Turkish Journal of Security Studies

ISSN: 2148-6166 e-ISSN: 2757-7716
Volume: 28 Article Type: Research
Received: 01.08.2025 Accepted: 12.06.2026

Spatial Imagination of Cyberspace Security Challenges for Europe and Türkiye

Cansu Ulu[*]

Abstract
This article investigates the divergent spatial imaginations of cyberspace and their implications for the strategic partnership between the European Union (EU) and Türkiye. The research problem centers on how conflicting conceptualizations influence biliteral cooperation in an increasingly contested domain. Theoretically, the study employs a comparative framework between realism and liberalism, analyzed through Weaver's categorization of Westphalian versus scalar orientations. Using qualitative discourse analysis of primary policy documents and strategic frameworks, the research examines the layered structure of cyberspace and the diffusion of power toward non-state actors as a security problem. The findings reveal a significant ontological gap across four analytical dimensions: the definition of cyberspace, governance model, primary motivation, and spatial orientation. The EU prioritizes a liberal, scalar imagination focused on openness, fundamental rights, and value-based globalism, whereas Türkiye increasingly adopts a realist, Westphalian stance centered on national security, physical infrastructure, and sovereign control. This divergence is particularly pronounced in the treatment of non-state actors: while the EU incorporates them as co-regulators in a multi-stakeholder framework, Türkiye positions them primarily as objects of regulatory oversight or security risk. Although cooperation continues in technical areas such as cybercrime enforcement via the Budapest Convention, the iPROCEEDS initiative, and joint exercises through NATO's CCDCOE, these asymmetric spatial understandings create systemic barriers to deeper normative alignment. This study concludes that overcoming these barriers requires developing a shared spatial imagination of cyberspace as a foundation for sustainable cooperation in cyber governance.

Key Words: *Cyberspace, Cybersecurity, Spatial Imagination, EU-Türkiye Relations, Cyber Governance*

[*] Lecturer, PhD, ORCID: 0000-0002-3976-218X, Turkish National Police Academy, İzmir Rüştü Ünsal PVSHE, e-mail: cansu.ulu@pa.edu.tr

Güvenlik Çalışmaları Dergisi

ISSN: 2148-6166 e-ISSN: 2757-7716
Cilt: 28 Makale Türü: Araştırma
Makalenin Geliş Tarihi: 01.08.2025 Makalenin Kabul Tarihi: 12.06.2026

Siber Uzayın Mekansal Tahayyüllü Avrupa ve Türkiye İçin Güvenlik Sorunları

Cansu Ulu[*]

Öz

Bu makale, siber uzayın farklılaşan mekânsal tahayyüllerini ve bu tahayyüllerin Avrupa Birliği (AB) ile Türkiye arasındaki stratejik ilişki üzerindeki etkilerini incelemektedir. Araştırma problemi, birbirleriyle çatışan kavramsallaştırmaların, giderek daha rekabetçi hale gelen bu alandaki ikili iş birliğini nasıl etkilediği üzerine odaklanmaktadır. Teorik düzlemde çalışma, realizm ve liberalizm arasındaki karşılaştırmalı çerçeveyi Weaver'ın Westphaliacı ve scalar yönelimler kategorizasyonu aracılığıyla ele almaktadır. Birincil politika belgeleri ve stratejik dökümanlar üzerinde uygulanan nitel söylem analizi yöntemiyle siber uzayın katmanlı yapısı ve bir güvelik sorunu olarak gücün devlet dışı aktörlere yayılımı analiz ediliştir. Araştırma bulguları önemli bir ontolojik ayrışmayı ortaya koymaktadır. AB; açıklık, ekonomik fırsatlar ve liberal normların dağılımına dayalı scalar bir tahayyüle öncelik verirken, Türkiye toprak kontrolü ve ulusal güvenliği vurgulayan Westphaliacı bir perspektifi benimsemektedir. Her iki aktör de siber güvenlik ve siber suçlara mücadele konularında NATO bünyesinde CCDCOE gibi platformlar aracılığıyla iş birliğini sürdürmektedir. Diğer yandan Türkiye'deki yasal düzenlemeler ve siber uzaya karşı tutum, AB'nin liberal durusu ile sistemik gerilimler yaratmaktadır. Çalışma bu asimetrik mekânsal anlayışların siber yönetişimde derin bir uyumu engellediğini vurgulamakta ve sürdürülebilir bir işbirliği için ortak bir siber mekan tahayyülü geliştirilmesinin gerekliliğini savunmaktadır.

Anahtar kelimeler: *Siber Uzay, Siber Güvenlik, Mekânsal Tahayyül, Siber Yönetişim, Avrupa Birliği – Türkiye İlişkileri*

[*] Dr. Öğr. Gör., ORCID: 0000-0002-3976-218X, Polis Akademisi, İzmir Rüştü Ünsal PMYO, e-posta: cansu.ulu@pa.edu.tr

Introduction

The emergence of the internet and cyberspace has introduced a novel and under-theorized domain into international relations. Far from being merely a technical extension of the internet, cyberspace constitutes a socio-political space in which power, authority, and governance are negotiated among state and non-state actors. The cyber and physical worlds are analytically distinct yet empirically interconnected. Cyberspace embodies a duality of the physical and the virtual realms. This study approaches cyberspace through the concept of spatial imagination, understood as how political actors perceive, construct, and attribute meaning to space in relation to sovereignty, power, and control. Spatial imaginaries influence not only regulatory and security preferences but also patterns of cooperation and conflict in cyberspace. The existing literature has primarily examined cyber governance and cybersecurity from legal, technical, and strategic perspectives. This article examines how differing spatial imaginations shape interstate relations. This study analyzes how spatial imaginations of cyberspace shape the European Union–Türkiye relationship, particularly in the context of cyberterrorism and cybercrime. Spatial imaginations of cyberspace will be studied in terms of cyber actors, power, and territorial sovereignty.

There is no universal consensus among states regarding the conceptual and legal definition of cyberspace. The term cyberspace was first introduced in William Gibson's novel *Neuromancer*. Cyberspace is defined as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts" (Gibson, 1989, p. 128). This definition emphasizes the virtual nature and common characteristics of cyberspace. While Gibson emphasizes the experiential and virtual dimensions of cyberspace, Kuehl foregrounds its infrastructural and technological foundations. Kuehl defines cyberspace within the scope of information and communication technologies (ICTs).

> Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies. (Kuehl, 2009, p. 28).

Cyberspace is generally defined through information and communication technologies and is often used interchangeably with the internet. However, rather than being identical to the Internet, cyberspace constitutes a broader virtual domain that the Internet enables. In this sense, the Internet functions as an infrastructural tool that facilitates access to cyberspace. Specific features of cyberspace include temporality, physicality, permeation, fluidity, participation, attribution, and accountability (Choucri, 2013, p. 3). Cyberspace provides a virtual environment in

which social networks are constructed and, with the emergence of the metaverse, even parallel forms of reality can be produced. The evolution of the web has therefore contributed to the emergence of hyperreality that increasingly blurs the boundaries between the physical and the virtual worlds (Nunes, 1995). Web 1.0 introduced the Internet to users worldwide through web browsers and HTML, featuring static websites and content (Benhaddi, 2017). Web 2.0 is less technical and offers more social interaction to the users (Berners-Lee, 1998). Lessig (2006) highlights the difference between the Internet and cyberspace by labeling Web 2.0 as the Internet and Web 3.0 as cyberspace. Web 4.0 is characterized by artificial intelligence, machine-to-machine communication, big data, and cloud computing (Nedeva & Nideva, 2012).

The organizational principle of domestic politics is hierarchy. The state holds the legitimate monopoly over the use of force. On the contrary, there is no sovereign authority above the states, so international affairs are anarchic (Art & Jervis, 2015). Cyberspace changes the meaning of 'anarchy'. Cyberspace does not have territorial constraints. It has its own dynamic and power relations. Cyberspace includes numerous and diverse actors that can access power resources. Cyberspace is an unregulated virtual world where power diffuses from states to all levels of non-state actors (Nye, 2011, pp. 113-114). States cannot declare their sovereignty easily in cyberspace, and all levels of units exist in so-called cyber anarchy. According to Schmidt (1999), "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had". The sovereignty of cyberspace is shared between states and non-state actors. Blockchain technology, cryptocurrencies, and the Deep Web transcend borders and erode state sovereignty. The deep web is the secret gateway that opens to cyberspace. Deep Web contains dynamic web pages that cannot be indexed by traditional search engines. The Deep Web represents a form of cyber governance beyond government control. The Deep Web serves as a safe haven for criminal and terrorist organizations.

While there is broad agreement at the technical level, significant disagreements persist regarding how cyberspace is spatially conceptualized. This study primarily draws on Weaver's spatiality conceptualization of cyberspace. The European Union generally frames cyberspace as an open, global, and rule-based space aligned with liberal norms, economic integration, and multilateral governance. Türkiye has increasingly emphasized a security-oriented and state-centric approach to cyberspace, prioritizing national security, public order, and sovereign control. These differing orientations coexist with ongoing cooperation in areas such as cybersecurity and cyber governance, yet they also generate tensions and asymmetries in expectations and practices.

The article proceeds as follows: the next section conceptualizes cyberspace as a spatial domain and outlines the theoretical framework of spatial imagination. Subsequent sections examine the European Union's and Türkiye's approaches to

cyberspace governance, followed by a comparative analysis of their implications for bilateral relations. The conclusion discusses prospects for enhanced cooperation and shared governance in cyberspace.

The Spatiality of Cyberspace

"Spatial imagination is the process through which social groups work out the relation between social and physical phenomena." (Chattopadhyay, 2014). Spatial imagination is how the subject imagines physical aspects such as space, borders, and territory. Cyberspace is created by humans and evolves with interactions between humans, machines, and artificial intelligence. Different actors hold distinct spatial understandings of cyberspace.

Weaver categorized spatial orientation in the literature as Westphalian, scalar, and relational. The Westphalian orientation conceives space as a container of sovereignty, closely linked to power relations and territory. The scalar orientation foregrounds globalization and economic power relations and how local, regional, and global spaces are created. The relational orientation considers space as a reproduction of human interactions (Weaver, 2020).

The Westphalian orientation conceptualizes state actors as territorially and politically grounded entities. Sovereignty, power relations, and security are closely connected to the physical world, including borders, land, and space. The Westphalian system coordinates state and territory, making each state sovereign in the territory to which it lays claim (Howland & White, 2008). Spruyt (1996) highlights the connection between fixed territory and sovereignty. Territory as a physically identified base determines internal and external sovereignty (Crawford, 2012). Cyberspace does not have borders or fixed territory. Cyberspace contains "three layers (physical, logical, and social) made up of five components (geographic, physical network, logical network, cyber persona, and persona)" (The United States Army, 2010, p. 8). Cyberspace is understood to have a physical layer that operates through material infrastructure. Cyberspace hosts critical infrastructures. Attacks against the physical layer affect critical infrastructures. For this reason, states want to dominate the physical layer to protect their critical infrastructure. The most notable example of these attacks is Stuxnet. However, states cannot effectively regulate cyberspace by exercising their territorial sovereignty. Dependence on the physical layer is decreasing due to technological developments such as cloud computing. Westphalian orientation tends to consider cyberspace as an operational domain that needs to be regulated by states. The best examples of Westphalian orientation are the spatial understanding of Russia and China. Both actors seek to extend their sovereignty into cyberspace. China exports its norms pertaining to global governance to reshape the international order and promote "Internet sovereignty" (Zeng et al., 2017).

Scalar orientation focuses on globalization and the local, regional, and global levels. Physical borders are challenged by the force of globalization. The spatial imagination is represented as levels. Globalization is spanning borders, but the power relations are still connected and come to the forefront in a physical predetermined world. "Globalization does not discard borders and spaces but changes them." (Schroer, 2019, p.3). Friedman defines the evolution of globalization as corresponding with technological development. Every step of globalization is changing the spatial imagination. Globalization 1.0 started with the discovery of the American continent. Globalization 2.0, characterized by the Industrial Revolution and the rise of multinational companies, reduced barriers in global trade. In Globalization 3.0, with information and communication technologies, the world has shrunk like never before, and power relations have flattened (Friedman 2007, p. 10). Digital globalization becomes prominent; the McKinsey Report indicates that globalization is determined by cyber technologies (Manyika et al., 2016). Data transfer has a greater volume than goods and services. The cyberization rate affects the meaning of space. Levels of digital globalization represent the scalar degree of spatial imagination.

Scalar orientation examines cyberspace as global commons. It serves shared interests, and actors should ensure access in accordance with international norms, practice, and law. Cyberspace and space as global commons have both insufficient or ineffective international norms and laws (Barrett et al., 2011, p.6). The Tallinn Manual, the Budapest Convention on Cybercrime, the General Data Protection Regulation (GDPR), and reports of the UN Group of Governmental Experts are examples of attempts to establish international cyber norms. Demand for cyber norms is raised not only by states. Microsoft warns of the danger of state hegemony in cyberspace. Microsoft suggests that cyberspace needs a Digital Geneva Convention with stakeholders like governments, the technology sector, and civil society groups (Microsoft, 2022). Cyberspace is human-made, shaped by social relations and overarching logic through which humans design and structure it. The norms should consider both human activities and the dynamics of cyberspace. Cyberspace is not limited, so it cannot be mentioned in the tragedy of the commons. The norms and practices that aim to regulate cyberspace have a different motivation than to secure access and clean cyberspace for the security of netizens (Cambridge Dictionary, 2022).

Relational orientation questions the space itself and its reproduction. Relational orientation suggests that the space is not given but constructed (Rodgers, 2004, p.8). The works of Harvey and Lefebvre are examples of relational orientation. Space is a social term; actors and networks live within space and ascribe meaning to it. As Weinert argues, "Spatiality thus packages togather individualized and collective ascriptions of meaning and significance to places, and relational processes." (Weinert, 2017, p. 414). Spatial triad of Lefebvre provides a framework to analyze relational orientation of cyber spatiality (Lefebvre, 1991). The meaning

of cyberspace can be perceived by the object that live in cyberspace and this object can also conceive cyberspace. Notions, terms, and meanings shape cyberspace, and cyberspace in turn shapes objects and their relations. According to Harvey, "space is neither absolute, relative, or relational in itself, but it can become one or all simultaneously depending on the circumstances." (Harvey, 1973, p. 13). This argument is also suitable for cyberspace. Cyberspace has layers, and the spatiality of cyberspace is differentiated by which layer the actor considers.

The Deep Web is the most complex example of relational orientation. TOR was originally created by the U.S. Naval Research Laboratory for anonymous communication. The Deep Web is not a criminal space by nature, but it is reproduced by its users' relations. Recently, the Deep Web has been going darker due to the crackdown of government agencies on it (Weimann, 2016, p. 196). According to Berton (2015), the Islamic State of Iraq and the Levant (ISIL) carried out its activities on the Dark Web. The Surface Web can be easily monitored by government authorities, but the Dark Web has an anonymous veil. It represents an ideal ecosystem for financing terrorist activities, connection to followers, and procuring guns.

The Internet globalizes the world and reduces dependence on territory. Cyberspace coexists within the physical world but apart from it. As mentioned before, cyberspace has layers and components. Cyberspace cannot be defined solely as a social construction. Each spatial orientation corresponds to a different theoretical framework. Westphalian orientation aligns with the state-centric assumptions of realism; scalar orientation addresses spatial dimensions; and the neoliberal institutionalist perspective, along with the relational orientation, shares certain affinities with critical theories. We need to find the answers: "Is cyberspace a new form of territory? If so, what are its boundaries, and what are the limits of sovereignty over such territory?" (Douzet, 2014, p. 5). A state-centric view of cyberspace intends to extend territorial sovereignty to cyberspace. States aim to regulate cyberspace by establishing norms and institutions. On the other hand, marginalized groups like terrorist organizations are using cyberspace to establish self-defined relational spaces (Lekhi, 2000, p. 28). Different spatial imaginations of cyberspace offer different power relations. The gap between the cyberspatial imagination of the state-centric view and the non-state view creates both vulnerabilities and advantages.

Methodology

This study adopts a qualitative research design to investigate the diverging spatial imaginations of cyberspace within the EU and Türkiye, and their impact on bilateral governance. The primary method employed is qualitative discourse analysis, which is applied to official strategy papers, legal frameworks, and policy

documents. Unlike content analysis, which focuses on the frequency of terms, discourse analysis allows for a deep examination of the meaning and the socio-political reality constructed by political actors regarding sovereignty, power, and governance.

The dataset includes primary sources such as the EU's "Cybersecurity Strategy for the Digital Decade" and "The Cybersecurity Act", alongside Türkiye's National Cyber Security Strategy and Action Plans. By analyzing the linguistic choices and strategic priorities within these documents, the study identifies how the EU constructs a liberal scalar imagination focused on openness and economic integration, while Türkiye articulates a realist Westphalian stance prioritizing national security and territorial integration. This methodological approach enables a critical comparison of the ontological foundations that shape each actor's orientation toward cyber governance and highlights the systematic asymmetries in their cooperative efforts.

How the EU Imagine Cyberspace

The EU conceptualizes cyberspace through a liberal stance, prioritizing a multi-stakeholder governance model that emphasizes the protection of fundamental rights, the free flow of data, and the expansion of the digital single market beyond traditional borders. The EU's spatial imagination of cyberspace can best be described as predominantly scalar. However, this orientation is not static. In response to evolving security threats, the EU increasingly incorporates selective Westphalian elements, particularly in areas related to critical infrastructure protection, cybercrime, and hybrid threats. This hybrid configuration does not replace the scalar imagination; rather, it complements it.

In this chapter, regulations and strategy reports will be analyzed. This chapter aims to answer the following questions: How does the EU define cyberspace?' 'What is the main concern with regard to cybersecurity?', and 'How is the EU's vision of cyberspace being implemented?'. The EU aims to increase cyberization by 2050 (European Commission, 2022a). The EU appreciates the importance of cyberspace, taking into consideration that it covers different sectors, actors, and social relations. Cyberspace is unlimited, and cyber capabilities are increasing while technology is evolving. This gives huge advantages to the actor who can use it. However, cyberspace offers the same advantages to malicious actors.

The EU consistently promotes a vision of cyberspace as a global, open, and borderless domain. This vision is grounded in the belief that cyberspace functions as a force multiplier for economic development, democratic participation, and societal connectivity. The Cybersecurity Act explicitly acknowledges the borderless nature of cyberspace, aligning with Choucri's emphasis on its permeability and transboundary character (Cybersecurity Act, 2019). Cyberspace

is increasingly framed as a virtual global common that penetrates all sectors of society, including economic activity, democratic processes, and social relations. At the same time, the EU recognizes that cyberspace is unevenly regulated and exposed to continuously evolving security threats. As stated in the Cyber Diplomacy Toolbox, "cyberspace offers significant opportunities, but also poses continuously evolving challenges for the EU" (Cyber Diplomacy Toolbox, 2017, p. 3).

From a security perspective, the EU identifies two broad categories of cyber threats. The first concerns challenges to the openness and integrity of the global Internet. Restrictions on Internet access and the fragmentation of cyberspace through digital borders are framed as security risks that undermine the EU's vision of an open digital environment (The EU's Cybersecurity Strategy for the Digital Decade, 2020). National approaches within the EU illustrate this tension. Germany's position paper on the application of international law in cyberspace rejects the notion of independent "cyber borders" detached from physical territory, reaffirming the territorial scope of state sovereignty in cyberspace (The Federal Government, 2021, p. 3). France's National Digital Security Strategy similarly emphasizes a safe, stable, and open cyberspace, while highlighting European strategic autonomy and the use of cyberspace as an instrument of soft power. France's vision of making Europe a digital territory that respects fundamental rights underscores the normative dimension of the EU's cyber imagination (Premier Ministre, 2015, p. 39).

The EU's Cybersecurity Strategy for the Digital Decade conceptualizes the Internet as a decentralized architecture governed through a multi-stakeholder model rather than centralized authority (The EU's Cybersecurity Strategy for the Digital Decade, 2020, p. 2). While Member States retain national cybersecurity strategies, the European Commission seeks to harmonize regulatory frameworks to prevent geopolitical fragmentation and digital protectionism. The Commission explicitly calls for strengthening European digital sovereignty through standard-setting in data, technology, and infrastructure governance (European Commission, 2022a). This approach reflects a scalar imagination in which cyberspace is governed through layered authority structures involving EU institutions, Member States, private actors, and civil society.

Economic considerations constitute a core dimension of the EU's spatial imagination of cyberspace. Cyberspace is viewed as an economic force multiplier essential to security, democracy, and societal resilience. The Cybersecurity Strategy opens by asserting that cybersecurity is integral to Europeans' security, linking digital stability directly to economic prosperity (The EU's Cybersecurity Strategy for the Digital Decade, 2020, p. 1). Regulatory instruments such as Regulation (EU) No. 2019/881 define network and information systems as the backbone of economic growth and societal development, likening digital infrastructure to critical utilities such as electricity and water supplies (Cybersecurity Act, 2019).

Within this framework, the Digital Services Act (DSA) and the Digital Markets Act (DMA) play a central role in embedding European values into cyberspace governance. As part of the "Shaping Europe's Digital Future" agenda, these instruments aim to create a safer digital environment while fostering fair competition and innovation in the Single Market (European Commission, 2022b). Their dual objectives—protecting fundamental rights and ensuring a level playing field—align with the EU's broader vision for cyberspace. Public consultations on the DSA reveal widespread concern regarding illegal content and goods online, reinforcing demands for platform transparency and effective regulatory oversight (European Commission, 2020).

Beyond economic regulation, the EU frames cyberspace as a normative and rights-based space. The European Declaration on Digital Rights and Principles for the Digital Decade articulates cyberspace as a social domain grounded in human dignity, fundamental rights, and democratic values. This declaration reinforces the EU's conceptualization of cyberspace not merely as infrastructure, but as a societal space requiring ethical and legal safeguards (European Commission, 2022c). The General Data Protection Regulation (GDPR) exemplifies this approach by harmonizing data protection standards across the EU and enhancing user awareness of personal data use (Herrle & Hirsh, 2019). Complementary initiatives such as the Action Plan on Disinformation and the Code of Practice on Disinformation further demonstrate the EU's commitment to protecting democratic processes in the digital sphere.

Institutionally, agencies such as ENISA and initiatives like the Joint Cyber Unit operationalize the EU's cyber governance framework. ENISA, strengthened by the EU Cybersecurity Act, promotes a high common level of cybersecurity through certification schemes and policy coordination (ENISA, 2022). The Joint Cyber Unit facilitates cooperation among EU institutions, Member States, and relevant stakeholders, enhancing collective responses to cyber threats and malicious activities, including cybercrime and cyberterrorism (European Commission, 2022d). These mechanisms reflect the EU's preference for coordinated multilevel governance rather than centralized control.

The EU shares some aspects of NATO's view of cyberspace, but the EU has a more social and scalar view. Ahmad (2020) analyzes the discourse of the EU about cyberspace and cybersecurity. The findings of the study show that the EU has a holistic approach to cyberspace, "ensuring both the protection of the state, but also the protection of the individual from external actors and potential state infringements on these fundamental rights" (Ahmad, 2020, p. 19). The Budapest Convention is an example of the holistic approach. This convention is the first international regulation that deals specifically with copyright violations, computer fraud, child pornography, and network security violations committed over the Internet and other computer networks (Council of Europe, 2021). The Budapest Convention focuses on cybercrime. The convention aims to achieve unity among

the members of the Council of Europe. It also recognized the value of fostering cooperation among member states. The need for a common criminal policy was stressed in the document (Council of Europe, 2001).

While the EU's spatial imagination of cyberspace remains predominantly scalar, recent strategic documents reveal the incorporation of selective security-oriented elements. The EU Cyber Defence Policy and the Strategic Compass for Security and Defence acknowledge cyberspace as a contested domain requiring enhanced resilience and defense cooperation, particularly in response to hybrid threats (Council of the EU, 2022; European Commission, 2013). Nevertheless, unlike NATO's explicit recognition of cyberspace as an operational military domain, the EU continues to emphasize civilian, regulatory, and normative dimensions. Cooperation with NATO, reflected in joint declarations and alignment with non-binding frameworks such as the Tallinn Manual, illustrates a complementary rather than fully militarized approach to cyberspace governance (Schmitt, 2013; NATO, 2018).

Among the European Union's recent regulatory efforts, the Artificial Intelligence Act (AI Act) stands out as a key legal instrument aimed at shaping the governance of artificial intelligence. More importantly, the AI Act reveals the EU's spatial orientation toward cyberspace by framing digitally mediated environments as extensions of its internal regulatory and security space. The AI Act seeks to impose normative boundaries on the use of artificial intelligence in areas such as border management, law enforcement, and the prevention of serious crime. This regulatory logic treats cyberspace not as a detached virtual realm but as an extension of the EU's internal security space, where digital tools are expected to align with fundamental rights, accountability mechanisms, and centralized oversight (Regulation (EU) 2024/1689, 2024).

Overall, the EU conceptualizes cyberspace as a borderless, open, and globally interconnected domain governed through multilevel regulation, economic integration, and normative standards. Although security concerns have prompted limited securitization, these measures coexist with a broader scalar imagination that prioritizes openness, rights protection, and international cooperation. This hybrid configuration shapes the EU's cyber diplomacy and its engagement with international partners, reinforcing a vision of cyberspace grounded in shared norms rather than exclusive territorial control.

Türkiye's Spatial Orientation of Cyberspace in Comparison with the EU

Türkiye adopts a realist approach perceiving cyberspace as a sovereign domain where national security, physical infrastructure integrity, and state-centric legislative control are paramount to countering hybrid threats. These threats are getting more attention because of the diffusion of power from non-state actors. Türkiye defines cyberspace as "All systems and services directly or indirectly

connected to the internet, telecommunication and computer networks" (*National Cyber Security Strategy 2020-2023,* 2020, p. 9). Türkiye recognizes the importance of digitalization, as economic relations and globalization necessitate robust cyber policies. Türkiye tends to interpret cyberspace as a potentially unregulated domain vulnerable to criminal activities, disinformation, and threats to national security. Compared to the EU, Türkiye's spatial orientation is closer to a Westphalian approach, prioritizing sovereignty, territorial control, and the protection of national interests.

President Erdoğan emphasizes extending national sovereignty to cyberspace, asserting that Türkiye will defend sovereign rights across all domains, "from the Blue Homeland to cyberspace" (Bilgi Teknolojileri ve İletişim Kurumu, 2020a). Ömer Abdullah Karagözoğlu, Chairman of the Information Technologies and Communications Authority, stated that Türkiye continues to strengthen information security, enhance cyber defense, protect critical infrastructure, and safeguard personal and national data (Bilgi Teknolojileri ve İletişim Kurumu, 2020b).

The motivation behind Türkiye's policies and regulations is twofold: developing adequate legal frameworks for cyberspace and digitally transforming institutional capacities and enhancing cyber security while countering disinformation. In this context, Turkish regulations in informatics have largely aligned with EU directives. Articles 243–246 of the Turkish Penal Code No. 5237 regulate cybercrimes, in parallel with Articles 4 and 5 of the Budapest Convention.

Institutional adaptation of cyber technologies is also central to Türkiye's approach. The Procedures and Principles Regarding Secure Internet Service (2011) aimed to provide a safe and predictable Internet environment for users and service providers, referencing the Council of Europe Convention on Cybercrime (Bilgi Teknolojileri ve İletişim Kurumu, 2022). In 2018, the Digital Transformation Office was established to unify digital transformation efforts across institutions and centralize studies on cyber security, national technologies, big data, and artificial intelligence. This step mirrors the multi-stakeholder cyber governance approach of the EU while maintaining a strong focus on national security. The Turkish Cyber Security Cluster was established to integrate state, private sector, and academic actors, with the goal of developing domestic cyber security technologies, including national software, hardware, and critical systems. Investments in domestic UAVs/UCAVs technologies further reinforce Türkiye's emphasis on technological sovereignty and cyber operational capability.

Cyberspace is both a domain for asserting sovereignty and a social arena. Security in cyberspace is essential for national security. Both the EU and Türkiye identify three primary cyber threats: cyber operations threatening territorial integrity, cyberattacks targeting critical infrastructure, and cybercrimes affecting social networks, financial systems, and human rights. Türkiye harmonizes legal procedures with the EU to address cyber threats. Compliance with the Budapest Convention and GDPR ensures alignment in cyber governance, facilitating joint

actions against cybercrime. Projects like iPROCEEDS, a joint EU and Council of Europe initiative, enhance inter-organizational and international cooperation, with workshops on Darknet activities, virtual currencies, cybercrime investigation, and electronic evidence handling (iPROCEEDS, 2019; Türkiye Adalet Akademisi Strateji & Arge, 2021; Ceza İşleri Genel Müdürlüğü, 2022).

Under NATO's umbrella, Türkiye collaborates with the EU on cyber policies. The 2010 Lisbon Summit identified cyber threats and outlined countermeasures, followed by the 2011 "Revised NATO Cyber Defense Policy" and the "Cyber Defense Action Plan" for coordinated responses across member states (NATO, 2010; NATO, 2011). The NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) serves as a hub where Turkish and European experts, including HAVELSAN, conduct joint exercises such as Locked Shields to test cyber resilience and interoperability (CCDCOE, 2022).

In the Action Plan of the National Cyber Security Strategy, eight steps have been defined to ensure the security of Türkiye's cyberspace. The protection of critical infrastructure, the development of national cyber capacity, the fight against cybercrime, developing and supporting domestic and national technologies, security of the new generation technologies, cyber security network, integration between cyber security and national security, and international cooperation are the steps of the Action Plan (*National Cyber Security Strategy 2020-2023*, 2020, p. 32-33). In the Action Plan, a strong emphasis was placed on national capabilities and national security.

Türkiye's National Cyber Security Strategy and Action Plan (2024–2028) further clarifies its spatial orientation. The strategy emphasizes that "the protection of the assets of institutions, organizations, and users in cyberspace is among the highest priorities of states and institutions," and recognizes that cybersecurity transcends purely technical measures, becoming part of national and international security strategies. Structured around the themes of "Human," "Defense," "Deterrence," and "Cooperation," the strategy articulates strategic objectives aimed at enhancing cyber resilience, institutionalizing proactive defense and deterrence mechanisms, ensuring the secure use of technology, reinforcing Türkiye's international digital standing, fostering domestic technological capacity for cyber threat mitigation, and advancing a human centric cybersecurity framework. (Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı, 2024).

Additionally, Türkiye's National Artificial Intelligence Strategy (NAIS) 2021–2025 complements its cyber orientation. The vision of NAIS is creating value on a global scale through an agile and sustainable AI ecosystem for a prosperous Türkiye, reflecting strategic priorities informed by national policies, sectoral strategies, and international benchmarking (*National Artificial Intelligence Strategy 2021-2025*, 2021). This strategy strengthens Türkiye's position at the intersection of AI and cyberspace, highlighting the country's focus on both sovereign capabilities and global technological integration.

On the legal side, Türkiye has aligned its domestic frameworks with EU directives. The Personal Data Protection Law (KVKK, 2016) predates the GDPR but is largely compatible with it, protecting personal data and fundamental rights. A recent parliamentary proposal to prevent disinformation and ensure a safe Internet references the EU's DSA, DMA, and GDPR, emphasizing cross-border challenges posed by anonymity and unregulated online sharing (TBMM, 2022).

Non-State Actors: Governance Partners vs. Security Threats

A critical dimension where the EU and Türkiye's spatial orientations diverge most sharply is their approach to non-state actors in cyberspace. The EU, operating from a scalar imagination, integrates non-state actors — including technology companies, civil society organizations, and academic institutions — as legitimate stakeholders in multi-level cyber governance. This is institutionally reflected in the Budapest Convention's multi-stakeholder rationale and in the EU's Digital Services Act, which assigns co-regulatory responsibilities to platforms. By contrast, Türkiye's Westphalian orientation treats non-state actors primarily as objects of regulation or potential sources of risk rather than as governance partners. Both actors recognize the security threat posed by malicious non-state actors, including criminal networks operating on the Dark Web, ransomware groups, and terrorist organizations such as ISIL that exploit the anonymity of the Tor network for financing and recruitment. However, their responses differ structurally: the EU prioritizes cross-border legal harmonization and platform transparency to constrain such actors, while Türkiye emphasizes sovereign enforcement capacity and infrastructure control. This asymmetry means that joint operations against transnational cybercrime — for instance, through the iPROCEEDS project — remain effective at the technical level, but broader normative convergence on the role of non-state actors in cyber governance remains elusive.

A deeper examination of the power diffusion dynamic reveals that the EU and Türkiye not only differ in how they govern non-state actors but also in how they theorize the spatial orientation that these actors hold. Nye's (2011) concept of cyber power explicitly identifies the diffusion of power from states to non-state actors as a defining feature of the digital age, one that disrupts traditional hierarchies of authority and creates new asymmetries in international relations. The EU incorporates this reality into its governance architecture by design: the recognition that no single state can unilaterally regulate a borderless domain underpins the multi-stakeholder model and explains the EU's investment in international norm-setting forums such as the Internet Governance Forum and the Global Forum on Cyber Expertise. Türkiye's response to the same dynamic is structurally inverse. The diffusion of power toward non-state actors — whether toward criminal networks exploiting the Dark Web, disinformation actors

operating across social media platforms, or foreign technology firms mediating critical communications infrastructure — is framed primarily as a sovereignty deficit requiring legal remedy. The Internet Law's requirement that large platforms appoint local representatives, store data on Turkish servers, and comply with content removal orders reflects a deliberate attempt to re-territorialize power that has diffused beyond state reach (İnternet Ortamında Yapılan Yayınların Düzenlenmesi, 2020). The practical consequence of this divergence is that the two sides approach the same problem from incompatible starting assumptions about who legitimate governance actors are.

Conclusion

Türkiye and the EU have different spatial orientations in their understanding of cyberspace. Cyberspace is a virtual realm. Cyberspace has a physical layer, and it is connected to infrastructure beyond national borders. However, cyberspace cannot be described in terms of physical layers. Cyber technologies possess material and physical components; however, encryption, cloud computing, and social networks contribute to the construction of a global, abstract, and borderless digital sphere. Cyberspace has different characteristics compared to other global commons. It is human-made and limitless. Space and cyberspace are two domains that lack comprehensive international norms and regulations. Cyberspace offers great opportunities because of its multiplier effect; on the other hand, the same opportunities can be used by malicious actors. Cyberspace changes power relations. It is now diffused to non-state actors. In particular, the Deep Web and Dark Web function as an incubator for criminal and terrorist activities.

The EU is aware of the possibilities of cyberspace. It deals with cyberspace, especially within the framework of globalization and the economy. The EU's vision is open, global, and secure cyberspace. According to the EU, open and global cyberspace will both increase economic resources and offer unlimited opportunities to spread European values. Türkiye's imagination of cyberspace is shaped mostly within the framework of security. Türkiye does not have a Westphalian orientation as much as China and Russia. It has been observed that Türkiye acts in harmony with the EU in legal arrangements regarding cyberspace. However, the motivations of the two sides in regulating cyberspace differ. This difference between Türkiye and the EU has political and economic reasons and consequences. However, this could be the subject of another study. Türkiye acts with a more realist and security-first perspective. It was stated that the last law proposal and the Internet Law were attempts to dominate the cyberspace and Article 29 harmed the freedom of expression (Dülger & Özkan, 2021; Görgülü, 2022).

Table 1. Comparative Spatial Orientations of Türkiye and the EU in Cyberspace Governance

Analytical Dimension	**EU**	**Türkiye**
Ontological view of cyberspace	Global & open	Global & Security oriented
Primary motivation	Economic integration & norm diffusion	Resilience & Security
Governance model	Multi-stakeholder	State supported private enterprise
Spatial Orientation	Scalar	Westphalian

Table 1 systematizes the core findings of this study. It demonstrates that the difference between the EU and Türkiye stems not only from policy choices, but from different spatial imaginations and normative foundations regarding cyberspace. In doing so, it makes visible the underlying theoretical assumptions shaping each actor's approach to cyber governance. The comparative data presented in the table serves as a visual representation of this asymmetric alignment. The table clearly demonstrates that the divide is not merely technical but ontological; as long as the EU maintains a scalar orientation and Türkiye pursues a Westphalian one, the partnership will likely remain transactional rather than transformational. Since cyberspace is still an evolving domain without norms and clearly defined boundaries, the orientations identified in this study cannot be evaluated in normative terms. Instead, they should be examined according to their compatibility with the respective strategic priorities of each actor.

The first analytical dimension — the ontological view of cyberspace — reveals a foundational divergence in how each actor conceptualizes the domain itself. The EU treats cyberspace as a global and open commons, a borderless extension of democratic society where the free flow of information, economic integration, and norm diffusion are primary concerns. This is institutionally reflected in frameworks such as the EU Cybersecurity Strategy, the Digital Single Market, and the European Declaration on Digital Rights and Principles. Türkiye, by contrast, views cyberspace as a global but security-oriented domain, one that is inherently contested and vulnerable to sovereign intrusion. Official statements by senior Turkish officials, which frame cyber defense as an extension of the "Blue Homeland" doctrine, illustrate that while Türkiye acknowledges cyberspace's global character, it filters this recognition through a national security lens (Directorate of Communications, Republic of Türkiye, 2020). This ontological divergence is not merely semantic; it shapes the entire normative architecture each actor builds around cyber governance.

The second dimension — primary motivation — further clarifies how each actor translates its ontological view into strategic priorities. The EU's primary motivation is economic integration and norm diffusion: it aims to create a unified digital market, export its regulatory standards globally (the so-called 'Brussels Effect') (Bradford, 2021), and embed liberal democratic values into the architecture of cyberspace. The GDPR, DSA, and the NIS2 Directive all serve this dual function of internal market harmonization and external normative projection. Türkiye's primary motivation, conversely, centers on resilience and security: the National Cyber Security Strategy 2024-2028 explicitly structures its goals around deterrence, defense, and domestic technological capacity. These motivations are not inherently incompatible, but the underlying logic differs significantly. The EU securitizes cyberspace insofar as threats undermine liberal norms; Türkiye securitizes cyberspace as a domain of sovereign competition. This motivational asymmetry explains why cooperation remains easier at the technical-operational level than at the policy or legislative level.

The third dimension — governance model — operationalizes these motivations into institutional arrangements. The EU adopts a multi-stakeholder model in which governments, private sector actors, civil society, and academic institutions collectively participate in shaping cyber policy. ENISA, the Joint Cyber Unit, and the Budapest Convention framework all embody this distributed authority structure. Türkiye's model is better described as state-supported private enterprise: the Turkish Cyber Security Cluster formally integrates private and academic actors, but ultimate coordination authority resides with the state through the Digital Transformation Office and the BTK. This distinction is consequential for bilateral cooperation because it creates structural asymmetries in decision-making: EU cyber policy emerges from a pluralistic deliberative process, while Türkiye's approach is more vertically organized. Joint initiatives therefore require bridging not only policy preferences but fundamentally different governance architectures, which increases transaction costs and reduces the depth of alignment achievable.

The fourth dimension — spatial orientation — synthesizes the preceding three into a coherent theoretical framework. The EU's scalar orientation means that cyberspace is understood as a multi-level, trans-boundary domain in which authority is distributed across local, national, regional, and global scales simultaneously. Power, in this view, is not exclusively territorial but is exercised through norms, standards, and network effects. Türkiye's Westphalian orientation, by contrast, reasserts the primacy of the territorial state in cyber governance: authority is bounded by national jurisdiction, and sovereignty over physical infrastructure is treated as a precondition for meaningful security. This spatial divergence is the root cause of the systemic asymmetries identified throughout this study. It means that the two actors are not simply disagreeing about policy details but are operating within different geopolitical imaginations of what cyberspace fundamentally is. If this foundational divergence persists, EU-Türkiye

cyber cooperation will remain confined to functional domains where immediate threat-sharing interests override deeper normative disagreements.

Although the EU and Türkiye have different orientations, they continue to cooperate in certain areas to accomplish their strategic security goals. The primary areas of cooperation are concentrated in the functional and technical spheres. Both actors find common ground in combating cybercrime and enhancing collective defense mechanisms through multilateral platforms such as NATO's CCDCOE. These collaborative efforts are driven by a shared recognition of common threats that transcend national borders, such as large-scale DDoS attacks and organized cyber-espionage. When the focus is on operational resilience, the EU's liberal-scalar approach and Türkiye's security-oriented stance converge on the necessity of technical interoperability.

The divergence of spatial imaginations, however, becomes prominent in the normative and legislative spheres. The table illustrates that the EU's emphasis on the protection of fundamental rights and the free flow of data increasingly clashes with Türkiye's Westphalian-centered legislation. While the EU views cyberspace as a global common that requires a scalar, multi-stakeholder governance model, Türkiye's strategic discourse treats it as a sovereign territory requiring strict state control. This shift toward digital borders in Turkish policy creates a systemic barrier to deeper integration with the EU's digital single market norms. This situation may create tension between the EU and Türkiye.

On the other hand, the malicious actors operating on the dark web have a relational orientation. Different orientations bring about different uses of cyberspace. An actor adopting relational orientation in cyberspace may be difficult for a Westphalian-oriented actor to comprehend, potentially resulting in asymmetric relations. Meeting of Türkiye and the EU in a similar cyberspace spatial imagination will make it easier for both sides to solve security problems. With a normative perspective, the EU and Türkiye should strengthen cyber governance. Türkiye's gradual shift toward a Westphalian orientation may narrow the scope of cooperation. Cooperation between the EU and Türkiye on data security and the fight against cybercrime should expand to other areas. Türkiye and EU member states conduct joint operations under the NATO umbrella. The multi-stakeholder cyber-governance platform, such as CCDCOE, which covers areas other than cybersecurity, can serve as an initiative to increase collaboration.

References

Ahmad, N. (2020). *Brave new world: NATO, the EU and the new age of cyberspace* [Master's thesis, University of Oslo].

Art, R.J. & Jervis, R. (2015). *International politics: Enduring concepts and contemporary issues*. Pearson.

Barrett, M., Bedford, D., Skinner, E. & Vergles, E. (2011). *Assured access to the global commons*. North Atlantic Treaty Organization.

Benhaddi, M. (2017). Web of goals: A proposal for a new highly smart web. *Proceedings of the 19th international conference on enterprise information systems*, 26-29 April, 687-694.

Berners-Lee, T. (1998, July 5). *The world wide web: A very short personal history.* W3. https://www.w3.org/People/Berners-Lee/ShortHistory.html.

Berton, B. (2015, May 12). *The dark side of the web: ISIL's one-stop shop?*. European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf

Bilgi Teknolojileri ve İletişim Kurumu. (2020a). *Ulusal siber güvenlik stratejisi ve eylem planı görüşüldü.* https://www.btk.gov.tr/haberler/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-gorusuldu

Bilgi Teknolojileri ve İletişim Kurumu. (2020b). *2020-2023 Siber güvenlik stratejileri BTK'da belirlendi*. https://www.btk.gov.tr/haberler/2020-2023-siber-guvenlik-stratejileri-btk-da-belirlendi

Bilgi Teknolojileri ve İletişim Kurumu. (2022). *Güvenli internet hizmeti*. https://internet.btk.gov.tr/guvenli-internet-hizmeti.

Bradford, A. (2021). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Cambridge Dictionary. (2022). *Netizen*. https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/netizen

CCDCOE. (2022). *Locked shields*. https://ccdcoe.org/exercises/locked-shields/

Ceza İşleri Genel Müdürlüğü. (2022). *Iproceeds-2 projesi kapsamında 11-13 Mayıs 2022 tarihlerinde Ankara'da "Darknet, sanal para ve mali araştırma" konusunda eğitim düzenlendi*. https://cigm.adalet.gov.tr/Home/SayfaDetay/iPROCEEDS-2%20E%C4%9Fitimi

Chattopadhyay, S. (2014, January). *Architectural history and spatial imagination.* Perspectives On History. https://www.historians.org/publications-and-directories/perspectives-on-history/january-2014/architectural-history-and-spatial-imagination#:~:text=Spatial%20imagination%20is%20the%20process,dimensions%20of%20iidea%20and%20ideals

Choucri, N. (2013, October 13-15). *Co-Evolution of cyberspace and international relations: New challenges for the social sciences.* The World Social Science Forum (WSSF) 2013, Montreal, Canada.

Council of Europe. (2001). *Convention on cybercrime.* No.185, https://rm.coe.int/1680081561

Crawford, J.R. (2012). *Brownlie's principles of public international law*. 8th edn. Oxford University Press.

Cyber Diplomacy Toolbox. (2017). *Draft council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ("Cyber Diplomacy Toolbox").* Council of the European Union. No: 9916/17.

Cybersecurity Act. (2019). *Regulation (EU) 2019/881 of the European Parliament and of the council of 17 April 2019 on ENISA (The European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU).* No 526/2013. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG

Directorate of Communications. (2020, 26 December). *We will defend our sovereign rights in every area from the blue homeland to cyberspace*. https://www.iletisim.gov.tr/english/haberler/detay/we-will-defend-our-sovereign-rights-in-every-area-from-the-blue-homeland-to-cyberspace

Douzet, F. (2014). Understanding cyberspace with geopolitics. *Hérodote*. 152-153, 3-21.

Dülger, M.V & Özkan, O. (2021). *Sosyal medya yasası meclis'ten geçti: Peki, şimdi? (Social media law passed by parliament: Now what?).* SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792394

ENISA. (2022). *About ENISA – The European Union Agency for cybersecurity towards a trusted and cyber secure Europe*. https://www.enisa.europa.eu/about-enisa

European Commission. (2013). *EU cybersecurity plan to protect open internet and online freedom and opportunity* (2013). https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94

European Commission. (2020). *Summary report on the open public consultation on the digital services act package*. https://digital-strategy.ec.europa.eu/en/summary-report-open-public-consultation-digital-services-act-package

European Commission. (2022a). *A Europe fit for the digital age*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

European Commission. (2022b). *Shaping Europe's digital future.* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

European Commission. (2022c). *European declaration on digital rights and principles.* https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

European Commission. (2022d). *Joint cyber unit*. https://digital strategy.ec.europa.eu/en/policies/joint-cyber-unit.

Friedman, T.L. (2007). *The world is flat: A brief history of twenty-first century*. Picador/Farrar, Straus and Giroux.

Gibson, W. (1989). *Neuromancer*. Berkley Publishing Group.

Görgülü, E. (2022, June 18). *Binlerce kişi yargılanma ile karşı karşıya kalacak.* DW.https://www.dw.com/tr/yaman-akdeniz-dezenformasyon-yasas%C4%B1-ile-binlerce-ki%C5%9Fi-yarg%C4%B1lanma-ile-kar%C5%9F%C4%B1-kar%C5%9F%C4%B1ya-kalacak/a-62176388

Harvey, D. (1973). *Social justice and the city*. Blackwell Publishing.

Herrle, J. & Hirsh, J. (2019). *The peril and potential of the GDPR*, Centre for International Governance Innovatio. https://www.cigionline.org/articles/peril-and-potential gdpr/?utm_source=google_ads&utm_medium=grant&gclid=Cj0KCQiAmKiQBhClARIsAKtSj-lOhlnLZcMOHqzBcc7KDULTrbu7h47IIxawSr1Z3k9ByjLmcZmFPdAaAmjcEALw_wcB

Howland, D. & White, L. (2008). Introduction: Sovereignty and the study of states. In D. Howland & L. White (Eds.), *The state of sovereignty: Territories, laws, populations* (pp. 1-18). Indiana University Press.

Iproceeds. (2019). Cooperation on cybercrime under the instrument of Pre-Accession (IPA): Project on Targeting Crime Proceeds on the internet in South-Eastern Europe and Turkiye. *Joint Project of the European Union (IPA II Multi-Country Action Programme 2014) and Council of Europe*. https://rm.coe.int/3156-iproceeds-summary-v5/

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun (2020). No. 7253 *Resmî Gazete* (No: 31202). https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm

Kuehl, D.T. (2009). Cyberspace to cyberpower: Defining the problem. F.D. Kramer, S.S. Stuart & K. W. Larry (Ed.), *Cyberpower and national security* (pp. 24-42). National Defence University Press.

Lefebvre, H. (1991). *The production of space*. Translated by Nicholson-Smith, D. Blackwell.

Lekhi, R. (2000). The politics of African America on-line. In P. Ferdinand (Ed.), *The internet, democracy and democratization* (pp. 76-101) Frank Cass.

Lessig, L. (2006). *Code Version 2*. Basic Books.

Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov & K., Dhingra, D. (2016). *Digital globalization: The new era of global flows.* Mckinsey & Company. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/ouo%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.ashx

Microsoft. (2022). *A digital Geneva Convention to protect cyberspace*. https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

National Artificial Intelligence Strategy 2021-2025. (2021, August), https://wp.oecd.ai/app/uploads/2021/12/Turkey_National_Artificial_Intelligence_Strategy_2021-2025.pdf#page=17.09

NATO. (2010). *Lisbon summit declaration.* https://www.nato.int/cps/en/natolive/official_texts_68828.htm

NATO. (2011). *Defending the networks the NATO policy on cyber defence*. https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

NATO. (2018). *Joint declaration on EU-NATO cooperation.* https://www.nato.int/cps/en/natohq/official_texts_156626.htm

Nedeva, V. & Nideva, S. (2012). New learning innovations with Web 4.0. In M. Vlada, G. Albeanu, D. M. Popovici (Eds.), *Virtual learning – Virtual reality, proceedings of the 7th international conference on virtual learning (ICVL)* (pp. 316-321). Bucharest University Press.

Nunes, M. (1995). Jean Baudrillard in cyberspace: Internet, virtuality, and postmodernity, *Style*, *29*(2), 314-327.

Nye, J.S. (2011). *The future of power*. Public Affairs.

Premier Ministre. (2015). *The French national digital security strategy.* https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Republic of Turkiye Ministry of Transport and Infrastructure. (2020). National cyber security strategy 2020-2023. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/national-cyber-security-strategy-2020-2023.pdf

Rodgers, J. (2004). *Spatializing international politics: Analysing activism on the internet*. Routledge.

Schmidt, E. (1999). *Oxford essential quotations*. https://www.oxfordreference.com/view/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00017947

Schmitt, M.N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Schroer, M. (2019). Spatial theories / Social construction of spaces. In A.M. Orum (Ed.), *The Wiley-Blackwell encyclopedia of urban and regional studies*. vol.5, Wiley-Blackwell.

Spruyt, H. (1996). *The sovereign state and its competitors: An analysis of systems change.* Princeton University Press.

TBMM. (2022). *Basın kanunu ile bazı kanunlarda değişiklik yapılmasına dair kanun teklifi*. http://www.tbmm.gov.tr/Yasama/Kanun-Teklifleri-Sonuc

The Federal Government. (2021). *On the Application of International Law in Cyberspace.* https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

The United States Army. (2010). *Cyberspace operations concept capability plan 2016-2028.* https://irp.fas.org/doddir/army/pam525-7-8.pdf

Türkiye Adalet Akademisi Strateji & Arge (2021). *Güneydoğu Avrupa ve Türkiye'de internet* üzerinden *elde edilen suç gelirlerinin* önlenmesi *devam projesi(Iproceeds-II).* https://vizyon.taa.gov.tr/sayfa/iproceeds-2

Türkiye Ulaştırma ve Altyapı Bakanlığı (2024). *Ulusal siber güvenlik stratejisi ve eylem planı 2024-2028.* https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf#page=17.44

Weaver, D. (2020, June 30). Spatiality and world politics. *International Studies.* https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-562#acrefore-9780190846626-e-562-bibliography-0002

Weimann, G. (2016). Going dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism*, *93*(3), 195-206.

Weinert, M. (2017). Grounding world society: Spatiality, cultural heritage, and our world as shared geographies. *Review of International Studies*. *43*(3), 409–429.

Zeng, J., Stevens, T. & Chan, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "Internet sovereignty". *Politics & Policy*. *45*(3), 432-464.