OBSERVARE
Universidade Autónoma de Lisboa
e-ISSN: 1647-7251
VOL. 17, Nº. 2
November 2026-April 2027

JANUS.NET
e-journal of International Relations

THE GEOPOLITICS OF DIGITAL SOVEREIGNTY: POWER, SECURITY AND FREEDOM OF EXPRESSION IN THE AGE OF GLOBAL PLATFORMS

MARCO MARSILI
info@marcomarsili.it
Assistant Professor, Department of Philosophy and Cultural Heritage, Ca' Foscari University of Venice (Italy). Associated Researcher, Centro de Estudos Internacionais (CEI–Iscte), ISCTE – Instituto Universitário de Lisboa.

Abstract

Over the past decade, digital sovereignty has emerged as a central yet contested concept in international relations, encapsulating struggles over control of data, infrastructures and online speech. While states seek to reassert authority in cyberspace, global platforms exercise quasi-sovereign power and fundamental rights face mounting pressures from securitisation and hybrid threats. This article bridges scholarship on digital sovereignty with normative debates on freedom of expression, arguing that sovereignty in cyberspace is not merely a legal or technical issue but a fundamentally geopolitical and ethical one. Methodologically, the study adopts a qualitative, theory-guided comparative case design, applying a tripartite analytical framework that distinguishes state, corporate and normative dimensions of digital sovereignty. Four configurations are examined: the European Union's regulatory model, Russia's securitised approach, China's doctrine of cyber sovereignty, and the contested landscape of the Mediterranean region. For each case, the analysis traces how legal instruments, platform governance and rights frameworks interact to shape the exercise of authority in cyberspace, with particular attention to the protection or restriction of freedom of expression. The comparative findings show that digital sovereignty is plural and contested, ranging from protective models that seek to reconcile security and rights to repressive configurations that subordinate freedoms to regime stability. The article's main contribution is twofold: theoretically, it refines the concept of digital sovereignty by integrating state, corporate and normative dimensions into a single framework; empirically, it demonstrates how this framework illuminates the spectrum of practices through which security imperatives, platform power and freedom of expression are negotiated in the digital age.

Keywords

Digital sovereignty, freedom of expression, geopolitics, international security, social media, information warfare.

Resumo

Ao longo da última década, a soberania digital emergiu como um conceito central, ainda que contestado, nas relações internacionais, encapsulando lutas em torno do controlo de dados, infraestruturas e expressão em linha. Enquanto os Estados procuram reafirmar a sua autoridade no ciberespaço, as plataformas globais exercem um poder quase soberano e os direitos fundamentais enfrentam pressões crescentes resultantes da securitização e das ameaças híbridas. Este artigo aproxima a produção académica sobre soberania digital dos debates normativos sobre liberdade de expressão, sustentando que a soberania no ciberespaço não é apenas uma questão jurídica ou técnica, mas sobretudo uma questão geopolítica e ética. Em termos metodológicos, o estudo adota um desenho qualitativo de estudo de caso comparativo guiado pela teoria, aplicando um quadro analítico tripartido que

distingue as dimensões estatal, corporativa e normativa da soberania digital. São analisadas quatro configurações: o modelo regulamentar da União Europeia, a abordagem securitizada da Rússia, a doutrina chinesa de soberania cibernética e a paisagem contestada da região mediterrânica. Em cada caso, a análise acompanha a forma como instrumentos jurídicos, governação das plataformas e enquadramentos de direitos interagem para moldar o exercício da autoridade no ciberespaço, com particular atenção à proteção ou restrição da liberdade de expressão. Os resultados comparativos mostram que a soberania digital é plural e contestada, variando entre modelos protetores que procuram conciliar segurança e direitos e configurações repressivas que subordinam as liberdades à estabilidade do regime. A principal contribuição do artigo é dupla: do ponto de vista teórico, refina o conceito de soberania digital ao integrar as dimensões estatal, corporativa e normativa num único quadro; do ponto de vista empírico, demonstra como esse quadro ilumina o espetro de práticas através das quais imperativos de segurança, poder das plataformas e liberdade de expressão são negociados na era digital.

Palavras-chave

Soberania digital, liberdade de expressão, geopolítica, segurança internacional, redes sociais, guerra de informação.

How to cite this article
Marsili, Marco (2026). The Geopolitics of Digital Sovereignty: Power, Security and Freedom of Expression in the Age of Global Platforms. *Janus.net, e-journal of international relations*. VOL. 17, Nº. 2, November 2026-April 2027, pp. 49-71. DOI https://doi.org/10.26619/1647-7251.17.2.3

Article submitted on 31 August 2025 and accepted on 31 July 2026.

THE GEOPOLITICS OF DIGITAL SOVEREIGNTY: POWER, SECURITY AND FREEDOM OF EXPRESSION IN THE AGE OF GLOBAL PLATFORMS

MARCO MARSILI

Introduction

Over the past two decades, cyberspace has evolved from being a technological infrastructure supporting communication and commerce into a fully-fledged strategic domain of international relations. As digital platforms, critical infrastructures and information systems have become integral to politics, economics and security, the question of digital sovereignty has emerged as one of the central debates of our time (Pohle & Thiel, 2020; Carr, 2021). Digital sovereignty broadly refers to the capacity of states and societies to exercise authority over their digital environment, encompassing issues of data governance, cybersecurity, technological autonomy and freedom of expression. This concept, however, remains deeply contested: while states seek to reinforce their control over cyberspace, private corporations and transnational platforms have acquired quasi-sovereign authority in regulating online speech, moderating content and shaping global narratives (Klonick, 2018; DeNardis, 2020).

The European Union has positioned itself at the forefront of this debate through landmark regulatory instruments such as the *General Data Protection Regulation* (GDPR) and, more recently, the *Digital Services Act* (DSA) and the *Digital Markets Act* (DMA). These initiatives illustrate what Bradford (2020) has termed the "Brussels Effect": the extraterritorial impact of EU regulation, which effectively extends European norms to global digital governance. The assertion of regulatory sovereignty in cyberspace, however, raises critical questions about the balance between state control, corporate power and individual freedoms. In particular, freedom of expression—enshrined in Article 19 of the *Universal Declaration of Human Rights* (UDHR, 1948)—faces new challenges as governments tighten surveillance and censorship regimes in the name of security, while private platforms increasingly arbitrate the boundaries of permissible speech (Marsili, 2020, 2025a).

From a geopolitical perspective, cyberspace has become a new arena of strategic competition, not only between major powers such as the United States, China and the European Union, but also within regional contexts such as the Mediterranean and post-Soviet space. States have weaponised information flows, conducted disinformation

campaigns and engaged in hybrid warfare that blurs the line between peace and conflict (Bachmann & Gunneriusson, 2019; Marsili, 2019). The rise of digital authoritarianism, exemplified by China's *Great Firewall* and Russia's *Sovereign Internet Law*,[1] further demonstrates the extent to which digital sovereignty is being mobilised as a tool of power politics, often at the expense of civil liberties (Deibert, 2020).

This article aims to contribute to the debate by bridging two strands of scholarship: the study of digital sovereignty as an evolving concept in international relations, and the normative analysis of freedom of expression in cyberspace. Building on a growing body of scholarship concerning power dynamics, hybrid threats, and freedom of expression in the age of social media (e.g., Marsili, 2019, 2020, 2025a; Bachmann & Gunneriusson, 2019; DeNardis, 2020), this paper argues that digital sovereignty is not merely a legal or technological issue, but a fundamentally geopolitical one. It involves the redistribution of power between states, corporations and individuals, and has profound implications for the structure of international order.

The article is structured as follows: Section 2 reviews the existing literature on digital sovereignty and freedom of expression in cyberspace. Section 3 illustrates the methodology and research design. Section 4 develops the theoretical and conceptual framework for understanding digital sovereignty as a geopolitical phenomenon. Section 5 examines empirical cases, including the EU's regulatory strategy, authoritarian approaches in China and Russia, and hybrid warfare in the Mediterranean. Section 6 discusses the implications for freedom of expression and democratic governance. Section 7 concludes with reflections on the prospects of reconciling state sovereignty with global digital rights.

Literature Review

The notion of "digital sovereignty" has gained increasing attention in international relations and political theory over the past decade. Initially associated with state capacity to regulate cyberspace, it has gradually evolved into a multifaceted concept encompassing data governance, technological autonomy, cybersecurity, and the authority to regulate online speech. Pohle and Thiel (2020) argue that digital sovereignty is best understood as a "floating signifier", whose meaning shifts depending on political, legal and cultural contexts. For European policymakers, it often connotes technological self-determination and protection from foreign surveillance; for authoritarian states, it legitimises information control and censorship.

From a geopolitical perspective, Carr (2021) highlights how digital sovereignty reflects broader struggles over the distribution of power in cyberspace. States increasingly assert control through legal and technical measures, while private corporations—particularly global platforms such as Meta, Alphabet and ByteDance—exercise governance functions once reserved to states. Klonick (2018) defines these corporations as "new governors" of online speech, operating with global reach but limited accountability. This dual

[1] The *Sovereign Internet Law* (Russian: Закон о «суверенном интернете») is the informal name for a set of 2019 amendments to existing Russian legislation that mandate Internet surveillance and grants the Russian government powers to partition Russia from the rest of the Internet, including the creation of a national fork of the Domain Name System (DNS).

structure, where states and platforms both claim authority, has produced new forms of digital interdependence and contestation.

The securitisation of cyberspace and the implications of disinformation for democratic governance have been central to this debate (Marsili, 2019, 2020). Subsequent studies have further examined how disinformation, hybrid conflict, cognitive warfare and generative AI affect democratic resilience, especially in the European context, while also highlighting the tension between security imperatives and freedom of expression (Marsili, 2025b; Marsili, 2025c; Marsili, 2026).

The impact of digital sovereignty on freedom of expression constitutes a major concern in both academic and policy debates. The traditional human rights framework, enshrined in Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR, 1966) guarantees the right to seek, receive and impart information across borders. Yet, as DeNardis (2020) argues, the globalised nature of digital communication complicates the application of these rights. When platforms mediate most public communication, the boundaries of permissible speech are increasingly determined not by democratic processes but by opaque private rules.

Empirical studies show that platform content moderation has a significant impact on political discourse. Klonick (2018) traces the emergence of complex governance systems within platforms, where automated tools, corporate policies and transnational pressures interact to shape online speech. Similarly, the normative challenges of ensuring freedom of expression in cyberspace have been emphasised, especially when disinformation is securitised as a hybrid threat (Marsili, 2020, 2025a). The danger, from this perspective, is that security-driven approaches may inadvertently suppress legitimate dissent and narrow the public sphere.

This resonates with Deibert's (2020) analysis of "digital authoritarianism", where governments invoke sovereignty to justify restrictions on online freedoms. Examples include China's *Great Firewall*, Russia's *Sovereign Internet Law*, and Turkey's regulations compelling platforms to establish local offices subject to state oversight. In democratic contexts, however, the challenge is subtler: the balance between combating harmful content (such as hate speech or disinformation) and safeguarding pluralism. The EU's *Digital Services Act* embodies this tension by demanding greater accountability from platforms while affirming fundamental rights.

Cyberspace is not merely a technological environment but a strategic domain of international competition. Bachmann and Gunneriusson (2019) conceptualise hybrid warfare as the blending of military, informational and digital means, where cyberspace plays a central role. Disinformation campaigns, electoral interference and cyberattacks have become common instruments of statecraft. For instance, Russian operations in Ukraine, the Baltic states and the broader European neighbourhood illustrate how information warfare undermines sovereignty and destabilises democratic societies (Marsili, 2021).

These developments can be framed within the broader shift towards hybrid threats (Marsili, 2019). By blurring the boundaries between war and peace, cyber operations undermine traditional international law and pose dilemmas for sovereignty. This perspective aligns with a growing body of scholarship that treats cyberspace as both a

battlefield and a political arena (Nye, 2010; Klimburg, 2017). Nye (2010) emphasises the notion of "cyber power", defined as the ability to use cyberspace to achieve strategic objectives, while Klimburg (2017) warns of the risks of "cyber sovereignty" when used to legitimise repression.

DeNardis (2020) underlines that critical infrastructures—ranging from energy grids to health systems—are increasingly networked and therefore vulnerable. Sovereignty in cyberspace is not only about controlling information but also about securing infrastructures essential to national survival. This has spurred states to seek "technological sovereignty" by reducing dependency on foreign suppliers, as seen in debates over 5G networks and semiconductor supply chains.

The European Union has emerged as a pioneer in the governance of digital sovereignty. Bradford's (2020) "Brussels Effect" illustrates how EU regulations set de facto global standards in areas such as data protection and competition law. The *General Data Protection Regulation* exemplifies this extraterritorial reach, compelling global corporations to align with European norms.

Carr (2021) notes that the EU's discourse on "digital autonomy" reflects both security concerns and a broader desire for normative leadership. Initiatives such as the DSA and the DMA represent attempts to balance regulation of online platforms with protection of rights. Marsili (2020) contributes to this debate by examining the securitisation of disinformation within Europe, cautioning against the risk of conflating harmful content with political dissent.

At the same time, European scholarship stresses the need to reconcile sovereignty with openness. Floridi (2019) introduces the notion of the "infosphere" as a normative framework, emphasising the ethical responsibilities of digital governance. For Floridi, sovereignty should not entail isolation or censorship but rather the capacity to shape digital ecosystems in accordance with democratic values.

Despite significant contributions, three gaps remain evident in the literature. First, most studies treat digital sovereignty either as a legal concept or as a security issue, but few integrate these perspectives into a broader geopolitical framework. Some recent contributions begin to bridge this gap by linking cyber threats, hybrid warfare and freedom of expression to international relations theory. Second, while much attention has been paid to authoritarian models of digital sovereignty, less has been written on how democratic societies can assert sovereignty without undermining rights. The European case offers insights but also raises questions about proportionality and unintended consequences. Third, the role of non-state actors remains underexplored. Platforms are often analysed as regulators of speech, but their geopolitical influence—shaping public opinion, mediating conflicts, and negotiating with governments—deserves greater scrutiny.

This article addresses these gaps by situating digital sovereignty within the broader geopolitics of cyberspace, with a specific focus on its implications for freedom of expression. It engages with contemporary debates on hybrid threats, information warfare and global digital governance, while also drawing on recent contributions that examine disinformation, cognitive warfare and AI regulation within the evolving framework of EU digital governance (Marsili, 2025b; Marsili, 2025c; Marsili, 2026).

Methodology and Research Design

This paper adopts a qualitative, theory-guided comparative case study design to analyse how different configurations of digital sovereignty affect freedom of expression and the broader geopolitics of cyberspace. Rather than seeking statistical generalisation, the goal is to develop a conceptually rich and empirically grounded understanding of how sovereignty is asserted, contested and legitimised in distinct political and regional contexts. The analysis is structured around four cases: the European Union, Russia, China and the Mediterranean region.

The selection of cases follows a most-different systems logic. The European Union, Russia and China represent three major poles of contemporary digital geopolitics with sharply divergent regime types, legal traditions and approaches to online governance. The EU is a supranational polity that frames digital sovereignty primarily through regulation and fundamental rights; Russia mobilises sovereignty through securitisation, information warfare and domestic control; China articulates a comprehensive doctrine of "cyber sovereignty" rooted in techno-authoritarian state leadership.

The Mediterranean region is included as a fourth case to capture a different configuration: a fragmented space of fragile states, hybrid threats and competing external influences, where digital sovereignty is contested rather than consolidated. Rather than treating the Mediterranean as a single, homogeneous unit, the analysis focuses on patterns of vulnerability and external interference that emerge across multiple states, illustrating how weak institutional capacity, dependency on foreign platforms and exposure to disinformation erode the exercise of sovereignty in cyberspace. Including the Mediterranean alongside the three state-centred cases makes it possible to contrast consolidated models of digital sovereignty with a context in which authority is diffuse, rights are precarious and hybrid threats proliferate.

Taken together, these four cases constitute a spectrum of digital sovereignty practices ranging from protective regulatory models to repressive authoritarian ones, and from consolidated to fragile configurations. The comparative logic is therefore heuristic: the aim is to trace how different combinations of state, corporate and normative sovereignty shape the governance of cyberspace and freedom of expression across this spectrum.

The empirical analysis is based on a combination of academic literature, legal and policy documents, and secondary analyses of cyber operations and disinformation campaigns. For the European Union, key sources include EU regulations and directives (such as the GDPR, the DSA and the DMA) as well as scholarship on the "Brussels Effect" and digital autonomy. For Russia, the analysis draws on legislation such as the *Sovereign Internet Law*[2] reports on information warfare and hybrid threats, and studies of Russian approaches to global internet governance.

The Chinese case is examined through official speeches and policy documents articulating the doctrine of cyber sovereignty, legal frameworks such as the *Cybersecurity Law*, and scholarly work on digital authoritarianism and domestic platform ecosystems. The

[2] The *Sovereign Internet Law* (Russian: Закон о «суверенном интернете») is the informal name for a set of 2019 amendments to existing Russian legislation that mandate Internet surveillance and grants the Russian government powers to partition Russia from the rest of the Internet, including the creation of a national fork of the Domain Name System (DNS).

Mediterranean section relies on case studies of specific countries (e.g. Libya, Syria, Lebanon) and regional analyses of hybrid warfare, disinformation and external influence, with particular attention to how these dynamics affect media systems and online public spheres.

Across all cases, the article draws on existing research on cyber power, hybrid threats and freedom of expression. These sources are not treated as mere background; rather, they provide empirical material and interpretive lenses that are systematically mapped onto the conceptual framework of digital sovereignty developed in Section 4.

The conceptual framework distinguishes three interrelated dimensions of digital sovereignty: state sovereignty, corporate sovereignty and normative sovereignty. In the empirical analysis, these dimensions are operationalised as follows.

State sovereignty refers to the authority of governments (or, in the EU's case, supranational institutions) to regulate cyberspace, secure critical infrastructures and assert technological autonomy through laws, policies and technical measures. Corporate sovereignty captures the quasi-sovereign power of digital platforms and technology companies to regulate speech, moderate content, design infrastructures and shape global digital ecosystems. Normative sovereignty assesses the legitimacy of authority exercised in cyberspace in light of fundamental rights, with particular attention to freedom of expression as protected by international human rights instruments.

For each case, the analysis proceeds through a structured, focused comparison. First, it identifies the main legal and technical instruments through which state actors assert sovereignty in cyberspace (e.g. regulatory acts, firewalls, surveillance infrastructures). Second, it examines the role of platforms and corporate actors in mediating or reinforcing this authority, analysing whether corporate sovereignty is constrained, co-opted or left largely unchecked. Third, it evaluates the implications of these configurations for freedom of expression, distinguishing between protective sovereignty (where authority is used to safeguard rights) and repressive sovereignty (where it serves to curtail them).

This structured application of the tripartite framework to each case ensures that the empirical sections do not merely describe existing practices but systematically relate them to the broader theoretical argument. It also enables comparative insights in Section 6, where the spectrum of digital sovereignty models is reconstructed and the trade-offs between security, sovereignty and freedom of expression are discussed.

Two limitations of this research design should be acknowledged. First, the qualitative and interpretive nature of the analysis means that it does not claim statistical representativeness or causal identification in a narrow sense. Its contribution lies instead in conceptual clarification and the synthesis of dispersed empirical evidence into a coherent analytical framework. Second, the focus on four cases, while allowing for depth and comparison, inevitably leaves out other important models of digital sovereignty, such as those found in Latin America, Africa or South-East Asia.

These limitations do not undermine the value of the analysis but rather delineate its scope. By making the research design explicit, the paper invites further work that might extend the framework to additional cases or complement qualitative insights with quantitative data.

Theoretical and Conceptual Framework

Sovereignty has traditionally been understood as the supreme authority of the state within its territorial borders (Krasner, 1999). Yet cyberspace challenges this Westphalian paradigm, as digital flows transcend physical frontiers and operate through infrastructures and platforms beyond the exclusive control of states. Nye (2010) introduced the notion of "cyber power" to capture the ability of actors to achieve objectives in and through cyberspace. Building on this, contemporary scholars conceptualise digital sovereignty as the assertion of authority in a domain that is simultaneously global, decentralised and technically mediated (Pohle & Thiel, 2020).

Scholarship on the securitisation of cyberspace has highlighted how this process reframes sovereignty: states perceive cyber threats as existential, legitimising extraordinary measures that extend state control into the digital sphere (Marsili, 2019; Bachmann & Gunneriusson, 2019). From this perspective, sovereignty is thus not merely a legal principle but a dynamic practice, exercised through surveillance, regulation and technological control. In this sense, digital sovereignty can be understood as the translation of classical notions of authority into a deterritorialised, networked environment.

From a geopolitical perspective, digital sovereignty reflects a redistribution of power between states, corporations and individuals. As DeNardis (2020) observes, private actors increasingly control infrastructures critical to sovereignty—such as domain name systems, cloud services and undersea cables. Platforms like Facebook, Google and TikTok regulate speech and information flows on a global scale, effectively exercising "platform sovereignty" (Klonick, 2018). This introduces a paradox: while states invoke sovereignty to assert authority, they are simultaneously dependent on corporations for the governance of digital spaces.

This interdependence, however, carries significant risks if securitised, as the fight against disinformation may legitimise restrictions on freedom of expression (Marsili, 2020). This insight resonates with Bachmann and Gunneriusson's (2019) theory of hybrid warfare, where information operations are deployed as tools of strategic influence. Digital sovereignty, therefore, cannot be reduced to state-centric control; it must be analysed as a contested field shaped by interactions between multiple actors with divergent interests.

A second dimension of the conceptual framework concerns the normative implications of digital sovereignty for freedom of expression. Classical theories of free speech, from Mill's *On Liberty* (1859) to contemporary human rights frameworks, rest on the principle that the public sphere should remain open to pluralism and dissent. Yet in cyberspace, governance is often privatised, with corporations enforcing standards that lack democratic legitimacy (Klonick, 2018).

The fragility of freedom of expression in the digital era has been underlined in recent research (Marsili, 2025a): as states expand surveillance and platforms police content, dissenting voices risk marginalisation. Deibert (2020) similarly warns of the rise of "digital authoritarianism", where sovereignty is invoked to justify repression. The

conceptual framework therefore distinguishes between protective sovereignty—where authority safeguards rights—and repressive sovereignty—where authority curtails them.

By integrating insights from recent scholarship with normative political theory, the article adopts a critical stance: sovereignty in cyberspace is legitimate only to the extent that it respects the fundamental right to freedom of expression. This perspective frames digital sovereignty not merely as a technical or legal issue, but as a normative choice about the distribution of rights and responsibilities in the digital public sphere.

The rise of hybrid threats further complicates the debate. Research demonstrates that disinformation and cyberterrorism blur the boundaries between security and communication (Marsili, 2019, 2020; Bachmann & Gunneriusson, 2019). Governments respond by securitising the digital environment, often conflating harmful content with political dissent. Bachmann and Gunneriusson (2019) identify this as a defining feature of hybrid warfare: the fusion of informational, political and military tools to destabilise adversaries.

The conceptual framework proposed here situates digital sovereignty at the intersection of security and rights. Recent analyses of cognitive warfare and cognitive security have shown how hybrid conflicts, platform ecosystems and generative AI extend this tension into the informational and psychological domains, eroding the conditions for free judgement and democratic participation (Marsili, 2023; Marsili, 2025c; Marsili, 2026). On one hand, states are compelled to defend their citizens against cyber threats; on the other, excessive securitisation undermines the democratic legitimacy of sovereignty. The balance between these imperatives constitutes a central challenge of the digital age.

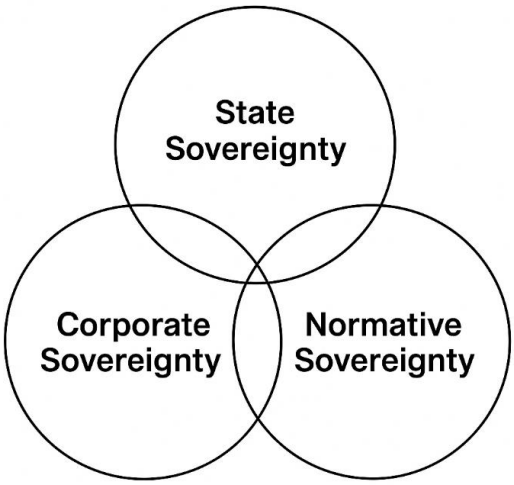
Building on the above insights, this article proposes a multilevel conceptualisation of digital sovereignty comprising three interrelated dimensions:

1. State Sovereignty: The authority of governments to regulate cyberspace, secure infrastructures and assert technological autonomy.
2. Corporate Sovereignty: The quasi-sovereign power of platforms and technology companies to regulate speech, moderate content and shape global digital ecosystems.
3. Normative Sovereignty: The legitimacy of authority exercised in cyberspace, measured against fundamental rights, particularly freedom of expression.

This diagram illustrates the tripartite model of digital sovereignty, highlighting the interplay between state sovereignty, corporate authority, and normative rights.

This framework enables a nuanced analysis of empirical cases. For instance, the EU's *Digital Services Act* exemplifies an attempt to reconcile state sovereignty with normative sovereignty, by holding platforms accountable while affirming rights (Bradford, 2020). Conversely, China's *Great Firewall* represents a model of repressive sovereignty, privileging control over freedoms. Research on the securitisation of disinformation in democratic contexts has cautioned that well-intentioned measures can erode the very rights they aim to protect (Marsili, 2019; Marsili, 2020).

Figure 1. Conceptual framework of digital sovereignty



Source: Author.

The theoretical contribution of this article is twofold. First, it bridges the gap between international relations theory and normative political philosophy by situating digital sovereignty within the broader geopolitics of cyberspace. Second, it develops an analytical framework that disaggregates sovereignty into state, corporate and normative dimensions, thereby capturing the complexity of governance in the digital age.

This approach draws on scholarship on hybrid threats, disinformation and freedom of expression, while integrating insights from international security studies and political theory. It provides a conceptual foundation for analysing case studies in the following sections, where the tensions between security, sovereignty and freedom will be examined in practice.

Case Studies

The European Union has emerged as a global frontrunner in the assertion of digital sovereignty through legal and regulatory instruments. Unlike authoritarian states, the EU frames its digital sovereignty primarily as an extension of normative commitments, seeking to protect fundamental rights while curbing the excessive influence of global platforms. This configuration can be analysed through the tripartite framework developed in this article, which distinguishes state, corporate and normative dimensions of sovereignty in cyberspace.

In terms of state sovereignty, the EU's approach is shaped by landmark regulatory initiatives such as the GDPR, the DSA and the DMA. This regulatory trajectory has recently been extended to artificial intelligence, with the AI Act interpreted as a key instrument for defending European technological and cognitive sovereignty against competing models of digital governance (Marsili, 2026).

As Bradford shows with the notion of the "Brussels Effect", EU rules often become de facto global standards, since multinational companies adjust their practices worldwide to comply with European law (Bradford, 2020). Through this extraterritorial reach, the Union exercises a form of legal–normative power that asserts sovereignty not by building technical barriers, but by projecting its regulatory framework into the digital domain.

Corporate sovereignty is equally central to the European configuration. Platforms such as Meta, Alphabet and ByteDance mediate public communication and control critical infrastructures of the infosphere, thereby exercising governance functions once reserved for states (Klonick, 2018; DeNardis, 2020). In the EU, however, these actors are increasingly subject to co-regulation and oversight: the DSA imposes risk-assessment, transparency and audit obligations on very large platforms, while the DMA constrains the market power of "gatekeepers" by limiting certain forms of self-preferencing and data consolidation. These instruments do not abolish corporate sovereignty, but they seek to rebalance it by embedding platform governance within a broader legal framework that asserts the primacy of public authority over private rule-making.

The normative dimension of sovereignty is particularly salient in the European case. Freedom of expression, protected by instruments such as the *European Convention on Human Rights* and the *EU Charter of Fundamental Rights*, functions as a benchmark for evaluating digital governance. Floridi's notion of the "infosphere" underscores that digital policy cannot be reduced to technical management, but entails ethical responsibilities for shaping information ecosystems (Floridi, 2019). At the same time, analyses of hybrid threats and disinformation warn that the securitisation of "fake news" within Europe may narrow the public sphere: measures adopted in the name of security risk conflating harmful content with legitimate dissent, shifting the balance from protective to potentially repressive sovereignty (Marsili, 2019, 2020, 2025a).

Overall, the EU exemplifies a regulatory model of digital sovereignty in which state power is exercised primarily through law and policy, corporate sovereignty is constrained but remains influential, and normative sovereignty functions both as a guiding principle and as a site of contestation. Authors such as Carr and Deibert highlight how this model seeks to couple technological autonomy with the protection of rights, positioning the Union as a normative actor in global digital governance (Carr, 2021; Deibert, 2020). Yet the European case also reveals the fragility of this equilibrium: as hybrid threats intensify and pressures to control online speech grow, the line between safeguarding and restricting freedom of expression becomes increasingly thin, confirming that even democratic configurations of digital sovereignty must constantly renegotiate the trade-off between security, platform power and rights (Pohle & Thiel, 2020).

The figure contrasts the European Union's regulatory approach with Russia's securitised model and China's techno-authoritarian system, outlining key similarities and differences across law, platforms, and rights.

Russia represents a contrasting model of digital sovereignty in which state authority is explicitly mobilised to consolidate control over the domestic information space. Legal instruments such as the *Sovereign Internet Law* require internet service providers to route traffic through state-controlled nodes, enabling the government to isolate the Russian segment of the network from the global internet and to centralise technical

control (Nocetti, 2015). This regulatory architecture is complemented by extensive surveillance, blocking of opposition websites and the criminalisation of online dissent, illustrating how digital sovereignty is deployed as a tool of regime security rather than as a means of safeguarding rights (Deibert, 2020).

Figure 2. Comparative models of digital sovereignty

Dimension	European Union (Regulatory)	Russia (Securitised)	China (Techno-authoritarian)
Legal approach	DSA; GDPR	Sovereign Internet Law	Great Firewall; Cybersecurity Law
Role of platforms	Co-regulation; accountability	State-controlled	State-directed
Freedom of expression	Protected with limits (e.g. hate speech)	Restricted under security pretexts	Heavily censored, state-prioritised
Security vs rights balance	Attempt at balance	Security dominates	Control dominates

Source: Author.

From the perspective of state sovereignty, Russia's approach exemplifies a form of repressive sovereignty in which the primary objective is to insulate the domestic information environment from external influence and internal contestation. The construction of national routing infrastructures and control mechanisms aims to reduce dependency on foreign technologies and platforms, while strengthening the capacity of security agencies to monitor and intervene in communication flows. This model thus combines legal, technical and coercive instruments to assert a high degree of state control over cyberspace, blurring the boundary between ordinary regulation and emergency measures.

Corporate sovereignty in the Russian context is closely intertwined with state power. Domestic platforms and technology companies – including major social networks and search engines – operate within a framework of legal and informal obligations that align their practices with governmental objectives. Content moderation, data retention and cooperation with law-enforcement agencies are shaped by requirements that effectively subordinate corporate governance to state priorities. Foreign platforms, when allowed to operate, face pressures to localise data, establish local offices and comply with requests that further extend state reach into the digital sphere. In this way, corporate sovereignty is not an autonomous counterweight to state power, but a vector through which state sovereignty is projected and reinforced.

The normative dimension of digital sovereignty in Russia is characterised by the systematic subordination of freedom of expression and other fundamental rights to security imperatives. Legal provisions on extremism, terrorism and "fake news" are interpreted broadly and applied in ways that restrict political speech, independent journalism and online activism (Nocetti, 2015). Research on hybrid warfare and information operations shows that Russia's information strategy extends beyond its borders, combining domestic control with external disinformation campaigns and cyber

operations that target other states (Marsili, 2019). These practices exploit the openness of liberal democracies while shielding the Russian digital environment through authoritarian control, producing an asymmetric configuration in which sovereignty is defended internally by closure and projected externally through disruptive interference.

Taken together, these features situate Russia towards the repressive end of the spectrum of digital sovereignty. State sovereignty is asserted through legal and technical measures that prioritise regime stability; corporate sovereignty is aligned with state objectives rather than constrained by independent regulation; and normative sovereignty is weakened by the erosion of rights in the name of security. This configuration highlights how digital sovereignty can function as a vehicle for authoritarian consolidation, demonstrating that appeals to sovereignty in cyberspace do not necessarily protect citizens, but can instead legitimise intensified control over information and expression.

China provides perhaps the most developed model of cyber sovereignty, rooted in the principle that each state has the right to regulate its own internet in accordance with national laws and interests (Creemers, 2017). The *Great Firewall* embodies this doctrine by filtrare contenuti stranieri, bloccare l'accesso a piattaforme globali e promuovere alternative domestiche come WeChat, Weibo e Baidu. Alongside this technical architecture, the *Cybersecurity Law* and related regulations consolidate state control over infrastructures, data and online speech, illustrating a comprehensive attempt to translate classical sovereignty into digital form.

From the perspective of state sovereignty, the Chinese model is characterised by a high degree of centralisation and by the fusion of legal, technical and organisational instruments. National routing, pervasive filtering and strict licensing regimes allow the state to determine which services operate, how data circulate and which information reaches domestic audiences (Creemers, 2017). This configuration reduces dependence on foreign technologies and platforms while enabling authorities to intervene quickly in digital communication, whether by removing content, closing accounts or reconfiguring access to services. In this sense, cyber sovereignty in China represents a maximalist interpretation of state authority in cyberspace.

Corporate sovereignty in the Chinese context is closely aligned with state objectives. Major domestic platforms and technology companies function within a framework in which responsibilities for content moderation, data collection and cooperation with security authorities are integrated into the business model. Companies are expected to enforce state-defined standards, participate in censorship and surveillance, and support policy goals such as social stability and ideological control (Deibert, 2020). Foreign platforms, when not outright blocked, face stringent requirements that limit their autonomy and ensure that their operations remain subordinated to national priorities. As a result, corporate sovereignty does not act as an independent pole of authority, but as an extension and instrument of state sovereignty.

The normative dimension of digital sovereignty in China is marked by the systematic prioritisation of control and security over freedom of expression and other fundamental rights. Legal and policy discourses on cyber sovereignty stress the need to protect national culture, social harmony and political stability, while downplaying universalist conceptions of human rights (Deibert, 2020). At the World Internet Conference in

Wuzhen, Xi Jinping's statement that each country has the right to choose its own path of cyber development and regulation formalised this vision of a fragmented, state-centred internet order. In practice, this has translated into extensive censorship of political content, restrictions on independent journalism and the use of digital tools for social control, including systems of reputational scoring and monitoring (Creemers, 2017).

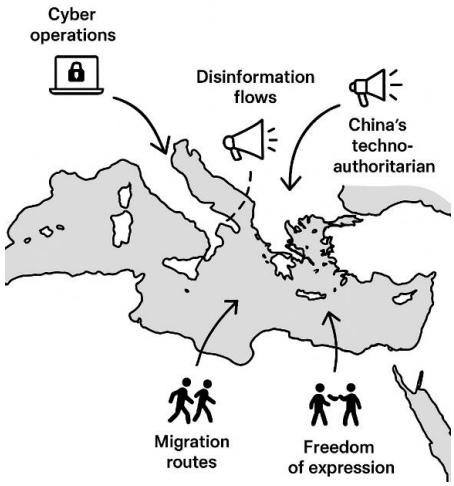
Empirical analyses show that this techno-authoritarian model coexists with a dynamic domestic digital economy, demonstrating that repressive sovereignty can be combined with innovation under strict state guidance (Deibert, 2020). Applying the tripartite framework, China appears as a configuration in which state sovereignty dominates, corporate sovereignty is co-opted, and normative sovereignty is subordinated to regime priorities. Freedom of expression is heavily constrained, not as an accidental by-product of security policy, but as a deliberate component of a broader project of digital governance. This places China firmly at the repressive end of the spectrum of digital sovereignty, while illustrating how appeals to cyber sovereignty can legitimise far-reaching restrictions on rights and contribute to the fragmentation of the global digital order.

The Mediterranean region illustrates a distinct configuration of digital sovereignty, characterised not by a single sovereign actor but by a constellation of states marked by fragile governance, external interference and hybrid threats. Unlike the European Union, Russia or China, the Mediterranean does not present a consolidated model of digital sovereignty; rather, it offers a laboratory in which the limits of sovereignty in cyberspace become visible under conditions of institutional weakness and geopolitical contestation. Analysing this region through the tripartite framework of state, corporate and normative sovereignty makes it possible to capture how authority is fragmented, rights are precarious and external actors exploit systemic vulnerabilities (Marsili, 2019, 2020).

This map illustrates how the Mediterranean region functions as a strategic crossroads where cyber operations, disinformation campaigns, and hybrid threats intersect.

From the perspective of state sovereignty, many Mediterranean countries – such as Libya, Syria and Lebanon – face acute challenges in asserting effective authority over digital infrastructures and information flows. Regulatory frameworks are often underdeveloped, unevenly enforced or subordinated to broader crises of statehood and security, which limit the capacity of governments to regulate platforms, secure networks or develop coherent digital strategies. In several cases, telecommunication infrastructures and cybersecurity capabilities depend heavily on foreign suppliers and external assistance, creating structural asymmetries that constrain domestic control over cyberspace. This weakness is compounded by the presence of regional and extra-regional powers that deploy cyber operations, disinformation campaigns and information warfare to advance their strategic interests, further destabilising the region and undermining the effective exercise of sovereignty.

Figure 3. The Mediterranean as a laboratory of hybrid threat



Source: Author.

Corporate sovereignty is particularly salient in this context. Global platforms such as Facebook, Twitter and YouTube dominate the information space, especially during the political and social mobilizations associated with the so-called Arab Spring. These platforms have enabled new forms of organization and transnational connection, contributing to the opening of public spheres in societies where traditional media are often controlled or censored. At the same time, the very infrastructures that support mobilisation have functioned as instruments of surveillance and repression: in the absence of strong regulatory regimes and independent oversight, state and non-state actors have used platform data and digital traces to monitor activists, identify opponents and target dissent (Marsili, 2020). The dominance of foreign platforms – and the limited leverage Mediterranean governments have over their governance – means that corporate sovereignty often operates without meaningful accountability to local publics, with decisions about content moderation, data access or cooperation with state agencies largely external to national democratic processes.

The normative dimension of digital sovereignty in the Mediterranean is marked by uneven and fragile protections of rights in cyberspace. Authoritarian regimes in the region invoke digital sovereignty to justify censorship, blocking of websites and criminalisation of online dissent, using security narratives to legitimise restrictions on expression and association. Even in more pluralistic or formally democratic systems, emergency measures, anti-terrorism laws and regulations targeting "fake news" can be deployed in ways that narrow the public sphere and chill critical speech. International human rights frameworks – including Article 19 of the ICCPR – provide normative benchmarks, but their implementation is inconsistent and often subordinated to short-term security imperatives or external conditionalities. In practice, normative sovereignty is frequently fragmented: rights protections depend on the interplay between domestic legal systems, international commitments and the policies of global platforms, none of which offer stable guarantees. Citizens experience digital rights as contingent and reversible, shaped by shifting

coalitions of state and corporate actors operating in a context of geopolitical competition (Marsili, 2019, 2020).

Viewed through the combined lenses of state, corporate and normative sovereignty, the Mediterranean does not exemplify a fully realised model of digital sovereignty but rather a contested field in which authority is diffuse and vulnerable. Weak state capacity, dependence on external platforms and uneven rights protections interact with hybrid threats to produce a landscape where sovereignty is constantly challenged and freedom of expression is exposed to overlapping pressures. This configuration stands in contrast to the more consolidated models observed in the European Union, Russia and China: whereas those cases demonstrate how digital sovereignty can be mobilised to protect or restrict rights within relatively stable institutional settings, the Mediterranean highlights the consequences of exercising sovereignty under conditions of fragility and external interference. Including the region in the comparative analysis therefore serves a specific analytical purpose: it shows that digital sovereignty is not only about how powerful states govern cyberspace, but also about how weaker states struggle to maintain authority and rights in environments shaped by foreign platforms and geopolitical competition. In this sense, the Mediterranean case is indispensable for capturing the full spectrum of digital sovereignty practices and for understanding how hybrid threats exacerbate the tension between security and freedom of expression in the contemporary international order (Marsili, 2019, 2020). These four case studies illustrate the diversity of digital sovereignty in practice:

1. European Union: A model of protective sovereignty, seeking to reconcile regulation with rights.
2. Russia: A model of repressive sovereignty, combining domestic control with external disinformation.
3. China: A comprehensive model of cyber sovereignty, prioritising state control and national platforms.
4. Mediterranean: A fragmented landscape, where weak states struggle to assert sovereignty against external powers and corporate platforms.

Together, they demonstrate that digital sovereignty is not a monolithic concept but a field of contestation shaped by political systems, strategic interests and normative commitments. Applying the framework of state, corporate and normative sovereignty allows us to capture these variations and assess their implications for freedom of expression and global order.

Discussion

The comparative analysis of the European Union, Russia, China and the Mediterranean region shows that digital sovereignty cannot be understood as a fixed or uniform concept, but as a spectrum of practices ranging from protective to repressive models. By systematically applying the tripartite framework of state, corporate and normative sovereignty to each case, the article reconstructs how different configurations of

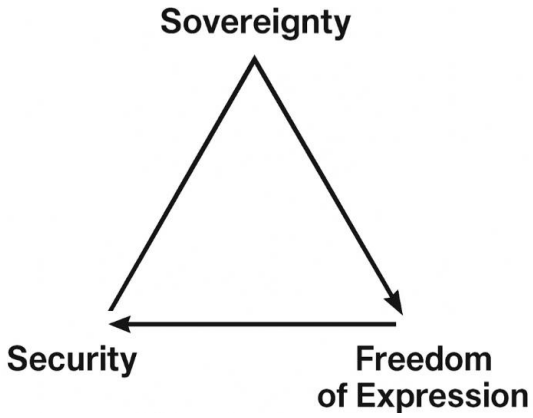
authority, platform power and rights shape the governance of cyberspace in diverse political and regional contexts.

At one end of this spectrum, the EU exemplifies a regulatory and largely protective model of digital sovereignty, in which state authority is exercised primarily through law and policy, corporate sovereignty is constrained by co-regulation, and normative sovereignty – rooted in fundamental rights – retains a central role despite tensions linked to the securitisation of disinformation. At the other end, Russia and China illustrate how digital sovereignty can be mobilised to consolidate authoritarian control: state sovereignty is asserted through legal and technical measures that insulate domestic information spaces, corporate sovereignty is aligned or co-opted to support regime objectives, and normative sovereignty is weakened by systematic restrictions on freedom of expression (Nocetti, 2015; Deibert, 2020). The Mediterranean represents a fragmented middle ground, where weak governance, dependence on external platforms and hybrid threats combine to undermine the effective exercise of sovereignty and to render rights precarious (Marsili, 2019, 2020).

This spectrum confirms Pohle and Thiel's argument that digital sovereignty functions as a "floating signifier": its meaning shifts with political regimes, strategic interests and cultural contexts, and cannot be reduced to a single legal or technical definition (Pohle & Thiel, 2020). The tripartite framework developed in the article helps to map these variations by distinguishing between the formal authority of states, the quasi-sovereign power of platforms and the normative legitimacy of digital governance. In each case, the balance between these dimensions differs: some configurations privilege state control over platforms and rights; others seek to rebalance corporate governance through regulation; others again struggle to assert any coherent form of sovereignty in the face of external influence and institutional fragility.

A central theme emerging from the comparison is the security–rights trade-off. States invoke digital sovereignty in response to threats such as cyberattacks, disinformation and terrorism, which blur the boundaries between peace and conflict and legitimise extraordinary measures (Marsili, 2019; Bachmann & Gunneriusson, 2019). In the EU, this manifests in policies against "fake news" and harmful content that risk encroaching on political dissent if not carefully designed (Marsili, 2020). In Russia and China, the trade-off is resolved decisively in favour of state security and regime stability, with little regard for individual rights (Nocetti, 2015; Deibert, 2020). In the Mediterranean, weak states oscillate between overreliance on foreign platforms and repressive crackdowns, often without adequate safeguards for rights or effective regulatory capacity. These trajectories illustrate that security and sovereignty are not inherently incompatible with freedom of expression, but without robust normative constraints and institutional checks, security-driven approaches tend to drift towards repression.

Figure 4. Balancing sovereignty, security, and freedom of expression



Source: Author

A triangular model depicting the trade-offs between digital sovereignty, state security imperatives, and the protection of fundamental rights in cyberspace.

Another key insight concerns the role of corporate sovereignty. Platforms such as Meta, Alphabet and ByteDance regulate global information flows, setting rules for speech, enforcing sanctions and designing infrastructures that shape public discourse (Klonick, 2018; DeNardis, 2020). In the EU, corporate sovereignty is partially constrained through instruments like the DSA and DMA, which embed platform governance in a legal framework that affirms public oversight. In authoritarian contexts such as Russia and China, domestic platforms align closely with state objectives, reinforcing control rather than counterbalancing it. In the Mediterranean, dependence on foreign platforms erodes state sovereignty, as governments lack leverage over corporate decision-making and rights protections depend on external policies beyond domestic democratic control (Marsili, 2020). This comparative insight underscores that digital sovereignty cannot be reduced to state action alone: it is co-constituted by the interplay between public authorities and private infrastructures.

The concept of normative sovereignty provides a lens to distinguish between protective and repressive models of digital sovereignty. Protective sovereignty aims to safeguard rights by regulating digital environments and ensuring accountability for both state and corporate actors, as in the European case when measures against disinformation remain anchored in human rights standards. Repressive sovereignty, by contrast, uses digital control to suppress dissent and consolidate power, as illustrated by Russia's *Sovereign Internet Law* and China's *Great Firewall* (Nocetti, 2015; Deibert, 2020). The Mediterranean case reveals a third configuration in which normative sovereignty is fragmented: rights protections are uneven, contingent and often undermined by hybrid threats and external manipulation (Marsili, 2019, 2020).

Taken together, these findings contribute to both theoretical and policy debates on digital sovereignty. Theoretically, they show that sovereignty in cyberspace must be situated within a multilevel framework that accounts for state authority, corporate power and

normative legitimacy, rather than being equated solely with territorial control or technical capacity (Krasner, 1999; Nye, 2010). Empirically, the comparative case study design demonstrates how different combinations of these dimensions produce divergent outcomes for freedom of expression and democratic governance. The discussion thus highlights that the future of digital sovereignty will depend not only on technological and legal innovations but also on the normative choices societies make about the balance between security, platform power and rights in the digital age.

Conclusion

The analysis presented in this article has examined digital sovereignty through the lenses of state, corporate and normative authority, applying this framework to four configurations: the European Union, Russia, China and the Mediterranean region. By adopting a qualitative, theory-guided comparative case study design, the paper has shown that digital sovereignty is neither a fixed nor a homogeneous concept, but a plural and contested set of practices shaped by divergent regime types, strategic interests and normative orientations.

At its core, digital sovereignty embodies a tension between security imperatives and fundamental rights. States invoke sovereignty to safeguard critical infrastructures, counter hybrid threats and defend against cyber operations, yet – as the case studies have demonstrated – these measures frequently come at the expense of freedom of expression. This trade-off is not unique to authoritarian regimes: even within the EU, policies against disinformation risk narrowing democratic discourse if they are not firmly anchored in human rights standards. The legitimacy of digital sovereignty therefore hinges on whether it functions as protective sovereignty – safeguarding rights – or degenerates into repressive sovereignty, curtailing them.

Theoretically, the study argues that sovereignty in cyberspace cannot be understood solely in terms of state control. It must be situated within a multilevel framework that acknowledges the quasi-sovereign role of corporations and the normative dimension of rights, extending classical insights on sovereignty's contingency into a digital domain where authority is fragmented and deterritorialised. Research on cyber threats, disinformation and freedom of expression underscores that sovereignty in cyberspace is simultaneously a question of power politics and normative legitimacy. By integrating these dimensions, the article contributes to bridging international relations theory with political philosophy and human rights scholarship, highlighting that digital sovereignty is not merely about controlling infrastructures but about making normative choices concerning the governance of the public sphere.

From a policy perspective, the findings suggest several lessons. For democratic states and the EU, regulatory sovereignty must be carefully calibrated to ensure that measures against disinformation and harmful content do not inadvertently suppress dissent; instruments such as the DSA and DMA provide valuable models, but they require constant monitoring and transparency mechanisms to prevent abuse. For authoritarian regimes, the cases of Russia and China illustrate the dangers of conflating sovereignty with repression: while effective in consolidating regime stability, such models erode normative legitimacy and contribute to global digital fragmentation. For fragile states in the

Mediterranean and beyond, the challenge is to build institutional capacity to regulate platforms without succumbing to authoritarian practices, drawing on international cooperation, capacity-building and regional frameworks to strengthen protective sovereignty while resisting external manipulation.

At the level of global governance, the coexistence of divergent models of digital sovereignty risks undermining the vision of an open, secure and rights-respecting internet. Multilateral fora and multi-stakeholder initiatives remain essential for fostering dialogue and establishing minimum norms, but they must be revitalised to remain effective in an era of intensifying geopolitical competition. Looking ahead, technological innovation, evolving platform governance and deepening normative contestation will continue to reshape the landscape of digital sovereignty. The future of sovereignty in cyberspace will thus depend not only on power relations and regulatory choices, but also on the normative struggles over the meaning and scope of rights in the digital age.

In conclusion, digital sovereignty is ultimately about who governs cyberspace and on what terms. It concerns how states, corporations and societies negotiate authority in a domain that transcends borders yet profoundly shapes political life. The comparative analysis of the EU, Russia, China and the Mediterranean illustrates the diversity of models, but also a common dilemma: how to reconcile security with freedom of expression. Ensuring that sovereignty becomes a tool for protecting freedoms rather than a pretext for curtailing them is the central challenge facing democracies, regimes and the international community as they confront the geopolitical and normative stakes of the digital age.

References

Bachmann, S., & Gunneriusson, H. (2019). Hybrid Wars: 21st Century's New Threats to Global Peace and Security. *Scientia Militaria, 43*(1), 77–98. doi:10.5787/43-1-1110.

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Carr, M. (2021). *Cyber Security in International Relations*. Routledge.

Creemers, R. (2017). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. *Journal of Contemporary China, 26*(103), 85–100. doi:10.1080/10670564.2016.1206281.

Deibert, R. (2020). *Reset: Reclaiming the Internet for Civil Society*. House of Anansi.

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press.

Floridi, L. (2019). *The Logic of Information: A Theory of Philosophy as Conceptual Design*. Oxford University Press.

International Covenant on Civil and Political Rights, adopted 16 December 1966, entered into force 23 March 1976, 999 UNTS 171.

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace*. Penguin.

Klonick, K. (2018). The New Governors: The People, Rules, and Processes Governing Online Speech. *Harvard Law Review, 131*(6), 1598–1670.

Krasner, S. (1999). *Sovereignty: Organized Hypocrisy*. Princeton University Press.

Marsili, M. (2019). The War on Cyberterrorism. *Democracy and Security, 15*(2), 172–199. doi:10.1080/17419166.2018.1496826.

Marsili, M. (2020). COVID-19 Infodemic: Fake News, Real Censorship. *Europea, 10*(2), 147–170. doi:10.4399/97888255402468.

Marsili, M. (2021). The Russian Influence Strategy in Its Contested Neighbourhood. In H. Mölder, V. Sazonov, A. Chochia, & T. Kerikmäe (eds.), *The Russian Federation in Global Information Warfare. Influence Operations in Europe and Its Neighborhood*, pp. 149-172. Springer. doi:10.1007/978-3-030-73955-3_8.

Marsili, M. (2025a). *Libertà di pensiero nell'era digitale. Genesi ed evoluzione della libertà di pensiero dal V sec. a.C. ad oggi: sfide, rischi e prospettive future*. Nuova edizione rivista e aggiornata. Edizioni dell'Università Popolare (Edup).

Marsili, M. (2025b), *Disinformation and Democratic Resilience in the European Union: Lessons from the Covid-19 Pandemic and Election Interference, Studia Administracji i Bezpieczeństwa, 19(19), 195-220. doi:10.5604/01.3001.0055.6584.*

Marsili, M. (2025c), Cognitive Warfare, Disinformation, and Corporate Influence in Europe's Energy Transition: Information Control, Regulation, and Human Rights Implications, *Applied Cybersecurity & Internet Governance*, *4*(1). doi:10.60097/ACIG/214045.

Marsili, M. (2026), *Europe's cognitive security: generative AI, hybrid conflict and democratic resilience, JANUS Yearbook, 24, 1-3. doi:1026619/2183-4822.2026.CJ.5.*

Mill, J.S. (1859). *On Liberty*. London: John W. Parker and Son.

Nocetti, J. (2015). Contest and Conquest: Russia and Global Internet Governance. *International Affairs, 91*(1), 111–130. doi:10.1111/1468-2346.12189.

Nye, J. (2010). Cyber Power. *Belfer Center for Science and International Affairs*. Harvard Kennedy School. https://www.belfercenter.org/publication/cyber-power.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4), 1–16. doi:10.14763/2020.4.1532.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Consolidated text: http://data.europa.eu/eli/reg/2016/679/2016-05-04.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), *OJ L 265, 12.10.2022, pp. 1–66*. http://data.europa.eu/eli/reg/2022/1925/oj.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), *OJ L 277, 27.10.2022, pp. 1–102*. http://data.europa.eu/eli/reg/2022/2065/oj.

United Nations General Assembly, Resolution 217 A (III), *Universal Declaration of Human Rights*, A/RES/217(III), 10 December 1948.