında başlayan savaş, devletlerarası siber sınırların jeopolitik bir araç olarak daha da belirginleşmesine yol açmıştır. Esasen Rusya'nın ülke sınırları dahilinde internet altyapısına yönelik müdahaleleri, bizzat Rus otoritesi tarafından "egemen internet" retoriği ile yasalaşan RuNet'in (Russian Internet) 2019'da yürürlüğe girmesiyle başlamıştır. İlgili yasa ile "dış tehditlere karşı" internet sağlayıcılarına ağ trafiğini izleme, filtreleme ve yeniden yönlendirme kapasitesine sahip özel ekipmanlar kurma zorunluluğu getirilmiştir. Böylece hükümet, interneti dijital içeriklerin doğrudan kontrol edilebildiği yarı kapalı bir sisteme dönüştürmüştür (Human Rights Watch, 2019; RAPSI News, 2019).

Ancak savaşla birlikte internet plâtformları adeta dijital askerî cepheler hâline gelmeye başlamıştır. Resmî olarak Rusya ile Ukrayna arasında gerçekleşse de ABD ve Avrupa Birliği ülkelerinin Ukrayna'ya verdiği dolaylı destek, savaşın çok daha geniş ölçekli bir karakter kazanmasına neden olmuştur. Rusya -Soğuk Savaş dönemine benzer şekilde-, "Batı Bloku"nun küresel çapta popüler ağları olan Facebook ve Instagram'ı (Meta) Ukrayna lehine bilgi yaymak ve Rus anlatısını sansürlemekle suçlamıştır. Bu plâtformları "aşırılıkçı örgüt" ilan etmiş ve mahkeme kararıyla ülke içindeki erişimlerini engellemiştir (Reuters, 2022). Ardından dijital izolasyon diğer Batı menşeli sosyal ağları da kapsayarak genişlemiş; sırasıyla Twitter, YouTube, WhatsApp ve Telegram gibi plâtformlara erişim kısıtlamaları getirilmiştir (Al Jazeera, 2025). Bu noktada Rusya'nın dijital egemenlik stratejisinin uzantısı olarak ilgili ağların yerli alternatiflerini (Facebook yerine VKontakte, YouTube yerine RuTube, WhatsApp ve Telegram yerine MAX gibi) geliştirme çabasının RuNet stratejisi olduğunu ve özellikle de Ukrayna Savaşı sonrası hız kazandığını belirtmek gerekmektedir (Bronnikova vd., 2024).

Rusya ve Ukrayna arasındaki savaş, internet altyapısının bir parçası olan deniz altı kablolarının da salt "teknik bir detay" olmanın ötesinde askerî açıdan daha kritik biçimde önem kazandığı bir sürecin kapılarını aralamıştır. İnternet trafiğinin %95'ini taşıyan; başka bir deyişle, küresel veri akışının bir nevi omurgası olan deniz altı kabloları, savaş durumlarında altyapıyı zayıflatmanın ve bu yolla süreci yönetmenin bir aracı olarak görülmektedir. NATO'nun siber uzmanları, Rusya'nın Baltık Denizi'nde deniz altı kablolarına sabotaj girişimlerinde bulunduğunu iddia etmiştir. İlgili girişim iddiaları kanıtlanamasa da bir ülkenin ya da bloğun düşmanca bir operasyonla deniz altı kablolarını hedef alması ihtimâli, savaşların internetin parçalanmasını daha da derinleştirme riskini ortaya çıkarmıştır (Eurasia Press & News, 2023).

Rusya'nın splinternet pratiklerine karşı Batı'nın dijital salvosu gecikmemiştir. Önce Avrupa Birliği'nde, ardından ABD, Kanada, İngiltere gibi diğer Batılı ülkelerde Facebook-Instagram (Meta), YouTube, X (Twitter) gibi plâtformlar, Rus devletine ait uluslararası yayın kuruluşları olan Russia Today ve Sputnik'e erişim engeli getirmiştir (Sputnik Africa, 2024). Ayrıca tıpkı deniz altı kabloları gibi internet altyapısının bir diğer kritik bileşeni olan uydu teknolojileri de bu savaş ile birlikte askerî açıdan stratejik bir öncelik kazanmıştır. İşgal ile birlikte Ukrayna'da iletişim altyapısının ciddi anlamda zarar görmesi üzerine, Amerikan şirketi Space X'e ait Starlink uydu internet sistemi kısa sürede kritik hâle gelmiş; şirket açtığı binlerce terminalle hem askerî alanda hükümete hem de sivil kullanıcılara destek vermeye başlamıştır (Al Jazeera, 2022). Bunun üzerine Rusya, Starlink'in açıkça "askerî bir hedef" olduğunu ilan etmiş; sinyallerini elektronik savaş yöntemleriyle bozmaya, devre dışı bırakmaya çalışmıştır. Ancak başarı elde edemeyince, 2024 yılı başlarından itibaren stratejisini değiştirerek özellikle cephe hattında ele geçirdiği terminalleri kendisi kullanmaya başlamıştır. Space X, her ne kadar sistemin Rusya'da hiçbir zaman aktif hâle getirilmediğinin altını çizse de terminallerin sahada Rusya tarafından da kullanılmasını engelleyememiştir (CNBC, 2024; Reuters, 2024). Bugün Rusya Starlink'i hem engellemeye çalışan hem de sınırlı ölçüde de olsa ondan yararlanmaya çalışan bir aktör hâline gelmiş durumdadır. Konuya splinternet açısından bakıldığında Starlink Olayı, internetin bir iletişim aracı olmasının ötesinde, özellikle savaşlarda jeopolitik aktörler arasında el değiştiren askerî bir güç unsuru hâline geldiğini göstermektedir. Bu durum, evrensel olması gereken internetin çatışma ve bölgesel bağlama dayalı kullanımını güçlendirmiş; bir başka deyişle, özgür erişim hakkı ülküsünü parçalayarak altyapısının kim tarafından kullanıldığı, kontrol edildiği ya da engellendiği belirsiz olan bir internet anlayışının yerleşmesine neden olmuştur.

Mücadelenin taraflar açısından çok daha asimetrik bir şekilde yürüdüğü İsrail-Filistin Savaşı'nda ise, savaş bölgesinden yayılan veriler ezici bir ağırlıkla İsrail'in hegemonyası doğrultusunda şekillenmektedir. Son dönemde her ne kadar İngiltere, Almanya, Fransa, İtalya ve İspanya gibi Batılı devletler dahi Gazze'ye yönelik askerî operasyonlar ve insanî yardımların engellenmesine açıkça tepki göstermiş olsa da İsrail'in güçlü bir askerî ve teknolojik altyapıya sahip oluşu, bölgedeki fiziksel kontrolünü pekiştirmesinin yanı sıra ona aynı zamanda bilgi akışı ve dijital gözetim konusunda kritik bir üstünlük kazandırmıştır. Nitekim uzmanlar da bu olguyu desteklemiş; sosyal medya ve diğer dijital plâtformların savaşın duyurulmasında önemli bir role sahip olduğunu, ancak algoritmaların Filistinli kullanıcılar tarafından gelen içerikleri ağır bir şekilde sansürlediğini belirtmiştir (Anadolu Ajansı, 2024).

İnsan Hakları İzleme Örgütü'nün yayımladığı rapora göre, 60'tan fazla ülkeden toplanan veriler doğrultusunda Facebook ve Instagram'da yayımlanan 1050 içerikten 1049'unun sansürlendiği tespit edilmiştir. Başta İngilizce olmak üzere çeşitli dillerde Filistin'e barışçıl desteğin ifade edildiği içerikler sansürlenmiştir. Bu sansürleme gönderilerin ve yorumların kaldırılması, hesapların askıya alınması veya kalıcı olarak devre dışı bırakılması, hesapları takip etme ya da etiketleme becerisine ilişkin kısıtlamaları kapsamaktadır. Başka bir deyişle, kullanıcıların farkında olmadan paylaşımlarının görünürlüğünün sınırlandırılması biçiminde gerçekleşen bu shadowbanning pratikleri, Meta bünyesinde yer alan bu plâtformların evrensel ifade özgürlüğü ve internete erişim haklarına aykırı hareket ettiğini kanıtlamaktadır (Human Rights Watch, 2023). X (Twitter), savaşın başlamasından kısa bir süre sonra yaptığı açıklamada, kullanıcıların anti-semitik söylemlerine karşı müdahale noktasında "proaktif" bir politika izlediğini belirtse de aynı hassasiyetin Filistinlilere gösterilmesi konusunda üç maymunu oynamaktadır. Şirketin o dönemki CEO'su Yaccarino, Hamas'la bağlantılı olduğu iddia edilen yüzlerce hesabın kapatıldığını belirtmiştir. Buna karşılık İsrailli yetkililerden gelen ve çoğu zaman dezenformasyonun da eşlik ettiği nefret ve şiddet söylemlerine yönelik hiçbir engellemeye başvurulmamıştır (El Pais, 2023). Arap Sosyal Medya Geliştirme Merkezi (7amleh), 2024 yılında yayımladığı rapor ile YouTube'un Filistinlilere karşı nefret ve şiddeti teşvik eden reklam materyallerinin yayımlanmasına olanak sağladığını saptamıştır. 2013 yılında Filistinlilerin dijital alandaki haklarını koruma ve seslerini duyurmalarına yardımcı olma amacıyla kurulan merkez, plâtformun İsrail'in Gazze'deki eylemlerini eleştiren içerikleri ise kısıtlama yoluna gittiğini ve Filistinlilerin savaş koşullarındaki yaşamları hakkında bilgi paylaşımlarını engellediğini ortaya çıkarmıştır (Bianet, 2024; 7amleh, 2024).

Meseleye bütünlüklü biçimde bakıldığında, savaşlarla birlikte teknolojik bölünmenin derinleştiği; verinin jeopolitik ve stratejik niteliğinin ağırlık kazandığı bir döneme geçilmiştir. Her iki savaş da pandemi sonrası dijital bloklaşmanın katalizörü hâline gelmiş; artık bir olayın gerçekte ne olduğundan ziyade hangi dijital evrende ne kadarının nasıl görüldüğü belirleyici olmaya başlamıştır. Ulusal sınırlar ile uluslararası bloklaşmalar siber alanda daha da keskinleşmiş; devletler/bloklar kendi gerçeklik anlatılarını, siyasi çıkarları doğrultusunda, inşa ettikleri bilgi filtreleri üzerinden şekillendirmeye yönelmiştir. Böylece internet, güvenlik odaklı ve savunmacı bir siyaset anlayışının kuşatması altında, veri akışı ve erişimin parçalandığı, yeniden yapılandırıldığı ve kontrol edildiği bir alana dönüşmüştür.

Savaşlarla birlikte splinternet, devletlerin yalnızca ulusal politikalarında uyguladıkları siber egemenlik stratejilerini yansıtan bir olgu olmaktan çıkmış; giderek devletler arası ölçekte dışsallaşan ve hegemonik nitelik kazanan bir güç aracına dönüşmüştür. Bu savaşlar, siber alanın artık ülkeler arası rekabetin bir uzantısı olarak işlediğini ve ağların bir iletişim ortamı olmaktan uzaklaşarak jeopolitik bir çekişme alanına dönüştüğünü göstermektedir (Fidler, 2025). Rusya ile Ukrayna arasındaki savaşta dijital plâtformlar, taraflar arasındaki askerî ve bilgi savaşlarının bir uzantısı hâline gelmiş; Rusya ile Batı devletleri arasındaki siber bloklaşmalar, internetin jeopolitik bir silah olarak kullanılmasına neden olmuştur. Benzer şekilde, İsrail ile Filistin çatışmasında ise, başta sosyal medya ağları olmak üzere dijital altyapı üzerindeki kontrol, bölgedeki asimetrik güç ilişkilerini pekiştirmiş; plâtformlar birer hegemonik araca dönüştürülmüştür. Böylece her iki savaş da splinternet olgusunun ulusal sınırları aşan, bir başka deyişle dışsallaşmış bir nitelik kazandığını ortaya koymaktadır (Nocetti, 2024). Gerbaudo'nun (2022) "yeni devletçilik" kavramsallaştırmasıyla da örtüşen bu eğilim, devletlerin siber altyapılar üzerindeki kontrolünü merkezî hâle getirerek bilgi üretimi, erişim ve dolaşımı doğrudan ulusal çıkarları doğrultusunda yönetme arzusunu yansıtmaktadır. Bu doğrultuda splinternet olgusu, ulusal/içsel bir ağ parçalanmasının ötesinde, devletler arası ölçekte güç projeksiyonu ve siber hegemonyanın yeniden üretildiği bir mekanizma hâline getirilmiştir. Küresel internet ideali ise, artık farklı aktörlerin kendi çıkarları doğrultusunda dijital gerçekliklerini dikte ettiği, parçalı ve hiyerarşik bir dijital düzenin gölgesinde varlığını sürdürmektedir.

SONUÇ

Bu çalışma, internetin küreselleşmenin özgürlükçü ideallerine dayalı bir iletişim alanı olarak tasarlanmasından günümüzde devletlerin siyasi, stratejik ve teknolojik çıkarları doğrultusunda parçalı bir yapıya dönüşümünü ele almayı amaçlamıştır. İnternet 1990'lı yıllarda bilgiye serbest erişim ve etkileşimin esas alındığı evrensel bir mecra olarak düşünülmüş olsa da günümüzde giderek bu ideallerin oldukça uzağına savrulan bir niteliğe bürünmektedir. Dünyada özellikle COVID-19 pandemisi sonrası hız kazanan dijital dönüşümle birlikte, devletler ve devletler üstü yapılar teknik ve politik düzlemde siber alan üzerindeki denetim kapasitelerini artırmıştır. Bu süreç internetin evrensel ve müştereklere dayalı bir alan olma idealini zedelemiş ve yerini, ulusal çıkarlar doğrultusunda parçalı ve panoptik mekanizmalarla kuşatılmış bir internet mimarisine bırakmıştır. Çalışmanın bulguları da bu eğilimi doğrulamaktadır: Ulusal güvenlik odaklı düzenleyici müdahalelerle dijital alanın giderek merkezîleşmesi ve plâtformların uluslararası düzlemde taraf konumuna itilmesi, internetin çok katmanlı bir egemenlik alanına dönüşmeye başladığını göstermektedir. Bu yönelim ise, evrensel bir ağ olan internetin siber egemenliğin bir uzantısına dönüşmesine işaret eden splinternet olgusunu gündeme taşımaktadır.

Son yıllarda sağ kanat popülist partilerin dünya çapında yükselişi, neoliberal küreselleşmenin gerileme eğilimine girmesine neden olmuş; Gerbaudo'nun "yeni devletçilik" olarak ele aldığı kavramsallaştırma çerçevesinde devletler, yerlilik, kültürel bütünlük, ulusal güvenlik gibi katı saiklerle daha içe kapalı ve denetleyici bir karakter kazanmıştır. Buna göre devletler, dijital uzamı artık yalnızca evrensel bilgi ve sermaye dolaşımı için değil; aynı zamanda ulusal, kültürel ve gerektiğinde askerî gücün sürdürülebilirliğini güvenceye alan jeopolitik ve stratejik bir iktidar sahası olarak kullanmaya başlamıştır. Devletler, geleneksel düzenleme yetkilerinin ötesine geçerek veri dolaşımından algoritmik görünürlüklere, altyapı standartlarından plâtform bazlı yasalara kadar uzanan geniş bir çerçevede belirleyici bir aktör hâline gelmiştir. Bu durum, hem teknik anlamda internetin

altyapısını parçalamış hem de internete erişim hakkını zayıflatarak kullanıcıların içerik deneyimlerinin farklılaşmasına neden olmuştur.

Özellikle pandemi sonrası "halk sağlığı" retoriği ile meşrulaştırılmaya çalışılan denetleme ve gözetim pratikleri, sağ popülizmin küresel çapta ivme kazanmasıyla derinleşmiş; devletler vatandaşlarını üzerinde siber egemenlik kurdukları izlenebilir bir veri üreticisi olarak konumlandırmaya başlamıştır. İnternetin siyasal iktidar ilişkilerine giderek daha fazla tabi hâle gelmesi, onu sınırları ulus devletler tarafından belirlenen parçalı ve çok katmanlı bir sisteme dönüştürmektedir. Buna göre Çin ve Rusya ileri/yüksek izolasyona ve alternatif ulusal dijital plâtformlar geliştirmeye dayalı ağ parçalama pratiklerine başvururken ABD, Almanya, Hindistan, Türkiye, Nijerya gibi devletler kısmî izolasyona ve plâtform denetimine dayalı politikaları tercih etmektedir. Devletler üstü bir yapı olarak Avrupa Birliği ise, son yıllarda uygulamaya koyduğu dijital düzenleme yasalarıyla kısmî izolasyon pratiklerine normatif bir kimlik kazandırma çabası içine girmiştir. Bu durum, ağ parçalanması farklılaşmalarını yansıtmasının yanında aynı zamanda Batılı ve özgürlükçü, özetle liberal değerleri idealize eden devletler ve devletler üstü rejimlerin de splinternet olgusuna başvurduğunu göstermektedir. Ayrıca ülke örneklerinde gözlemlenen katı, seçici ve dalgalı izolasyon biçimleri, splinternet'in farklı politik rejimlerde farklı yoğunluklarda işleyen bir yönelime sahip olduğunu ortaya koymaktadır. Ulusal egemenlik temelli daha kapalı modeller ile devletler üstü regülasyon odaklı kısmî müdahalelerin aynı anda varlık göstermesi, siber alanın giderek çok ölçekli bir egemenlik yapısına büründüğüne işaret etmektedir. Bu bağlamda splinternet olgusu, teknik ayrışmaların yanı sıra devletlerin ve devletler üstü yapıların demokratik nitelikleri, jeopolitik konumları, kurumsal kapasiteleri ve çalkantılı dönemlerde izledikleri siyasal stratejilerin de belirleyici olduğu karmaşık bir dijital düzen tartışması hâline gelmiştir.

Literatürde devletler ve devletler üstü yapılar, ağ parçalanmasının aslî sorumluları olarak anılsa da son yıllarda yaşanan savaşlar artık uluslararası şirketlerin de bu olguda giderek taraf hâline geldiğine işaret etmektedir. Buna göre, Rusya-Ukrayna ve İsrail-Filistin savaşları, başta sosyal medya plâtformları olmak üzere dijital ağların Schmittçi bir anlayışla "dost" veya "düşman" ekseninde konumlandırıldığını ve hatta -Starlink örneğinde olduğu gibi- çatışmaların bir nevi aktörü hâline getirildiğini göstermektedir. Bu savaşlar aynı zamanda splinternet olgusunun dışsallaşarak hegemonik bir yapıya büründüğünü; siber egemenliğin ulusal sınırların ötesine taşınarak tarafların veri akışı, söylemleri, erişim kısıtları ve algoritmik manipülasyonları doğrultusunda yeniden inşa edildiğini ortaya koymaktadır. Böylece dijital alan, artık savaşların yalnızca temsil edildiği değil; aynı zamanda küresel hegemonya mücadelesinin yürütüldüğü askerî bir güç uzamı hâline gelmiştir.

Bu çalışmada ele alınan splinternet olgusu, dijital çağın yeni siyasal jeopolitiği ve stratejilerini anlamada merkezî kavramlardan biri konumundadır. Bugün artık internet, küresel bir kamusal alan hâline getirilme idealinden giderek uzaklaşmakta; başta ulus devletler ve devletler üstü yapılar olmak üzere siyasal aktörlerin -ayrıca uluslararası şirketler gibi giderek siyasallaşan aktörlerin- siber egemenlik çıkarları doğrultusunda parçalı ve çok katmanlı bir yapıya bürünmektedir. Bu yönüyle çalışma, splinternet tartışmasını teknik düzenlemeler ya da altyapı kırılmaları çerçevesinden çıkarıp doğrudan siber egemenlik, jeopolitik ve küresel güç rekabeti perspektifinden ele almasıyla Türkçe literatüre mütevazı bir katkı sunmayı amaçlamaktadır. Özellikle pandemi sonrası devletler, ulusal güvenlik gerekçesini araçsallaştırarak veri akışını, görünürlüğü ve genel çerçevede internete erişim hakkını yeniden tanımlamakta; şirketler ise altyapı tekelleri aracılığıyla devletlerarası politikalarda taraf olmaya itilmektedir. Bu nedenle, plâtform sorumluluğu, algoritmik şeffaflık ve veri taşınabilirliğine yönelik bağlayıcı uluslararası normların oluşturulması acil bir gereklilik hâline gelmiştir.

Splinternet'in derinleşmesi, basitçe bir teknik kırılmanın ötesinde, internete erişim hakkının coğrafî, sınıfsal ve kültürel sınırlar çerçevesinde yeniden tanımlanması anlamına gelmekte; bu durum da dijital müşterekleri koruma çabasının mücadelesini evrensel bir zemine taşımaktadır. Bu tehdidi sınırlandırmanın yolu, uluslararası yönetişim mekanizmalarını güçlendirmekten geçmekte; siber alanın ve dijital hakların küresel bir çerçeveyle güvence altına alınması gerekmektedir. Zira gerçek anlamda demokratik bir dijital geleceğin inşası, teknolojik gelişmelerin hızıyla değil; ancak bu ilerlemelerin özgürlükçü

ve eşitlikçi ilkelerle uyum içinde sürdürülmesiyle mümkün olacaktır. Bu çalışma, splinternet olgusunu giriş mahiyetinde ele almaktadır. Bu bağlamda ileride yapılacak araştırmalarda, farklı ülkelerdeki internet politikalarının karşılaştırılmalı olarak analiz edilmesi, veri erişimi ve sansür mekanizmalarının ortaya konulması önerilmektedir. Ayrıca kullanıcıların internete erişim hakkı, çevrim içi katılım ve bilgiye erişim deneyimlerini merkeze alan saha araştırmalarının yapılması da splinternet olgusunun gündelik yaşam üzerindeki somut etkilerinin daha yakından tespit edilmesi açısından kritik bir öneme sahiptir.

KAYNAKÇA

Ananthaswamy, A. (2011). *Age of the splinternet. New Scientist, 211* (2821), 42-45.

Baltra, G. & Heidemann, J. (2021). *What is the internet? (Considering partial connectivity)* [Technical Report] USC/Information Sciences Institute.

Baritci, Z. F. (2024). Avrupa'da aşırı sağ politikaların yükselişi ve göçmen sorununun Avrupa medyasına yansıması. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 2024 (54),* 193-212.

Bronnikova, O., Dauce, F., Ermoshina, K., Kossov, V., Loveluck, B., Musiani, F., Ostromooukhova, B., Poupin, P., & Zaytseva, A. (2024). Circumventing the "sovereignization" of the Russian Internet: Toward an infrastructure-based sociology of digital sovereignty and its resistances in Russia. In M. Jiang & L. Belli (Eds.), *Digital sovereignty in the BRICS countries: How the global south and emerging power alliances are reshaping digital governance* (pp. 167-189). Cambridge University Press.

Castells, M. (2016). *İletişim gücü* (E. Kılıç, Çev.). İstanbul Bilgi Üniversitesi Yayınları.

Clayton, R., Murdoch, S. J., ve Watson, R. N. M. (2006). Ignoring the Great Firewall of China. In *PET 2006: Proceedings of the 6th International Workshop on Privacy Enhancing Technologies* (pp. 20-35). Robinson College.

Creemers, R. (2020). *China's approach to cyber sovereignty.* Konrad-Adenauer-Stiftung.

Çetin, M. (2020). Popülizm ve salgınla ulus devlete geçiş, gıda tedarik zinciri ile birliğe dönüş. *EURO Politika, 4* (2), 163-186.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L. ve Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review, 34* (2), 193-203.

Deibert, R. (2013). *Black code: Inside the battle for cyberspace.* Signal/McClelland & Stewart.

Demir, B. N. (2025). İnternet özgürlüğü ve erişim engelleme: İfade özgürlüğü bağlamında bir değerlendirme. *Bilişim Hukuku Dergisi, 7* (1), 364-423.

Ekici, M. ve Erdem, D. Ö. (2024). Sosyal medya kullanıcılarının "yalan haber" nedeniyle Alman Ceza Kanunu (STGB) kapsamında sorumluluğu. *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi, 6* (1), 706-746.

Fick, N. ve Miscik, J. (2022). *Confronting reality in cyberspace: Foreign policy for a fragmented internet.* (Independent Task Force Report No. 80). The Council On Foreign Relations (CFR).

Fidler, M. J. R. (2025). *Internet fragmentation's outward turn.* (Research Paper No. 4-31). Sciences Po-C-hair Digital, Governance & Sovereignty.

Floridi, L. (2023). On the Brussels-Washington consensus about the legal definition of artificial intelligence, *Philosophy & Technology, 36* (4), 1-9.

Foote, C. ve Atkinson, R. D. (2020, November 23). *Chinese competitiveness in the international digital economy.* Information Technology & Innovation Foundation.

Gerbaudo, P. (2022). *Büyük geri tepme: Popülizm ve pandemi sonrası politika* (K. Tanrıyar, Çev.). Ayrıntı Yayınları.

Gorwa, R. (2024). *The politics of platform regulation: How governments shape online content moderation.* Oxford University Press.

Hoffman, S., Lazanski, D. ve Taylor, E. (2020). Standardising the splinternet: How China's technical standards could fragment the internet. *Journal Of Cyber Policy, 5* (2), 239-264.

İyiekici, B. (2024). Sağ popülizmin COVID-19 krizindeki yansımaları: Trump ve Bolsonaro'nun yaklaşımlarının analizi. *Mülkiye Dergisi, 48* (4), 920-952.

Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E. ve Troath, S. (2022). Virtual sovereignty? Private internet capital. *International Affairs, 98* (6), 1977-1999.

Krzyzanowska, Z. (2025, June 24). *Discipline and punish: How Turkey controls the internet* (OSW Commentary No. 562). OSW-Centre for Eastern Studies.

Litvinenko, A. (2021). Re-defining borders online: Russia's strategic narrrative on internet sovereignty. *Media And Communication, 9* (4), 5-15.

Mhalla, A. (2023, January 17). *Splinternet: How geopolitics is fracturing cyberspace.* Polytechnique Insights.

Merrill, N. ve Komaitis, K. (2020, December 17). *The consequences of a fragmenting, less global internet.* Brookings Institution.

Morozov, E. (2019). *Twitter'dan sonra bir tarih kaldı mı?: Sanal ağ yanılsaması* (M. Tekin, Çev.). Açılım Kitap.

Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review, 22* (4), 779-801.

Nocetti, J. (2024). *A splintered internet? Internet fragmentation and the strategies of China, Russia, India and the European Union.* (Ifri Working Paper, 1-33). The French Institute Of International Relations (Ifri).

Perarnaud, C., Rossi, J., Musiani, F. ve Castex, L. (2022). *'Splinternets': Addressing the renewed debate on internet fragmentation.* (STOA Study EPRS-STU(2022)729530). European Parliament.

Pierucci, F. (2025). Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace. *Digital Society, 4* (Article 27), 1-19.

Pohle, J. ve Thiel T. (2020). Digital sovereignty. *Internet Policy Review, 9 (4)*, 1-19.

Racine, E. (2023). The far-reaching implications of China's AI-powered surveillance state post-COVID. *Surveillance & Society, 21* (3), 269-275.

Schmitt, C. (2012). *Siyasal kavramı.* (E. Göztepe, Çev.). Metis Yayınları.

Tai, K., Zhu, Y. Y. (2022). A historical explanation of Chinese cybersovereignty. *International Relations Of The Asia-Pacific, 22* (3), 469-499.

Türk, M. (2024). Anadolu'da Roma egemenliğine karşı ilk büyük tepki: Aristonikos isyanı. *Birey ve Toplum Sosyal Bilimler Dergisi, 14* (2), 83-96.

Wright, J. ve Breindl Y. (2013). Internet filtering trends in liberal democracies: French and German regulatory debates. *Internet Policy Review, 2* (2), 1-10.

İNTERNET KAYNAKLARI

Akçay, Ü. (2025). Neoliberalizmin sonu mu? Parçalı ve çelişkili değişimler ve süreklilikler. https://www.ayrim.org/dosya/neoliberalizmin-sonu-mu-parcali-ve-celiskili-degisimler-ve-sureklilikler/

Al Jazeera (2025). Russia calls on WhatsApp, Telegram as internet control tightens. https://www.aljazeera.com/news/2025/14/russia-restricts-calls-on-whatsapp-telegram-as-internet-control-tightens

Al Jazeera (2022). Elon Musk says Starlink internet service 'active' in Ukraine. https://www.aljazeera.com/news/2022/2/27/elon-musk-starlink-internet-service-ukraine-russian-invasion?utm

Anadolu Ajansı (2024). Social media platforms face accusation of censoring Gaza content. https://www.aa.com.tr/en/middle-east/social-media-platforms-face-accusation-of-censoring-gaza-content/3351704

Bianet (2024). Jalal Abukhater: Filistinlilerin sesini duyurmak ve korumak gerekiyor. https://bianet.org/haber/jalal-abukhater-filistinlilerin-sesini-duyurmak-ve-korumak-gerekiyor-300870

BirGün (2025). Trump'tan yeni adım: TikTok'un satışı için süre uzayabilir. https://www.birgun.net/haber/trumptan-yeni-adim-tiktokun-satisi-icin-sure-uzayabilir-653762

Britannica (2025). National Security Agency. https://www.britannica.com/topic/National-Security-Agency

CNBC (2024). Musk denies selling Starlink terminals to Russia after Kyiv alleges their use in occupied areas. https://www.cnbc.com/2024/02/12/musk-denies-selling-starlink-terminals-to-russia-after-kyiv-alleges-use.html

El Pais (2023). Censorship of pro-Palestinian voices on social media soars amid war in Gaza. https://english.elpais.com/international/2023-12-27/censorship-of-pro-palestinian-voices-on-social-media-soars-amid-war-in-gaza.html

Eurasia (2023). Defending submarine cables in the Black Sea: A challenge for NATO and the region. https://eurasia.ro/2023/03/04/defending-submarine-cables-in-the-black-sea-a-challenge-for-nato-and-the-region/

European Commission (2020). *Shaping Europe's digital future.* https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf

Freedom House (2024). Freedom on the net 2024: Turkey country report. https://freedomhouse.org/country/turkey/freedom-net/2024

Freedom House (2019). Freedom on the net 2019: The crisis of social media. https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf

Human Rights Watch (2023). Meta: Systemic censorship of Palestine content: Overhaul flawed policies; improve transparency. https://www.hrw.org/news/2023/12/20/meta-systemic-censorship-palestine-content

Human Rights Watch (2019). Russia: New law expands government control online. https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online

IMF (2021). *World economic outlook October 2021.* https://www.imf.org/en/Publications/WEO/Issues/2021/10/12/world-economic-outlook-october-2021

OECD (2021). *OECD employment outlook 2021.* https://www.oecd.org/en/publications/oecd-employment-outlook-2021_5a700c4b-en/full-report.html

RAPSI News (2019). Sovereign internet law protects from external threats-Putin. https://rapsinews.com/legislation_news/20191219/305235697.html

Reuters (2024). Ukraine seeking action to stop Russian use of Starlink, minister says. https://www.reuters.com/world/europe/ukraine-seeking-action-stop-russian-use-starlink-minister-says-2024-02-19/

Reuters (2022). Russian court bans Facebook, Instagram after Meta found 'extremist'-TASS. https://www.reuters.com/world/europe/russian-court-bans-facebook-instagram-after-meta-found-extremist-tass-2022-03-21/

Sputnik Africa (2024). Musk says social media platform X experiences little influence activity from Russia. https://en.sputniknews.africa/20240409/musk-says-social-media-platform-x-experiences-little-influence-activity-from-russia-1065988520.html

The Economic Times (2024). US supreme court sidesteps dispute on state laws regulating social media. https://economictimes.indiatimes.com/tech/technology/us-supreme-court-sidesteps-dispute-on-state-laws-regulating-social media/articleshow/111428138.cms?from=mdr

T24 (2025). ABD, TikTok yasağı başlangıcını erteledi. https://t24.com.tr/abd-tiktok-yasagi-baslangicini-erteledi/

World Internet Conference (2024, January 16). *Sovereignty in cyberspace: Theory and practice (Version 4.0).* https://www.wicinternet.org/2024-01/16/c_956165.htm

7amleh (2025). YouTube's impact on Palestinian digital rights during the war on Gaza. https://7amleh.org/post/youtube-s-impact-on-palestinian-digital-rights-during-the-war-on-gaza