Coğrafi Bilimler Dergisi / Turkish Journal of Geographical Sciences
2026; 24(1): 340-356 DOI: 10.33688/aucbd.1788517
Araştırma Makalesi / Research Article

# Siber mekânın siyasi coğrafyası: Şifreleme, gözetim ve küresel güç ilişkileri

## *The political geography of cyberspace: Encryption, surveillance, and global power relations*

**Semih Nargül**[*a]

[a] Van Yüzüncü Yıl Üniversitesi, Coğrafya Bölümü, Van/Türkiye

### *Öz*

*Dijital çağ, siyasi coğrafyanın sınırlarını kökten dönüştürmektedir. Bu çalışma, siber mekânın klasik devlet-merkezli düzeni nasıl aşındırdığını ve yeniden kurduğunu üç boyut üzerinden incelemektedir: şifreleme, gözetim ve yeni aktörler. Şifreleme teknolojileri bireylere ulusal sınırların ötesinde ifade ve örgütlenme özgürlüğü tanırken, aynı zamanda suç ve terör ağlarına da alan açmaktadır. Dijital panoptikon çerçevesinde ele alınan gözetim teknolojileri, devletlerin egemenlik kapasitesini toprak sınırlarının ötesine taşıyarak mahremiyet, güvenlik ve kamusal alanı yeniden tanımlamaktadır. WikiLeaks, Anonymous ve Snowden örnekleri ise bireylerin ve ağ tabanlı kolektiflerin uluslararası siyasette yeni güç biçimleri ürettiğini göstermektedir. Bulgular, siber mekânın özgürleşme ile denetim, birey ile devlet, sınır ile ağ arasındaki gerilimde şekillenen çok aktörlü ve veri temelli bir siyasi coğrafya yarattığını ortaya koymaktadır.*

***Anahtar Kelimeler:*** *Siber mekan, Siyasi coğrafya, Şifreleme, Gözetim, Yeni aktörler*

### *Abstract*

*The digital age is fundamentally transforming the boundaries of political geography. This study examines how cyberspace erodes and reconfigures the classical state-centered order through three dimensions: encryption, surveillance, and new actors. While encryption technologies grant individuals freedom of expression and organization beyond national borders, they also provide a space for criminal and terrorist networks. Surveillance technologies, examined within the framework of the digital panopticon, extend the sovereignty of states beyond territorial borders, redefining privacy, security, and the public sphere. Examples such as WikiLeaks, Anonymous, and Snowden demonstrate that individuals and network-based collectives are producing new forms of power in international politics. The findings reveal that cyberspace creates a multi-actor, data-driven political geography shaped by tensions between liberation and control, the individual and the state, and borders and networks.*

***Keywords:*** *Cyberspace, Political geography, Encryption, Surveillance, New actors*

***Sorumlu Yazar/Corresponding Author:** semihnargul@yyu.edu.tr
**Geliş/Received:** 21.09.2025 **Kabul/Accepted:** 10.04.2026 **Yayın Tarihi/Online Published**: 23.04.2026
**Atıf/To Cite:** Nargül S. (2026). Siber mekânın siyasi coğrafyası: Şifreleme, gözetim ve küresel güç ilişkileri, *Coğrafi Bilimler Dergisi/ Turkish Journal of Geographical Sciences,* 24(1), 340-356, https://doi.org/10.33688/aucbd.1788517

# EXTENDED ABSTRACT

## 1. Introduction

The foundations of modern political geography are deeply rooted in a state-centered order where sovereignty is defined by exclusive control over a specific territory. This Westphalian model, particularly solidified after World War I and institutionalized in the United Nations Charter, links the exercise of rights and authority directly to physical borders and state jurisdiction. In this classical arrangement, the individual is a passive carrier of rights, and their political existence is constrained by the spatial limits of the nation-state. However, the advent of the 21st century and the rise of cyberspace have precipitated a radical transformation in this established understanding, introducing an ontological tension between the static, territorial logic of the state and the fluid, borderless nature of digital networks.

This study defines the scope of this transformation by analyzing how cyberspace erodes and simultaneously reconfigures the classical state-centered order. The problem identified is that the "territorial trap" of traditional international relations is insufficient to explain a world where individuals can exercise political agency globally without physical movement. As Habermas (2001, s. 114), the presence of individuals on a specific piece of land is no longer the sole determinant for their recognition as political actors. Furthermore, Castells (2010) argues that digital networks replace the static logic of places with a dynamic logic of flows, rendering physical distance increasingly irrelevant. This creates a "deterritorialized" space, as described by Deleuze and Guattari (2015), where sovereignty and identity are constantly renegotiated.

The objective of this paper is to map this rupture in international political geography through three critical dimensions: encryption, surveillance, and new actors. It explores how encryption technologies provide individuals with autonomy from state law, how states respond through digital surveillance to extend their sovereignty beyond their physical borders, and how new non-state actors—from hacktivists to tech giants—challenge the state's monopoly on power. By integrating these theoretical perspectives, the study provides a comprehensive overview of the transition from a land-based political geography to a multi-actor, data-driven geopolitical reality.

## 2. Methodology

Given the complex and rapidly evolving nature of the subject matter, this study employs a qualitative conceptual analysis rooted in the discipline of critical geopolitics. Rather than relying on quantitative metrics, which often fail to capture the shifting ontological status of sovereignty and power, the research utilizes a theoretical framework that examines the "mutual permeability of power" between the physical and digital realms. This approach allows for the dissection of power relations that are no longer hierarchical but networked and fluid.

The analytical framework is structured around a tripartite typology:

Encryption: Analyzing the technological redistribution of power from the state to the individual.

Surveillance: Analyzing the state's strategic adaptation to reassert control via data.

New Actors: Analyzing the emergence of hybrid and non-state entities as geopolitical players.

To operationalize this framework, the study employs a case-study method, drawing on significant empirical events that have shaped the contemporary digital landscape. These cases are not

merely illustrative but are treated as critical junctures that reveal the underlying shifts in political geography. Specific examples include Edward Snowden's revelations about the PRISM program, the diplomatic disruptions caused by WikiLeaks, the rise of the hacktivist collective Anonymous, and the kinetic cyber-physical attacks such as Stuxnet and the 2024 Lebanon pager explosions. By interrogating these specific instances, the methodology demonstrates that it is the most effective means of understanding how the "inside/outside" distinction of classical international relations is being dissolved and how sovereignty is being exercised in the absence of territorial control.

## 3. Results

The investigation into the three dimensions of cyber-political geography yields the following results:

Encryption Findings: The study finds that encryption technologies have fundamentally altered the balance of power between the individual and the state. Historically, states maintained a monopoly on secure communication (cryptography), but the democratization of these tools—what Greenberg (2012) describes as part of a "Cambrian explosion" of privacy tools—has granted individuals a form of "transnational identity". As DeNardis (2014) highlights, encryption has become a mandatory infrastructure for modern life. The result is the creation of an autonomous zone in which individuals can exercise freedom of expression and association beyond the reach of local laws; this concept was championed by the Cypherpunk movement. However, the findings also highlight a dual-use paradox: while encryption empowers dissidents and protects privacy (e.g., during social movements, as noted by Fielder (2013) and Castells (2007), it simultaneously provides a "shield" and operational space for criminal networks and terrorist organizations. The study identifies that groups such as DAESH have used encrypted applications, such as Telegram to manage operations remotely; this is exemplified by the 2024 Crocus City Hall attack, in which perpetrators received instructions and payments via digital channels without physical contact with leadership. Thus, encryption does not merely hide data; it creates a "quasi-state" function for non-state actors.

Surveillance Findings: The results demonstrate that states have responded to the loss of territorial control by expanding their borders through data surveillance. The analysis of the Snowden documents reveals that the US National Security Agency (NSA) and its "Five Eyes" partners have constructed a global surveillance architecture that bypasses territorial sovereignty. Through programs such as PRISM, states access the servers of global tech giants (Google, Facebook, and Microsoft) to harvest metadata, thereby extending their jurisdiction to wherever American digital infrastructure exists. This creates a "Digital Panopticon," a concept adapted from Foucault (1995) and elaborated by Cohen (2008). Unlike the physical Panopticon, the digital version does not require a visible guard; the awareness of data collection compels individuals to discipline themselves and modify their behavior, creating "docile bodies" even in the absence of physical coercion. The study finds that legal frameworks such as US FISA Section 702 facilitate this by allowing surveillance of "non-US persons" located outside the US, thereby projecting sovereignty extraterritorially through digital infrastructure. As Greenwald (2014b) notes, this system eliminates the expectation of privacy for anyone using these global networks.

Findings on new actors: The research confirms the emergence of a diverse array of non-state actors challenging the state's traditional monopolies. The findings categorize these actors into three groups: leakers (e.g., Julian Assange of WikiLeaks), hacktivists (e.g., Anonymous), and infrastructure

capitalists (e.g., Elon Musk of Starlink). WikiLeaks has been shown to have successfully challenged the state's information sovereignty by turning diplomatic secrecy into public data. Domscheit-Berg (2011) argues that Assange's strategy was specifically designed to paralyze the diplomatic networks of superpowers. Hacktivist groups such as Anonymous have evolved from protesters into cyber-mercenaries, participating in conventional conflicts, including the Russia–Ukraine war, and targeting state infrastructure (Svyrydenko & Mozgin, 2022). Furthermore, the study finds that private corporations have become geopolitical actors; for instance, Starlink's ability to maintain or cut off Ukraine's communication capabilities demonstrates that critical infrastructure sovereignty is now shared with "technological feudal lords". Finally, the results highlight the blurring of the kinetic–digital divide, as evidenced by the 2024 Lebanon pager attacks and the Colonial Pipeline attack (Russon, 2021), in which digital supply-chain infiltration resulted in physical lethality or paralysis, demonstrating that cyber power can now destroy physical bodies and environments.

## 4. Discussion

The findings of this study point toward a complex restructuring of global power that defies simple categorization. A central theme emerging from the analysis is the formation of a "Baroque" power structure (DeNardis, 2014). Unlike the clear, linear hierarchies of the Westphalian system, this new structure is ornamental and complex, characterized by low accountability and high interdependence. Power does not reside solely in the state apparatus; it circulates among intelligence agencies, multinational technology corporations, and decentralized hacker networks. The discussion highlights that states often act as "proxies" for corporations, and vice versa. For example, the US government utilized financial blockades via Visa and MasterCard to cripple WikiLeaks, demonstrating a fusion of state authority and corporate mechanisms.

The classical Westphalian view relies on the "inside/outside" distinction—order inside the state; anarchy outside. The study argues that cyberspace obliterates this distinction. The case of Edward Snowden, stranded in the transit zone of a Moscow airport, exemplifies this liminality: legally outside US territory yet digitally present everywhere through his leaks. The discussion posits that while states attempt to re-establish borders through "digital firewalls" or national intranets (like RuNet), the fluid nature of information flow renders these territorial defenses increasingly porous.

The discussion emphasizes a fundamental paradox: Encryption technologies liberate the individual from the state's territorial gaze, granting them a "transnational identity" (Habermas, 2001, p. 118). Yet, the very infrastructure that enables this freedom—commercial internet networks—simultaneously feeds the state's surveillance apparatus. The individual is caught between the liberation afforded by encryption and the discipline of the Digital Panopticon. While encryption permits the expansion of political rights and the expression of dissent, it also facilitates a culture of impunity among cybercriminals and terrorists (Moore & Rid, 2016), creating a security dilemma that traditional geography cannot resolve.

Finally, the discussion critiques the limitations of traditional borders in the face of cyber-physical attacks. The Stuxnet virus (Alvarez, 2015) and the Hezbollah pager explosions (BBC, 2024) demonstrate that the "battlefield" is no longer confined to a specific geographic zone. A digital signal sent from one continent can cause physical destruction on another, rendering geographical distance

meaningless. This implies that national security can no longer be guaranteed solely by guarding physical frontiers, as threat vectors are embedded in the devices and supply chains of daily life.

## 5. Conclusions

This study concludes that the emergence of cyberspace has fundamentally and irreversibly transformed political geography. It is no longer sufficient to view the world merely as a collection of territorial containers; rather, it must be understood as a data-driven, connective reality where power is defined by the control of codes and networks as much as by the control of land.

The primary generalization inferred from the results is that sovereignty is being "deterritorialized." The state's monopoly on violence and information—the two pillars of modern statehood—has been fractured. However, the state is not disappearing; it is mutating. Through mass surveillance and cooperation with technology giants, the state is reconstructing its sovereignty not on the soil but through the data flows that traverse it.

The theoretical and practical implications are profound. Theoretically, the study suggests that the "individual" has become a competitor to the "state" in the international arena, capable of wielding power previously reserved for governments (e.g., encryption, cyberattacks). In practice, this means that states are entering an era of "hybrid warfare" and "surveillance capitalism" (Zuboff, 2019), in which they must constantly negotiate their authority with private entities and invisible networks. The distinction between peace and war and between civilians and soldiers is becoming increasingly blurred.

Consequently, this study posits that future scholarship in political geography must transcend the limitations of the traditional terracentric paradigm. Scholars and policymakers must conceptualize new spatial realities produced by algorithms and digital platforms. To understand security, rights, and power in the 21st century, one must examine the tension between the liberating potential of encryption and the recentralizing force of surveillance. The future of political geography lies in mapping these invisible tensions that now shape the physical world.

## 1.Giriş

Modern siyasi coğrafyanın temelleri, egemenliğin belirli bir toprak parçası üzerinde tanımlandığı devlet merkezli bir düzene dayanmaktadır. Özellikle I. Dünya Savaşı sonrasında uluslararası toplum, çatışmaların önlenmesi ve barışın tesisi amacıyla yeni bir yönetişim arayışına girmiş; bu süreçte Milletler Cemiyeti ve ardından Birleşmiş Milletler (BM) gibi yapılarla uluslararası hukuk sistemini kurumsallaştırmaya çalışmıştır. Bu dönemin en belirgin özelliği, hakların ve yetkilerin kullanımının mutlak surette devlet egemenliği ve ülke sınırları ile ilişkilendirilmiş olmasıdır. 1945 tarihli BM Antlaşması'nın 1. maddesinin 2. fıkrası, "halkların kendi kaderini tayin hakkı" ilkesini vurgulayarak insan haklarını uluslararası siyasetin meşru bir unsuru haline getirse de bu hakların hayata geçirilmesinde devleti birincil ve zorunlu bir aracı olarak konumlandırmıştır.

İnsan Hakları Evrensel Bildirgesi (1948) ve onu izleyen uluslararası sözleşmelerle bireye evrensel bir kimlik atfedilmiş olsa da uygulamada bu evrensel kimlik, daima ulusal kimliğin sınırlarına tabi kalmıştır. Borgwardt (2005)'ın da işaret ettiği gibi, devletler hem insan haklarının başlıca sağlayıcısı hem de egemenlik kaygılarıyla bu hakların önündeki en büyük engel haline gelebilmiştir. Devletler, uluslararası hukuk mekanizmalarına tam bağlanmak istemediklerinde, egemenliklerini bir kalkan olarak kullanarak kendi siyasi coğrafyaları içindeki hak ihlallerini iç işleri kapsamında meşrulaştırma eğilimi göstermişlerdir. Dolayısıyla, klasik uluslararası düzende birey, hakların pasif bir taşıyıcısı olarak kalmış; siyasi ve hukuki varlığı fiziksel mekânın (toprak) sınırlarıyla kısıtlanmıştır.

Ancak 21. yüzyıla gelindiğinde, ulus-devletin mekânsal tekeline dayanan bu yerleşik kabul, siber mekânın yükselişiyle köklü bir dönüşüm sürecine girmiştir. Siber mekân, bireyin devletlerin toprak sınırlarıyla çevrili fiziksel coğrafyasından bağımsız, alternatif ve sınır aşan bir siyasi coğrafya içinde varlık göstermesine olanak tanımaktadır. Habermas (2001, s. 114)'ın belirttiği gibi, bireylerin belirli bir toprak parçasına ve zamana bağlı varlığı, artık onların hak sahibi ve siyasi aktör olarak tanınmasında tek belirleyici ölçüt olmaktan çıkmaktadır. Dijital ağlar, klasik siyasi coğrafyanın durağan toprak mantığının karşısına, dinamik ve akışkan bir ağ mantığını yerleştirmektedir (Castells, 2010). Bu yeni mekânsal düzen, fiziksel mesafeyi anlamsızlaştırarak bireye klasik devlet denetiminin ötesinde yeni bir hareket alanı sunmakta; onu haklarının ve eylemlerinin doğrudan aracısı haline getirmektedir. Dolayısıyla siber mekân, sadece bir iletişim ortamı değil, egemenliğin ve kimliğin yeniden müzakere edildiği yurtsuzlaşmış (Deleuze & Guattari, 2015) bir alan olarak işlev görmektedir. Bu yeni durum, kimliğin sınır ötesi bir boyuta taşınmasını sağlayarak, hak sahipliğini ve siyasi eylemliliği devlet merkezli mekânsal sınırlardan kısmen bağımsızlaştırmakta ve küresel bir boyuta taşımaktadır.

Bu bağlamda çalışmanın temel problematiği, klasik siyasi coğrafyanın katı *"sınır"* ve *"egemenlik"* kabulleri ile siber mekânın sınırsız ve akışkan doğası arasındaki ontolojik gerilimdir. Çalışma, siber mekânın uluslararası siyasi coğrafyada yarattığı kırılmayı ve dönüşümü üç temel eksen üzerinden analiz etmektedir. Birincisi, şifreleme teknolojilerinin bireylere sağladığı özerkliktir; bu teknolojiler sayesinde bireyler ve gruplar, yerel yasaların kısıtlamalarından sıyrılarak ifade ve örgütlenme özgürlüğünü küresel ölçekte kullanabilmektedir. İkincisi, devletlerin bu yeni mekânsal gerçekliğe yanıt olarak geliştirdiği gözetim stratejileridir. Devletler, dijital gözetim teknolojileri aracılığıyla egemenlik kapasitelerini toprak sınırlarının ötesine taşıyarak siyasi mekân anlayışını yeniden tanımlamaktadır. Üçüncüsü ise, WikiLeaks ve Anonymous gibi yeni aktörlerin sahneye çıkışıdır; bu aktörler, ağ tabanlı güç biçimleriyle devletlerin otoritesine meydan okumakta ve küresel güç ilişkilerinde yeni bir denge arayışını temsil etmektedir.

## 2. Şifreleme: Birey, Devlet ve Güvenlik

Modern şifrelemenin kökenleri, II. Dünya Savaşı sırasında Alan Turing ve ekibinin Enigma[1] şifrelerini çözme çalışmalarına dayansa da günümüzde bu teknoloji askeri tekelden çıkarak sivil hayatın ve küresel iletişim ağlarının merkezine yerleşmiştir. Turing'in (Berlinski, 2000) temellerini attığı hesaplama mantığı, o dönemde devletlerin tekelinde olan bir güç unsuruyken; günümüzde modern işlemcilerin kapasitesi sayesinde her bireyin cebine giren sıradan bir araca dönüşmüştür. Bugün dijital şifreleme, askeri bir strateji olmakla beraber siber mekânın fiziğini oluşturan temel yapı taşıdır.

Dijital şifrelemeyi çözebilmek, devasa bir işlem gücü veya doğru matematiksel anahtara sahip olmayı gerektirir. Mevcut şifreleme teknikleri, devletlerin sahip olduğu süper bilgisayarların dahi makul bir sürede çözemeyeceği matematiksel zorluklar üzerine kuruludur. Bu durum, teknik bir detay gibi görünse de siyasi coğrafya açısından devrim niteliğinde bir sonuç doğurur: Birey, matematiksel algoritmalar sayesinde, devletin nüfuz edemediği, gözetleyemediği ve denetleyemediği özerk bir alan yaratma kapasitesine erişmiştir.

Gündelik hayatta şifreleme, çevrim içi ticaretin ve güvenli iletişimin görünmez omurgasıdır. Amazon ve Alibaba gibi e-ticaret devlerinin varlığı, Bitcoin ve Ethereum gibi kripto varlıkların merkeziyetsiz finansal işlemleri veya WhatsApp üzerinden yapılan kişisel yazışmaların mahremiyeti, tamamen bu teknolojinin sağladığı güven zeminine dayanır. Benzer şekilde, pandemi sonrası iş yapış biçimlerini kalıcı olarak değiştiren Zoom ve Microsoft Teams gibi platformlar, emeğin fiziksel mekândan koparılmasını yine uçtan uca şifreleme protokolleri sayesinde mümkün kılmıştır. Ayrıca, Apple Pay ve Google Wallet gibi dijital cüzdanlardan, e-Devlet kapıları üzerinden erişilen bürokratik hizmetlere kadar uzanan geniş bir yelpaze, kimliğin ve varlıkların dijitalleştiği bu yeni düzende şifrelemeyi, modern yaşamın sürdürülebilirliği için zorunlu bir altyapı haline getirmiştir (DeNardis, 2014, s. 93). Ancak şifrelemenin asıl dönüştürücü etkisi, ticari kullanımdan ziyade siyasi alanda, birey-devlet ilişkisindeki güç asimetrisini sarsmasıyla ortaya çıkmaktadır. Tarihsel olarak devletler, iletişim teknolojilerini kontrol altında tutarak egemenliklerini pekiştirmişlerdir (Kahn, 1996). Ancak 1990'larda Phil Zimmermann (1995) tarafından geliştirilen PGP (Pretty Good Privacy) gibi yazılımlar, askeri düzeyde şifrelemeyi sivil kullanıma açarak bu denklemi değiştirmiştir. ABD hükümeti, PGP'yi askeri mühimmat kategorisine alarak ihracatını yasaklamaya çalışmışsa da internetin sınır tanımaz doğası karşısında başarısız olmuştur. Kodun dijital ağlar üzerinden küresel ölçekte yayılması, devletlerin ulusal sınırları içerisindeki bilgi akışını denetleme kapasitesini fiilen ortadan kaldırmıştır (Lessig, 2006). Bu süreç, kodun yerel yasalara tabi olmayan, küresel ve sınır-aşan bir ifade özgürlüğü biçimine dönüşmesini sağlamıştır.

Bu dönüşüm, özellikle otoriter rejimlerde yaşayan muhalifler ve aktivistler için hayati bir önem taşır. İnternet, toplumsal hareketlere hız ve örgütlenme kolaylığı sağlarken (Castells, 2007; Fielder, 2013, s. 162), şifreleme teknolojileri bu gruplara devletin gözetiminden korunabilecekleri güvenli bir siber alan sunmaktadır. Bu durum, 1990'larda ortaya çıkan ve kriptografiyi politik bir direniş aracı olarak gören Cypherpunk hareketinin temel argümanıyla örtüşmektedir. Bu perspektife göre, devletler iktidarlarını bilgi üzerindeki tekelleriyle sürdürür; kriptografi ise bireylere bu tekele meydan okuma ve özerklik kazanma imkânı tanır (Blount, 2019, s. 138; Greenberg, 2012, s. 148). Julian Assange ve WikiLeaks örneği, bu teorik yaklaşımın pratiğe dökülmüş halidir. Assange, geliştirdiği Rubber Hose şifreleme sistemiyle, devletin fiziksel baskısına karşı dijital verinin dokunulmazlığını savunmuştur (Greenberg, 2012, s. 126-127). Burada ortaya çıkan tablo, fiziksel coğrafya ile siber coğrafya arasındaki

gerilimdir. Devlet, bireyin bedenini fiziksel sınırları içinde hapsedebilir; ancak şifreleme sayesinde bireyin zihni, iletişimi ve verisi bu sınırların ötesine geçerek devletin erişemeyeceği bir alanda varlığını sürdürür.

Öte yandan şifrelemenin sunduğu bu sınırsızlık, madalyonun diğer yüzünde siber suçlular ve terör örgütleri için de bir koruma kalkanı ve operasyonel bir alan oluşturmaktadır. Muhalifler için bir özgürlük aracı olan şifreleme, suç şebekeleri için hukuki takipten kaçışın ve cezasızlık kültürünün bir yolu haline gelmektedir (Moore & Rid, 2016). Geleneksel karanlık ağ (darknet) faaliyetleri; uyuşturucu ve çocuk istismarından, günümüzde devletlerin kritik altyapılarını hedef alan Hizmet Olarak Fidye Yazılımı modellerine evrilmiştir. LockBit gibi küresel siber suç kartelleri, şifrelemeyi sadece veriyi gizlemek için değil, kurbanın verisini rehin alarak kripto paralar üzerinden fidye talep etmek için kullanmaktadır. Burada önemli bir mekânsal ayrım mevcuttur. Muhalifler şifrelemeyi kullanarak siyasi haklarını genişletirken, suçlular hukuki yükümlülüklerini aşmakta; ancak her iki grup da veriyi devletin egemenlik alanının dışına kaçırmaktadır.

Bu durumun en uç ve tehlikeli boyutu ise terörizmin mekânsal dönüşümüdür. 2015 Paris saldırılarıyla başlayan süreç, günümüzde terör örgütlerinin uzaktan radikalleşme ve saldırı yönetimi kapasitesine ulaşmasıyla yeni bir evreye girmiştir. Devletlerin güvenlik gerekçesiyle şifrelemeye arka kapı açma arzusu, Avrupa Birliği'nin Chat Control yasa tasarıları veya İngiltere'nin Çevrimiçi Güvenlik Yasası gibi girişimlerle hukuki bir mücadeleye dönüşmüştür. Ancak terör örgütleri, 11 Eylül sonrası hiyerarşik yapılardan, merkeziyetsiz ve hücre tipi ağlara dönüşerek siber mekânı stratejik bir derinlik olarak kullanmaya devam etmektedir (Blount, 2019).

Bunun en çarpıcı ve güncel örneği, Mart 2024'te Moskova'daki Crocus City Hall'a düzenlenen DEAŞ saldırısıdır. Saldırganlar, fiziksel olarak hiç bulunmadıkları ülkelerdeki örgüt yöneticileriyle Telegram gibi uçtan uca şifreli uygulamalar üzerinden haberleşmiş, talimatları ve kripto para transferlerini bu dijital tüneller üzerinden almıştır. Bu vaka, teröristlerin fiziksel sınırları geçmeden, sadece veri akışları üzerinden bir başka ülkenin başkentinde şiddet uygulayabildiğini göstermektedir. Dolayısıyla şifreli uygulamalar, terörün yersiz-yurtsuzlaşmasını (deterritorialization) tetikleyerek, tehdidi belirli bir coğrafyadan çıkarıp, ağın ulaştığı her noktaya yaymaktadır.

Bu bağlamda düşünüldüğünde, siber mekân, terör örgütlerine *"yarı-devlet"* benzeri bir işlev kazandırmakta ve onlara sınır-aşan bir siyasi aktör niteliği yüklemektedir (Clapham, 1998). Bu tarz örgütler, fiziksel bir toprağa ihtiyaç duymadan, dijital ağlar üzerinden ideolojilerini yayabilmekte ve hedef ülkelerin siyasi coğrafyasına nüfuz edebilmektedir. Bu bağlamda şifreleme, terörizmin nedeni değil; ancak terörizmi çevreleyen siyasi coğrafyanın dönüştürücüsüdür. Güç, artık sadece şiddet tekeline sahip devletlerin elinde değil; matematiksel kodlara ve güvenlik tasarımına hâkim olan yapıların da kullanımındadır (Greenberg, 2012, s. 154).

Dolayısıyla, şifreleme teknolojileri bireylere veya devlet dışı aktörlere ulusal sınırlarla çevrili klasik siyasi coğrafya içinde kendilerine verilmeyen bir gücü kullanma özerkliği sağlamaktadır. Habermas'ın (2001, s. 118) belirttiği üzere, bu teknoloji bireylere ulus-ötesi bir kimlik kazandırmaktadır. Devletler, yasama yoluyla şifrelemeye arka kapı koymaya çalışsa da (Berkman Center, 2016), kodun küresel dağılımı ve açık kaynak niteliği, bu çabaları büyük ölçüde etkisiz kılmaktadır. Bu gelişmeler, devletlerin kendi siyasi coğrafyalarındaki iletişim koşulları üzerindeki münhasır kontrol yetkisini kaybettiklerini göstermektedir (Cohen, 2008). Şifreleme, internetin 21.

yüzyılın kamusal alanı olarak işlev görmesini sağlayan, sınırları devletler tarafından değil, kodlar tarafından çizilen yeni bir siyasi coğrafya inşa etmektedir (Clinton, 2011).

### 3. Gözetim: Siber Teknolojiler ve Siyasi Coğrafyanın Yeniden İnşası

Uluslararası hukuk ve klasik siyasi coğrafya anlayışı, devletlerin yargı ve denetim yetkisini tarihsel olarak egemenlik sınırları kabul edilen toprak parçası ile sınırlandırmıştır. II. Dünya Savaşı sonrasında şekillenen mekânsal düzende, bir devletin kendi sınırları dışındaki bireyler üzerinde doğrudan hak iddia etmesi veya müdahalede bulunması, egemenlik ilkesinin ihlali olarak görülmüştür. 1960 yılında Adolf Eichmann'ın İsrail istihbaratı tarafından Arjantin'den kaçırılması hadisesi, bu ilkenin katılığını gösteren tarihsel bir örnektir (Arendt, 1963). O dönemde, adaletin tecellisi için dahi olsa sınırların ihlal edilmesi diplomatik krizlere yol açmış; uluslararası yönetişim, İsrail'in yargılama talebinden ziyade Arjantin'in toprak bütünlüğünü esas almıştır (United Nations Security Council, 1960). Bu vakadan çıkarılacak temel ders, 1945 sonrası düzende devletlerin bireylerin haklarına kendi toprakları dışında aracılık etmelerinin istisnai ve zorlu bir süreç olduğudur. Devletler, suçluların iadesi gibi konularda ancak karşılıklı anlaşmalar ve diplomatik prosedürler yoluyla, yani diğer devletin egemenliğine saygı duyarak hareket edebilmişlerdir.

11 Eylül saldırıları ve sonrasındaki güvenlik paradigması, bu sınır algısında köklü bir kırılma yaratmıştır. Devletler —başta ABD olmak üzere— sınırlarını artık sabit hatlar değil, güvenliğin gerektirdiği ölçüde değişken ve genişletilebilir yapılar olarak kavramsallaştırmaya başlamıştır (Bowman, 2007). Bu yeni kavramsallaştırmada siber mekân, devletlerin kendilerini yeniden konumlandırmalarında araçsal ve kurucu bir rol oynamıştır. Günümüzde devletler, dijital gözetim teknolojileri ve siber altyapılar aracılığıyla, başka ülkelerin egemenlik sahasındaki bireylerin haklarına ve mahremiyetine, diplomatik izinlere ihtiyaç duymadan rutin biçimde müdahale edebilmektedir (Lessig, 2006, s. 209).

Siber mekânın bireylere sağladığı sınır aşan özgürlük dinamikleri, paradoksal biçimde devletlerin de sınır aşan bir gözetim kapasitesine ulaşmasını sağlamıştır. Şifreleme teknolojileri her ne kadar erişilebilir olsa da küresel iletişimin ve veri akışının büyük bölümü ticari ağlar üzerinde, şifreli ancak *"metaveriye"* (metadata) açık şekilde gerçekleşmektedir. Bu ağlar, büyük veri olgusunun temelini oluşturarak bireyler hakkında devasa miktarda bilgi birikimine olanak tanır. Lessig (2006, s. 216)'in belirttiği gibi, "internette yaptığınız her şey veri üretir ve bu veriler bir araya getirildiğinde son derece değerlidir". Sıradan bir internet servis sağlayıcısı veya sosyal medya platformu, kullanıcının IP adreslerinden ilgi alanlarına, politik görüşlerinden en mahrem ilişkilerine kadar uzanan bir dijital izi kayıt altına almaktadır. Zuboff'un (2019) 'Gözetim Kapitalizmi' olarak adlandırdığı bu yeni ekonomik mantıkta, insan deneyimi davranışsal veriye dönüştürülmekte ve devletler bu ticari veri havuzlarından faydalanarak istihbarat kapasitelerini maliyetsiz bir şekilde artırmaktadır. ABD Yüksek Mahkemesi (2014) de bu durumu teyit ederek, modern cep telefonlarında saklanan verilerin, bir bireyin tüm özel yaşamını yeniden inşa etmeye yetecek yoğunlukta olduğunu kabul etmiştir. Devletlerin bu verilere erişim kapasitesi, geleneksel fiziki takiple elde edilebilecek istihbaratın çok ötesine geçerek, birey üzerinde mutlak bir şeffaflık alanı yaratmaktadır.

Siber mekânın her yerde mevcut olması, hükümetlerin Google, Microsoft veya Facebook gibi küresel ticari kuruluşlara erişim sağlamaları halinde, dünya genelindeki bireyler hakkında kapsamlı bilgi profilleri elde edebilecekleri anlamına gelmektedir (Lessig, 2004, s. 278). Edward Snowden'ın 2013

yılında ifşa ettiği belgeler, bu teorik olasılığın ABD Ulusal Güvenlik Ajansı (NSA) tarafından pratiğe döküldüğünü kanıtlamıştır (Greenwald, 2014a). Snowden belgeleri, ABD ve müttefiklerinin (Beş Göz ittifakı[2]), 11 Eylül sonrasında küresel iletişimi yakalamak için kurdukları gizli hukuki ve teknik altyapıyı gün yüzüne çıkarmıştır. Bu ifşaatlar, gözetim sisteminin yalnızca suçluları değil, sıradan vatandaşları ve müttefik devlet liderlerini de kapsayan bir dijital ağ ördüğünü göstermiştir (Greenwald, 2014b, s. 2).

Bu noktada, PRISM programı, devletin gözetim kapasitesinin mekânsal sınırları nasıl aştığına dair en çarpıcı örnektir. Snowden belgeleriyle ortaya çıkan PRISM, NSA'in dokuz büyük ABD merkezli internet şirketinin sunucularından doğrudan veri akışı sağladığı bir programdır (Gellman & Poitras, 2013; National Security Agency, 2013). E-postalar, sesli aramalar, videolar ve sosyal medya etkileşimlerini kapsayan bu veri havuzu, NSA'in topladığı internet iletişimlerinin yaklaşık %91'ini oluşturmaktadır (PCLOB, 2014, s. 33-34). Mahremiyet ve Sivil Özgürlükler Gözetim Kurulu'nun raporuna göre, bu yöntemle yılda yaklaşık 26,5 milyon internet işlemi sorgulanmaktadır. Bu sistem, istihbarat toplama faaliyetini bireyin bulunduğu fiziksel mekândan (örneğin Berlin'deki bir ofisten) koparıp, verinin depolandığı siber mekân (örneğin Virginia'daki bir sunucu) üzerinden gerçekleştirerek, devletin müdahale alanını teknik altyapının sınırlarına kadar genişletmektedir.

Gözetim sisteminin yaslandığı hukuki zemin, siyasi coğrafyadaki vatandaş ve yabancı ayrımının nasıl dönüştüğünü anlamak açısından kritiktir. ABD'de 11 Eylül sonrası yürürlüğe giren ve zamanla revize edilen Yabancı İstihbarat Gözetim Yasası'nın (FISA) 702. maddesi, bu dönüşümün merkezindedir. ABD Anayasası'nın 4. Değişikliği, Amerikan vatandaşlarını nedensiz arama ve el koymaya karşı korurken; bu koruma ABD vatandaşı olmayan ve ABD sınırları dışında bulunan yabancılara teşmil edilmemektedir (PCLOB, 2014, s. 20-21). Bu hukuki ayrım, NSA'in gözetim faaliyetlerini *"hedefin toprakla sınırlı olmaması"* ilkesine dayandırmasına olanak tanımıştır. Yani bir kişi fiziksel olarak ABD toprağında değilse, verisi ABD üzerinden geçse dahi yabancı statüsüyle herhangi bir yargı kararı olmaksızın gözetlenebilir. Ancak küresel internet trafiğinin çok büyük bir kısmının ABD merkezli sunucular ve fiber optik kablolar üzerinden akması, bu yerel yasayı fiilen küresel bir dijital egemenlik aracına dönüştürmüştür. ABD, yabancı tanımını kullanarak, kendi topraklarını (sunucularını) bir kaldıraç gibi kullanmakta ve diğer devletlerin topraklarındaki bireyler üzerinde denetim kurmaktadır (Lam, 2013; Poitras vd., 2013).

Snowden'ın ortaya çıkardığı tablo, devletin gözetim yoluyla siyasi mekânı yeniden inşa etmesidir. Bu inşa süreci, Michel Foucault (1995)'nun modern toplumların denetim mekanizmasını açıklamak için Jeremy Bentham'dan ödünç aldığı Panoptikon metaforu ile açıklanabilir. Foucaultcu anlamda Panoptikon, bireyin sürekli izlendiğini veya her an izlenebileceğini varsayarak iktidarın kurallarını içselleştirdiği, görünmez bir disiplin mekanizmasıdır. Geleneksel Panoptikon'da gözetim fiziksel bir mimariye dayanırken; Cohen (2008, s. 184-186) bu kavramı günümüze uyarlayarak, veri ağları ve algoritmalar üzerinden işleyen "*dijital bir Panoptikon"*dan bahseder. Bu sistemde gözetim, birinin o an gerçekten ekran başında izleyip izlemediğinden bağımsız olarak mekân deneyimini değiştirir. Bireyler, dijital izlerinin kaydedildiğinin farkında oldukları için davranışlarını değiştirir, otosansür uygular ve uysal bedenlere dönüşürler (Greenwald, 2014b, s. 3).

Bu bağlamda ulusötesi gözetim, siber mekânı sadece bir iletişim ortamı olmaktan çıkarıp, iktidarın güç ilişkilerini sürekli yeniden ürettiği bir siyasi coğrafyaya dönüştürür. Snowden'ın Avrupa Parlamentosu'ndaki (2014) "*sandalyemden kalkmadan, bu komitenin herhangi bir üyesinin veya herhangi bir sıradan vatandaşın özel yazışmalarını okuyabilirdim.*" ifadesi, bu mekânsal dönüşümün

teknik boyutunu özetlemektedir. Gözetim altındaki mekânlar (internet, akıllı şehirler), karar alıcıların ve vatandaşların sürekli izlenebilirlik kaygısı taşıdığı disiplin alanlarına dönüşürken; mahremiyet, iktidarın erişemediği çok dar alanlara sıkışmaktadır (Dittmer, 2015). Gözetim teknolojileri, mekânlar arasında görünmez bir ayrım çizgisi çeker. Bir yanda şeffaflaştırılan ve denetlenen alanlar, diğer yanda bu denetimin dışında kalabilen (örneğin şifreli ağlar) kör noktalar vardır.

Devletin bu sınır ötesi gücü, yalnızca kendi kurumlarıyla değil, kurumsal aracılar (teknoloji şirketleri) üzerinden de işlemektedir (Timberg & Nakashima, 2013). Devletler, şirketlerin sunduğu gündelik konforu (e-posta, sosyal medya, bulut depolama) bir tuzak gibi kullanarak bireylerin gönüllü olarak gözetim sistemine dahil olmasını sağlar (Cohen, 2008, s. 187). Örneğin, bireylerin ev güvenlikleri için taktıkları Amazon Ring kameralarının verilerinin kolluk kuvvetleriyle paylaşılması veya devletlerin İsrail merkezli NSO Group'tan satın aldıkları Pegasus yazılımı ile sınır ötesi muhalifleri dinlemesi, bu iş birliğinin somut kanıtlarıdır. Bireyler, ücretsiz hizmetler karşılığında verilerini paylaşmayı normalleştirirken, devletler bu verilerin ham gücünü işleme kapasitesinden stratejik fayda sağlar. Bu durum, devlet-şirket iş birliğine dayalı, hesap verilebilirliği düşük Barok bir güç yapısı ortaya çıkarır (DeNardis, 2014, s. 15). Gözetim artık tek bir devletin tekelinde değil; ABD, İngiltere (GCHQ) ve diğer müttefiklerin oluşturduğu çok merkezli bir ağ üzerinden yürütülmektedir (Hopkins & Borger, 2013).

Devletin siber mekân üzerinden siyasi coğrafyayı dönüştürme kapasitesi, yalnızca veri toplamakla sınırlı kalmayıp, fiziksel altyapıları ve yaşamı doğrudan hedef alan bir aşamaya evrilmiştir. Nesnelerin İnterneti (IoT) ve siber-fiziksel sistemler, dijital kodların kinetik bir güce dönüşmesine olanak tanımaktadır. Stuxnet virüsü, İran'ın nükleer tesislerini hedef alarak, bir devletin asker göndermeden başka bir ülkenin en kritik tesislerini fiziksel olarak yok edebileceğini gösteren ilk büyük örnekti (Alvarez, 2015). Ancak günümüzde bu tehdit, endüstriyel tesislerden gündelik yaşamın altyapısına kaymıştır.

Örneğin, 2021 yılında ABD'de gerçekleşen Colonial Pipeline siber saldırısı (Russon, 2021), dijital bir müdahalenin fiziksel petrol akışını durdurarak devletin enerji egemenliğini nasıl felç edebileceğini ve yakıt tedarik coğrafyasını nasıl değiştirebileceğini kanıtlamıştır. Benzer şekilde, Rusya-Ukrayna Savaşı sırasında Viasat uydu iletişim ağlarına yapılan siber saldırılar (Boschetti vd., 2022), dijital cephe ile fiziksel cephe arasındaki sınırın tamamen silikleştiğini göstermiştir.

Bu dönüşümün en çarpıcı ve güncel örneği ise 2024 yılında Lübnan'da yaşanan çağrı cihazı ve telsiz patlamalarıdır (BBC, 2024). Tedarik zincirlerine sızan aktörlerin, uzaktan gönderilen dijital bir sinyalle sivil cihazları patlayıcıya dönüştürebilmesi, siber gücün yalnızca veriyi değil, insan bedenini ve fiziksel çevreyi de doğrudan imha edebilecek bir boyuta ulaştığını ortaya koymuştur. Bu vaka, siber savaşın artık belirli bir cephe hattı ile sınırlı olmadığını, cebimizdeki cihazların dahi birer ulusal güvenlik sahasına dönüşebileceğini göstermektedir.

Paralel olarak, ABD'nin insansız hava aracı (İHA/Predator) politikasıyla başlayan dijitalleştirilmiş şiddet, bugün otonom sistemler ve yapay zeka destekli hedefleme ile yeni bir boyuta taşınmıştır. Nevada'daki bir operatörün veya bir algoritmanın, binlerce kilometre ötedeki bir hedefi uydu ve internet altyapısı üzerinden vurabilmesi, coğrafi mesafeyi anlamsızlaştıran yeni bir güç teknolojisidir (Michel, 2015). Bu teknoloji, savaş alanı kavramını belirli bir coğrafyadan çıkarıp, gözetim ve veri akışının ulaşabildiği her yere taşımaktadır. Dolayısıyla, siber mekân üzerinden işleyen

gözetim ve şiddet pratikleri, uluslararası sistemde mekânın anlamını köklü biçimde dönüştürmekte; egemenlik, sınırlar ve güvenlik kavramlarını topraktan veriye ve bağlantısallığa doğru kaydırmaktadır.

## 4. Yeni Aktörler: Küresel Siyasi Coğrafyada Gerçek ve Sanal Unsurlar

Gücün karşılıklı geçişkenliği, siyasi coğrafyadaki değişimleri yerel düzeyde açıklamaya yardımcı olsa da bu değişimlerin uluslararası mekânın siyasi coğrafyası üzerindeki kurucu etkilerinin daha derinlikli sorgulanması gerekmektedir. Klasik uluslararası ilişkiler disiplini ve Westphalia düzeni, gücü devletler ve uluslararası örgütler arasındaki hiyerarşik ilişkiler üzerinden okurken; siber mekân bu denkleme ağ tabanlı, merkeziyetsiz ve devlet dışı yeni aktörleri dahil etmiştir. Devletlerle doğrudan rekabet edebilecek kapasiteye ulaşan bu aktörler ağa bağlandıklarında, fiziksel sınırların nasıl aşındığı ve egemenliğin nasıl paylaşıldığı daha açık hale gelmektedir. İnternet yönetişiminde devletlerin yetki devretmesi ve çevrimiçi altyapının (sunucular, kablolar, uydular) özel sektöre veya dağınık ağlara bağımlı hale gelmesi, klasik egemenlik alanında ciddi boşluklar yaratmıştır.

Bu bağlamda, teknolojiyi (hacking) siyasi değişim amacıyla kullanarak küresel siyasi coğrafyada yeni bir güç odağı oluşturan hacktivistler incelenmeye değerdir. Greenberg (2012, s. 131)'in belirttiği üzere, bu aktörler şifrelemeyi gücü halka aktarmak için bir kaldıraç olarak kullanmakta ve devletin bilgi üzerindeki tekelini kırmaktadır. Hacktivizm, sadece dijital bir protesto biçimi değil, küresel siyasi coğrafyadaki dönüşümü görünür kılan ve sınırların geçirgenliğini kanıtlayan mekânsal bir olgudur. Bu aktörler, fiziksel bir toprağa ihtiyaç duymadan, kodlar ve ağlar üzerinden siber topraklar işgal edebilmekte ve devletlerin karar alma süreçlerini etkileyebilmektedir.

Bu dönüşümün ilk büyük kırılma noktası ve devletin bilgi egemenliğine vurulan en büyük darbe, Julian Assange tarafından kurulan WikiLeaks organizasyonudur. 2010 yılında Cablegate sızıntılarıyla ABD Dışişleri Bakanlığı'na ait 250 binden fazla diplomatik yazışmayı yayımlayan WikiLeaks, devletlerin gizlilik zırhını delerek diplomatik mahremiyeti küresel bir kamusal veriye dönüştürmüştür. Assange, WikiLeaks'i "dünyanın en çok baskı gören belgeleri için bir kütüphane" olarak tanımlayarak, bilgiye sığınma hakkı verdiğini iddia etmiştir. Bu eylem, sadece ifşa niteliği taşımamakta; bilginin mekânsal kontrolüne dair bir egemenlik mücadelesi olarak görülmektedir. Daniel Domscheit-Berg (2011), Assange'ın stratejisinin özellikle ABD'yi hedef alarak, süper gücün küresel imajını ve diplomatik ağlarını felç etmeyi amaçladığını belirtir. Sızıntılar, ABD'nin diplomatik yazışmalarını, devletin kontrol edemediği, sınırlarını kapatamadığı bir siber uzamda erişilebilir kılarak, devletin bilgi üzerindeki egemenlik iddiasını boşa çıkarmıştır.

WikiLeaks vakası, devletlerin siber tehditlere karşı verdiği tepkinin hibrit ve Barok doğasını da ortaya koymuştur. Devlet, siber alandaki bu tehdidi bertaraf etmek için sadece kendi kolluk kuvvetlerini değil, küresel finansal altyapıyı kontrol eden özel şirketleri de birer vekil (proxy) olarak kullanmıştır. ABD, Assange'ı etkisiz hale getirmek için klasik diplomatik ve hukuki baskı araçlarını kullanırken; eş zamanlı olarak Amazon, PayPal ve MasterCard gibi küresel şirketleri birer siber silah gibi kullanarak WikiLeaks'in finansal altyapısını çökertmiştir. Bu durum, siber mekânda egemenliğin sadece devletler tarafından değil, devlet-şirket iş birlikleri üzerinden yürütülen karmaşık bir güç yapısı tarafından şekillendirildiğini göstermektedir. Assange'ın 2012'den 2019'a kadar Ekvador Büyükelçiliği'ne sığınması, ardından Belmarsh hapishanesine konulması ve nihayetinde 2024'te ABD Adalet Bakanlığı ile yaptığı anlaşma sonucu serbest kalması, bireyin fiziksel bedeni üzerindeki devlet denetimi ile dijital

varlığının alanı arasındaki gerilimi simgeler. Assange bedenen hapsedilse bile, ortaya koyduğu dijital arşiv ve kurduğu ağ, devlet sınırlarını ihlal etmeye devam etmiştir.

Bu güç mücadelesinde sahneye çıkan bir diğer aktör olan Anonymous, liderlik yapısı olmayan ve coğrafi olarak dağınık bir kovan zihniyeti ile hareket etmektedir. Başlangıçta Scientology Kilisesi gibi hedeflere yönelen grup, Cablegate sürecinde WikiLeaks'e sansür uygulayan şirketlere yönelik siber saldırılarla politize olmuştur. Ancak Anonymous'un siyasi coğrafya üzerindeki etkisi, özellikle 2022 Rusya-Ukrayna Savaşı ile yeni ve stratejik bir boyuta taşınmıştır. Grup, Rusya'ya karşı siber savaş ilan ederek devlet sitelerini, medya organlarını ve enerji altyapılarını hedef almıştır (Svyrydenko & Mozgin, 2022). Bu durum, hacktivist grupların artık sadece protestocu değil, konvansiyonel savaşların seyrini etkileyebilen yarı-askeri siber aktörlere dönüştüğünü göstermektedir. Ukrayna hükümetinin çağrısıyla kurulan Ukrayna Bilişim Ordusu (IT Army of Ukraine) ile paralel hareket eden bu gruplar, fiziksel cephe hattından bağımsız olarak, çatışmayı küresel ağlar üzerinden düşman devletin iç sahasına taşıyabilmektedir (Soesanto, 2022). Bu siber partizanlar, devletin toprak bütünlüğünü dijital yollarla ihlal ederek, savaşın coğrafyasını cephe hattından sunucu odalarına kadar genişletmiştir. Bu durum, 17. yüzyıl deniz savaşlarındaki devlet onaylı korsan geleneğinin dijital ortamda yeniden canlandırılmasıdır. Nasıl ki o dönemde devletler, denizlerdeki egemenlik boşluğunu doldurmak için korsanlara yetki verip onları deniz gücünün bir parçası haline getirdiyse; bugün de devletler, siber uzamdaki egemenlik açıklarını kapatmak için "siber paralı askerleri" ve hacktivist grupları vekil güç olarak kullanmaktadır. Bu, devletin şiddet tekelinin siber mekânda özelleştiğini ve parçalı hale geldiğini gösteren en net kanıttır.

Siber mekânın sınırları nasıl anlamsızlaştırdığının ve aynı zamanda devletlerin bu sınırları nasıl yeniden üretmeye çalıştığının en çarpıcı örneği ise Edward Snowden vakasıdır. ABD Ulusal Güvenlik Ajansı'nın (NSA) küresel gözetim ağını ifşa eden Snowden, devletin sınır algısını hem dijital hem de fiziksel düzlemde test etmiştir. Snowden'ın pasaportunun iptal edilmesine rağmen haftalarca Moskova'daki bir havalimanının transit bölgesinde kalması, uluslararası hukukun ve siyasi coğrafyanın gri alanlarına işaret eder. Transit bölgeler, hukuken bir devletin toprağı sayılsa da giriş yapmadıkça o devletin tam yargı yetkisine tabi olunmayan istisnai mekânlardır. Bu süreçte, Bolivya Devlet Başkanı'nın uçağının Snowden şüphesiyle Avrupa hava sahasında durdurulması ve aranması, devletlerin dijital bir hayaleti yakalamak için fiziksel egemenlik kurallarını ve diplomatik dokunulmazlığı nasıl ihlal edebileceğini, yani dijital paniğin fiziksel agresyona nasıl dönüşebileceğini kanıtlamıştır.

Yeni aktörler bağlamında, son dönemde altyapı sağlayıcı özel teknoloji şirketlerinin rolü de devlet dışı aktörlerin mekânsal gücünü göstermesi açısından kritiktir. Elon Musk'ın sahibi olduğu Starlink uydu internet sistemi, bu durumun en güncel örneğidir. Ukrayna savaşında görüldüğü üzere, bir devletin karasal iletişim altyapısı tahrip edildiğinde, küresel bir şirket olarak Starlink uydu interneti sağlayarak o devletin dijital egemenliğini ve askeri operasyon kabiliyetini ayakta tutabilmiştir. Ancak aynı aktörün, politik gerekçelerle belirli bölgelerde (örneğin Kırım çevresinde) hizmeti kısıtlayabilmesi, altyapı gücünün devlet tekelinden çıkarak, ulus-ötesi şirketlerin inisiyatifine geçtiği yeni bir jeopolitik gerçekliği işaret etmektedir. Bu durum, devletlerin kendi topraklarındaki iletişim üzerinde dahi mutlak egemenlik kuramadığını, egemenliğin teknolojik derebeylikler ile paylaşıldığını göstermektedir. Bu alanda faaliyet yürüten şirketlerin gücü sadece fiziksel altyapıyla sınırlı değildir. Google Haritalar'ın sınırları nasıl çizdiği veya Facebook algoritmalarının hangi siyasi içeriği öne çıkarıp hangisini sansürlediği, uluslararası kamuoyunun coğrafi algısını şekillendiren jeopolitik bir eylemdir. Dolayısıyla

bu aktörler, sadece mekânı kullanan değil, mekânın algısını da üreten siyasi kartografl gibi hareket etmektedir.

Bu vakalar ve güncel gelişmeler ışığında, siber mekânın uluslararası siyasi coğrafyada yarattığı dönüşüm ve yeni aktörlerin rolünü üç temel analitik eksende değerlendirmek mümkündür:

Birincisi, şifreleme teknolojilerinin dönüştürücü rolüdür. Greenberg (2012)'in ifadesiyle internet, bireyi güçlendiren araçlarda bir "Kambriyen patlaması" yaratmıştır. Tıpkı biyolojik tarihte bir anda binlerce yeni türün ortaya çıkması gibi, dijital dünyada da bireyi güçlendiren araçlar bir anda, durdurulamaz bir hızla ve büyük bir çeşitlilikle türemiştir. Bu metaforik patlama, bireyin devlet karşısındaki konumunu kökten değiştirmiştir. Şifreleme; Snowden, Assange ve Anonymous üyelerine kimliklerini gizleyerek veya değiştirerek küresel siyasete müdahale etme gücü vermiştir. Birey, vatandaş kimliğinden sıyrılarak, devletin tanımlayamadığı, vergilendiremediği ve dolayısıyla klasik yöntemlerle denetleyemediği bir ağ aktörüne dönüşmüştür. Bu dönüşüm, devletin vatandaş üzerindeki biyopolitik kontrolünü zayıflatmaktadır.

İkincisi, sınırların işlevsizleşmesi ve yeniden inşasıdır. Devletler, siber tehditleri engellemek için sınırlarını dijital güvenlik duvarları veya ulusal intranet projeleri (RuNet) ile tahkim etmeye çalışsa da bilgi akışı bu sınırları aşındırmaktadır. Snowden ve Assange örnekleri, toprak kavramının hukuki bir kurgu olduğunu, devletlerin egemenlik iddialarının siber akışlar karşısında yetersiz kaldığını göstermiştir. Coğrafi ikilik burada devreye girmektedir: Bireyler, fiziksel olarak bir odaya veya bir terminale hapsolsalar dahi, ağa erişimleri olduğu sürece siber mekânın coğrafyasını kullanarak küresel siyasi süreçleri etkilemeye devam edebilmişlerdir. Bu durum, mekân kavramının fiziksel koordinatlardan koparak, bağlantısallık üzerinden yeniden tanımlanmasını zorunlu kılar.

Üçüncüsü ise, gücün ifadesindeki "Barok" örüntülerdir. Güç artık tek bir merkezde toplanmamakta; devletler, küresel şirketler ve hacktivist ağlar arasında sürekli yer değiştirmektedir. WikiLeaks'e karşı finansal ablukada görüldüğü üzere, devletler güçlerini şirketler üzerinden dolaylı yollarla kullanmaktadır. Diğer taraftan Kuzey Kore'nin Sony'ye saldırısı veya hacktivistlerin devlet altyapılarına saldırıları, siber mekânın devlet ve devlet dışı ayrımını bulanıklaştıran, çok aktörlü ve çatışmalı yeni bir siyasi coğrafya yarattığını doğrulamaktadır. Devletin gücü artık monolitik değil, çeşitlendirilmiş bir portföy halini almıştır; bazen bir hacker grubunu taşeron olarak kullanmakta, bazen de bir teknoloji devinin altyapısına muhtaç kalmaktadır.

## 5. Sonuç

Siber mekânın siyasal coğrafyayı dönüştürme biçimlerini şifreleme teknolojileri, dijital gözetim pratikleri ve küresel ölçekte ortaya çıkan yeni güç ilişkileri üzerinden inceleyen bu çalışmada, elde edilen bulgular, klasik uluslararası düzenin devlet-merkezli sınır anlayışını aşındıran, fakat aynı zamanda onu yeni biçimlerde tahkim eden ikili bir dinamik ortaya koymaktadır.

Öncelikle şifreleme, bireylere ulusal hukuk düzenlerinin dışında konumlanabilecek yeni bir siyasal alan sunmaktadır. Muhalif hareketler, sivil toplum örgütleri ve bireyler, şifreleme sayesinde yerel yasaların sınırlandırıcı etkilerinden kısmen bağımsız biçimde ifade ve örgütlenme özgürlüğünü kullanabilmektedir. Bununla birlikte, aynı teknolojiler suç ve terör ağlarına da imkân tanımakta, böylece devlet otoritesinin ötesinde yeni tehdit alanları üretmektedir. Şifreleme, bu anlamda bireyin haklarını genişleten özgürleştirici bir araç olduğu kadar, hukuki yükümlülüklerden kaçışı kolaylaştıran müphemleştirici bir mekanizma işlevi de görmektedir.

Dijital gözetim mimarileri ise devletlerin sınır-ötesi müdahale kapasitesini radikal biçimde artırmıştır. Snowden belgeleriyle açığa çıkan PRISM gibi programlar, devletlerin kendi yurttaşlarının ötesinde yabancı bireylerin iletişimlerine doğrudan erişebildiğini ve böylece mekânı yeniden tanımlayan bir iktidar ilişkisi kurduğunu göstermektedir. Gözetim yalnızca bireyin mahremiyetini ihlâl etmemekte; aynı zamanda gözetim altındaki mekânları disiplin üreten alanlara dönüştürmektedir. Bu bağlamda devlet egemenliği artık sadece toprak parçasına değil, veri akışlarının denetlenmesine dayalı bir mekânsal mantıkla yeniden inşa edilmektedir.

Küresel düzeyde ise hacktivist gruplar ve bunlara ait platformlar devletlerin mutlak otoritesine meydan okuyan yeni siyasal aktörler olarak belirmektedir. WikiLeaks, Anonymous ve Snowden vakaları, bireylerin ve dağınık kolektiflerin uluslararası siyasetin gündemini değiştirecek ölçüde etkili olabileceğini göstermiştir. Dolayısıyla, devletler birbirleriyle rekabet içerisinde olduğu kadar, çok uluslu şirketler ve ağ tabanlı hareketlerle de sürekli bir güç mücadelesi içinde yer almaktadır. Ortaya çıkan barok güç işleyişleri, klasik Westphalia düzeninden farklı olarak, çok-merkezli ve çok-aktörlü bir siyasal coğrafyaya işaret etmektedir.

Sonuç olarak, siber mekânın siyasi coğrafyası, bireyin özerkliğini artıran şifreleme ile devletin egemenliğini yeniden kuran gözetim arasındaki gerilimde şekillenmektedir. Bu gerilim, uluslararası siyasetin temel parametrelerinden biri haline gelmiş; egemenlik, güvenlik ve özgürlük arasındaki dengeyi yeniden tanımlamıştır. Gelecek araştırmalar açısından, siber mekânın yalnızca teknik bir alan değil, mekânın siyasal anlamını kökten dönüştüren bir zemin olduğu açıktır. Bu nedenle siyasal coğrafya, devlet-toprak merkezli geleneksel paradigmanın ötesine geçerek, kodun, ağların ve dijital platformların ürettiği yeni mekânsal gerçeklikleri kavramsallaştırmak durumundadır.

## Notlar

1. II. Dünya Savaşı sırasında Nazi Almanyası tarafından askerî haberleşmeyi şifrelemek için kullanılan elektromekanik bir şifreleme cihazıdır (O'Brien, 2019).
2. Amerika Birleşik Devletleri ve Birleşik Krallık başta olmak üzere Avustralya, Kanada ve Yeni Zelanda'nın oluşturduğu İstihbarat ittifakıdır.

## Etik ve Yazar Beyanları / *Ethical and Author Declarations*

**Çıkar Çatışması**

Yazar, bu çalışmanın hazırlanması ve yayımlanması sürecinde çıkar çatışması oluşturabilecek herhangi bir ticari veya finansal ilişki içinde olmadığını beyan eder.

***Conflict of Interest***

*The author declares that they have no commercial or financial relationships that could give rise to a conflict of interest during the preparation and publication of this study.*

**Araştırma Etiği Beyanı**

Bu çalışmanın hazırlanma sürecinde bilimsel araştırma ve yayın etiği ilkelerine riayet edilmiş; yararlanılan tüm kaynaklar eksiksiz biçimde kaynakçada belirtilmiştir.

***Ethical Statement***

*The authors confirm that this study was conducted in accordance with the principles of academic research and publication ethics, and that all sources used are appropriately cited.*

**Etik Onay**

Bu çalışma, etik kurul izni gerektirmeyen nitelikte olup kullanılan veriler literatür taraması/yayınlanmış kaynaklar üzerinden elde edilmiştir.

***Ethical Approve***

*This study does not require ethical committee approval, and the data used were obtained through a literature review/published sources.*

## Referanslar/References

ABD Yüksek Mahkemesi. (2014). Riley v. California, No. 13-132. Erişim adresi: https://supreme.justia.com/cases/federal/us/573/13-132/case.pdf

Alvarez, J. (2015). Stuxnet: The world's first cyber weapon. Stanford Center for International Security and Cooperation. Erişim adresi: https://cisac.fsi.stanford.edu/news/stuxnet

Arendt, H. (1963). *Eichmann in Jerusalem: A Report on the Banality of Evil.* New York: Penguin.

Avrupa Parlamentosu (2014). Introductory statement by Edward Snowden submitted to the European Parliament's inquiry into the Electronic Mass Surveillance of EU Citizens. European Parliament. Erişim adresi: https://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf

BBC. (2024). Hizbullah'ın çağrı cihazlarının patlatılması: Hangi sorular yanıt buldu? Erişim adresi: https://www.bbc.com/turkce/articles/czj978p0w39o

Berkman Center (2016). Don't Panic Making Progress on the "Going Dark" Debate Erişim adresi: https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Berlinski, D. (2000). *The Advent of the Algorithm: The 300-Year Journey from an Idea to the Computer.* Houghton Mifflin Harcourt.

Blount, P. J. (2019). *Reprogramming the World: Cyberspace and the Geography of Global Order. E*-International Relations Publishing.

Borgwardt, E. (2005). *A New Deal for the World: America's Vision for Human Rights.* Cambridge, MA: Belknap.

Boschetti, N., Gordon, N. G. & Falco, G. (2022, October 24). Space Cybersecurity Lessons Learned from the ViaSat Cyberattack. *ASCEND 2022*. https://doi.org/10.2514/6.2022-4380

Bowman, G. W. (2007). Thinking Outside the Border: Homeland Security and the Forward Deployment of the US Border. *Houston Law Review*, 44(2): 189–251. Erişim adresi: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=921121

Castells, M. (2007). Communication, Power and Counter-Power in the Network Society. *International Journal of Communication*, 1(1): 238-266. Erişim adresi: https://ijoc.org/index.php/ijoc/article/view/46

Castells, M. (2010). *The rise of the network society.* Wiley-Blackwell.

Clapham, C. (1998). Degrees of Statehood. *Review of International Studies*, 24(2): 143–57.

Clinton, H. (2011). Internet Rights and Wrongs: Choices & Challenges in a Networked World remarks. U.S. Department of State. Erişim adresi: https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm

Cohen, J. E. (2008). Privacy, Visibility, Transparency, and Exposure. *The University of Chicago Law Review*, 181–201. Erişim adresi: https://scholarship.law.georgetown.edu/facpub/805/

Deleuze, G. & Guattari, F. (2015). *A thousand plateaus : capitalism and schizophrenia.* Bloomsbury.

DeNardis, L. (2014). *The Global War for Internet Governance.* New Haven: Yale University Press.

Dittmer, J. (2015). Everyday Diplomacy: UKUSA Intelligence Cooperation and Geopolitical Assemblages. *Annals of the Association of American Geographers*, 105(3), 604–619. https://doi.org/10.1080/00045608.2015.1015098

Domscheit-Berg, D. (2011). *Inside Wikileaks: My Time with Julian Assange at the World's Most Dangerous Website.* New York: Crown Publishers.

Fielder, J. D. (2013). "The Internet and Dissent in Authoritarian States," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, (Eds.) In Panayotis A. Yannakogeorgos & Adam B. Lowther, pp. 161-191. Boca Raton: Taylor & Francis.

Foucault, M. (1995). *Discipline and Punish: The Birth of the Prison.* New York: Vintage Books.

Gellman, B. & Poitras, L. (2013). U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret

Program. *The Washington Post.* Erişim adresi: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Greenberg, A. (2012). *This Machine Kills Secrets: How WikiLeakers, Cypherpunks and Hacktivists Aim to Free the World's Information.* New York: Dutton.

Greenwald, G. (2014a). NSA Collecting Phone Records of Millions of Verizon Customers Daily. *The Guardian.* Erişim adresi: http://www. theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G. (2014b). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York: Metropolitan Books.

Habermas, J. (2001). *The Postnational Constellation: Political Essays.* MIT Press.

Hopkins, N., Borger, J. & Harding, L. (2013). GCHQ: Inside the Top Secret World of Britain's Biggest Spy Agency. The Guardian. Erişim adresi: http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden

Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Scribner.

Lam, L. (2013). EXCLUSIVE: US Hacked Pacnet, Asia Pacific Fibre-Optic Network Operator, in 2009. South China Morning Post. Erişim adresi: http://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator

Lessig, L. (2004). *Free Culture : The Nature and Future of Creativity*. New York: Penguin Books.

Lessig, L. (2006). *Code 2.0.* Basic Books.

Michel, A. H. (2015). How Rogue Techies Armed the Predator, Almost Stopped 9/11, and Accidentally Invented Remote War. Wired. Erişim adresi: https://www.wired.com/2015/12/how-rogue-techies-armed-the-predator-almost-stopped-911-and-accidentally-invented-remote-war/

Moore, D. & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, 58(1): 7–38. https://doi.org/10.1080/00396338.2016.1142085

National Security Agency. (2013). PRISM/US-984XN Overview of the SIGAD Used Most in NSA Reporting Overview. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-055.pdf

O'Brien, J. (2019). Keeping Enigma Secret From The Germans– Many Lives Were Lost Sacrificed Doing So, War History Erişim adresi: https://www.warhistoryonline.com/instantarticles/times-allies-didnt-use-enigma.html

PCLOB. (2014). Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act. Erişim adresi: https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20(002).pdf

Poitras, L., Rosenbach, M. & Stark, H. (2013). NSA Spies on 500 Million German Data Connections. Spiegel Online. Erişim adresi:http://www.spiegel.de/international/germany/nsa-spies-on-500-million-german-data-connections-a-908648.html

Russon, M-A. (2021). ABD'de siber saldırı: Bilgisayar korsanları ülkenin en büyük boru hattını devre dışı bıraktı, akaryakıt karayoluyla taşınacak. BBC. Erişim adresi: https://www.bbc.com/turkce/haberler-dunya-57056048

Snowden, E. (2014). Testimony before the Parliament of the European Union. Erişim adresi: http://library.blountsfolly.com/space/items/show/171.

Soesanto, S. (2022). The IT Army of Ukraine Structure, Tasking, and Eco-System. CyberDefense Report. Erişim adresi: https://www.research-collection.ethz.ch/bitstreams/388e09e6-ce5e-4330-a284-13e873952f67/download

Svyrydenko, D. & Mozgin, W. (2022). Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia's War against Ukraine. Future Human Image, 17. https://doi.org/10.29202/fhi/17/6

Timberg, C. & Nakashima, E. (2013). Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance. The Washington Post. Erişim adresi: http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html

United Nations Security Council. (1960). S/RES/138 Question relating to the case of Adolf Eichmann. Erişim adresi: https://digitallibrary.un.org/record/112107?v=pdf

Zimmermann, P. R. (1995). *The Official PGP User's Guide*. MIT Press.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for The Future at the New Frontier Of Power.* Profile Books.