ISSN 3071-9658

European Journal of Interdisciplinary Issues

https://www.eujini.org.pl

Institutional Coordination Models Between Telecommunications Operators and Public Stakeholders

Yevhenii Valiienko [1] *

[1] *Bohdan Khmelnytsky National University of Cherkasy, Cherkasy (Ukraine). Master's Degree in History, Owner of a Telecommunications Company.*

* ***Corresponding Author,*** e-mail: valienko12@ukr.net

ARTICLE INFO

Research Article

Received:
29 September 2025
Revised:
15 November 2025
Accepted:
15 December 2025
Published online:
25 December 2025

DOI: 10.5281/zenodo.19312127

ABSTRACT

This study analyzes the evolution of institutional coordination models between telecommunications operators and public stakeholders, demonstrating the untenability of traditional hierarchical governance methods. Employing qualitative analysis and multilevel modeling, the paper identifies three interaction levels: strategic (macro), applied (meso) and situational (crisis). The article systematizes international experience (European Union, Asia, USA), revealing a global shift from rigid regulation (ex-ante) to collaborative governance (sandbox regulation) and Public-Private Partnership (PPP) models. The theoretical framework of the study is validated by the author's direct operational experience in the US telecommunications market (City Cable USA). This practical perspective confirms that flexible coordination models significantly reduce administrative friction and accelerate infrastructure deployment in highly competitive environments. Particular attention is devoted to the dialectical contradiction between personal data protection and national security imperatives, where the operator acts as an "institutional filter". The research findings substantiate that the efficiency of digital economy development directly correlates with the state's capacity to transition from a fiscal approach to spectrum management to a model of infrastructure co-investment. The study also demonstrates that effective telecom governance increasingly depends on institutional agility, cross-sector trust and the ability to balance public value with commercial sustainability. Particular significance is attached to adaptive regulatory design that supports innovation without undermining competition or civil liberties. These conclusions may be applied in shaping resilient national strategies for digital infrastructure modernization.

KEYWORDS

institutional coordination, telecommunications governance, Public-Private Partnership (PPP), digital infrastructure, regulatory frameworks, data compliance, 5G deployment.

Introduction

Telecommunications infrastructure has today surpassed the threshold of mere technical utility, firmly establishing itself as a fundamental asset of state sovereignty and macroeconomic stability. In this new reality, the traditional duality of "state-regulator" and "operator-service provider" is rapidly becoming obsolete. The formation of a complex institutional architecture, where boundaries of responsibility are blurring is evident (Bauer & Bohlin, 2022). Henceforth, private companies are becoming operators of critical data on a national scale, while public institutions are compelled to adopt flexible market mechanisms to implement social guarantees. Such policy transforms the telecommunications sector into an arena of constant negotiation, where the logic of shareholder value maximization clashes with national security imperatives.

Institutional coordination in this context represents a multilevel governance system covering a spectrum from physical network deployment to algorithmic ethics and data sovereignty. Telecommunications operators, possessing the "last mile" and backbone channels, de facto control citizens' access to digital goods, which imposes quasi-state functions upon them. Conversely, public stakeholders realize that administrative pressure is no longer sufficient to stimulate technological breakthroughs. New mechanisms are required that allow for risk-sharing and the coordination of long-term planning under conditions of high uncertainty.

The economic scale of this interaction dictates the necessity of revising established models. According to 2023 data from the International Telecommunication Union (ITU), the global base of internet users has reached 5.4 billion. However, the rapid pace of digitalization creates a colossal load on infrastructure (ITU, 2023). According to GSMA estimates, the full-scale deployment of 5G networks and preparation for the transition to 6G will require the global telecom industry to invest over 1.5 trillion dollars in the period up to 2030 (GSMA, 2023). Furthermore, a significant portion of these investments must be directed towards zones with low commercial viability, rendering network development impossible solely on market principles without deep integration with state support programs. Unfortunately, even now, despite the scale of digitalization and the frenetic pace of technological development, sparsely populated areas remain without adequate connectivity and network access, as the organization of network coverage there is deemed irrelevant. This is detrimental, as a multitude of people still remain unconnected, while large industrial and well-developed agglomerations are already on the verge of 6G.

Moreover, the very nature of the telecommunications asset has changed. If in the 3G/4G era the focus was predominantly on a "pipe" for traffic transmission, modern infrastructure represents distributed computing power integrated with artificial intelligence and big data (Cave & Nicholls, 2017). This adds a new layer of complexity to the coordination equation.

Questions of cyber resilience, personal data protection and operational transparency become inseparable from issues of cable laying and tower installation. Thus, the search for effective interaction models between operators and public institutions becomes a leading factor in the resilience of the digital economy in the face of global challenges.

Literature Review

In the works of J. M. Bauer and E. Bohlin, the influence of the regulatory environment on innovation in 5G markets is analyzed; the authors demonstrate that the quality of regulation is directly related to operators' investment activity (Bauer & Bohlin, 2022). The International Telecommunication Union (ITU) provides global data on digital development and the scale of internet penetration, forming the empirical basis of the study (ITU, 2023). GSMA focuses on the economic parameters of the mobile industry and the investment needs associated with the deployment of new networks (GSMA, 2023). M. Cave and R. Nicholls substantiate the multifunctional nature of spectrum auctions as an instrument not only of fiscal policy but also of infrastructure policy (Cave & Nicholls, 2017).

A significant theoretical foundation is provided by the works of D. C. North, in which institutions are defined as rules structuring the interaction between the state and the market (North, 1990). R. E. Freeman, within the stakeholder approach, emphasizes the need to consider the interests of

all relevant parties in the governance process (Freeman, 2010). M. Cave, in the concept of the "ladder of investment," shows how regulation can stimulate infrastructure-based competition (Cave, 2006). J. Pfeffer and G. R. Salancik, through resource dependence theory, explain operators' dependence on access to strategic resources and state decisions (Pfeffer & Salancik, 2003). The work of 5G PPP summarizes practices of public-private interaction in the development of 5G infrastructure, confirming the transition toward collaborative governance models (5G PPP, 2021).

Problem Statement

The purpose of this paper is to analyze and conceptualize modern institutional coordination models between telecommunications operators and public stakeholders in the context of global digital transformation, highlighting the limitations of traditional hierarchical governance and the shift toward collaborative, multi-level frameworks. The study aims to identify key levels of interaction, evaluate international best practices, assess the role of public-private partnerships in addressing infrastructure investment gaps, and examine the balance between data protection and national security, ultimately substantiating the importance of institutional agility and adaptive regulation for the sustainable development of the digital economy.

Methods and Materials

The relevance of this research is explained by the pressing situation, where old managerial templates, created in the era of simple voice communication and 3G, demonstrate their untenability in the face of challenges posed by the AI era, 6G and ubiquitous cyber threats. The problem's acuteness is exacerbated by the colossal gap between technological ambitions and financial reality. GSMA estimates the investment deficit at $1.5 trillion by the end of the decade. Under these conditions, neither the state (bureaucratically inert) nor the private sector (constrained by margins) are capable of building the digital infrastructure of the future in isolation.

The search for a balance between the citizen's right to privacy of correspondence and the state's right to security only raises the stakes, rendering this research critically important for understanding how the human digital tomorrow will be governed.

The scientific novelty of the work lies in the conceptualization of institutional coordination as a three-level ecosystem, which facilitates overcoming the fragmentation of existing approaches that view interaction either exclusively through the prism of law or economy. Within a single study, the author Yevhenii Valiienko has systematized and juxtaposed global governance models (European, Asian, North American), identifying a correlation between the type of regulatory regime (harmonization vs state-strategist vs market innovations) and the rates of technological adoption. The author substantiates the transition from "vertical subordination" to "collaborative governance" and identifies specific risks of "regulatory capture" under conditions of technological oligopoly.

An original classification of PPP models based on risk distribution, adapted specifically for the telecommunications sector, is proposed.

This research is based on a qualitative design employing a systems approach to the analysis of institutional interactions. The methodological core of the work is the synthesis of new institutional economics and stakeholder theory (North, 1990; Freeman, 2010). This allowed for viewing the telecommunications sector as a complex ecosystem of contractual relations, where transaction costs and information asymmetry determine the choice of coordination models. To structure the interaction between operators and the state, the method of multilevel modeling was applied. This allowed for decomposing the object of study into three hierarchical levels: macro-level (strategic regulation), meso-level (regional deployment) and situational level (anti-crisis management).

The empirical basis of the research is formed via data triangulation from three categories of sources, covering the period from 2018 to 2024, with a forecasting horizon up to 2030. A unique element of the empirical base is the participant observation method applied within the operational management of City Cable USA. The analysis incorporates internal case studies of interaction between the operator and municipal authorities in the United States, demonstrating the practical efficacy of the

market innovations model in real-world scenarios. Quantitative data from the International Telecommunication Union (ITU) on global internet penetration, GSMA Intelligence forecasts on capital expenditures (CAPEX) for 5G/6G and ENISA analytical reports on cyber threats in the critical infrastructure sector were utilized. A content analysis of "Transparency reports" from leading global operators (Vodafone, Orange, Deutsche Telekom, Verizon) was conducted to assess the volume of state intervention and data disclosure requests. Financial reports of infrastructure companies (Cellnex, China Tower) were also analyzed to assess the efficiency of asset separation models. Texts of key regulatory directives were studied, including GDPR (EU), NIS2 Directive (EU), CBRS system regulations (USA) and national digitalization strategies (K-Network 2030, South Korea).

To identify best practices, comparative legal and comparative economic analysis was applied. The sample of jurisdictions (European Union, USA, Asia-Pacific region) was conditioned by their role as flagships in forming various regulatory paradigms: harmonized (EU), market-driven (USA) and state-centric (Asia).

To assess the efficacy of PPP models and regulatory frameworks, risk analysis matrix instruments and the regulatory ladder of investment theory (Cave, 2006) were employed. This facilitated the classification of models according to the distribution of economic risks between the public and private sectors.

The study has a number of objective limitations. First, the high dynamics of the technological landscape lead to the rapid obsolescence of empirical data. Conclusions relevant for the 5G deployment stage may require adjustment, when transitioning to 6G standards. Second, the analysis is based predominantly on open sources (transparency reports, public strategies), where a significant part of the interaction between operators and intelligence agencies in the sphere of national security is of a confidential nature and remains outside public discourse. Third, the proposed governance models represent "ideal types" and may possess country-specific features conditioned by a unique political context or corruption level, which limits the possibility of direct extrapolation of findings to developing markets with weak institutions.

Results and Discussion

Interaction between telecom companies and public institutions

The interaction between telecommunications operators and public institutions represents a complex, multilayered process. In modern institutional theory, these relations are characterized as a complex ecosystem of resource exchange: the state provides legitimacy and access to scarce resources (radio frequency spectrum, land allocations), while operators provide technological expertise, data and infrastructural coverage (Pfeffer & Salancik, 2003).

It is expedient to divide the architecture of this interaction into three hierarchical levels, each possessing its specific coordination characteristics.

At the macro-level (national), interaction bears a strategic character. Key counterparties here are relevant ministries and national regulators. The primary communication channel involves the formation of long-term industrial policy, including spectrum allocation. Historically, this process was highly centralized. However, with the introduction of 5G standards, a shift towards consultative models is observed. Through industry associations (e.g., GSMA or regional unions), operators actively participate in legislative activities, providing technical expertise to formulate realistic standards (5G PPP, 2021). This constitutes a form of "soft lobbying", which is essential for ensuring regulatory requirements correspond to the physical capabilities of technologies.

At the meso-level (regional and municipal), interaction acquires an applied, often conflict-prone character. It is here that the "landing" of national strategies occurs - the approval of locations for base stations, the laying of fiber-optic communication lines (FOCL) through urban infrastructure and access to municipal property objects. Building density and rigid urban planning norms create bottlenecks that are impossible to overcome without close coordination with local administrations. Statistics indicate that up to 40% of network deployment time is consumed specifically by bureaucratic approval procedures at the local level, forcing operators and municipalities to transition to "one-stop-shop" models to accelerate processes (Analysys Mason, 2020).

The third level is situational or crisis-driven. It has manifested vividly in recent years against the backdrop of global upheavals (the COVID-19 pandemic, geopolitical instability). Under these conditions, emergency interaction protocols are activated. Operators ensure priority communication for emergency services, the dissemination of alerts (cell broadcast) and, in certain cases, provide the state with aggregated population mobility data (Big Data) for epidemiological or security situation monitoring (OECD, 2020).

Here, institutional coordination shifts into an operational headquarters mode, where boundaries between private interest and public duty blur in the name of the common good and national security.

It is important to note changes in the very nature of the dialogue. Where the "Ex-ante" model (preliminary rigid regulation) previously dominated, the "Sandbox regulation" approach is now increasingly applied (Attrey et al., 2020). Within such sandboxes, state bodies allow operators to test new technologies (for example, the use of artificial intelligence in traffic management or IoT solutions) in a limited environment without the rigid application of all existing norms, in order to jointly develop optimal rules of the game for the future.

This finally testifies to a transition from hierarchical management to collaborative governance, where the state and business act as co-authors of the digital environment rather than rivals (Table 1).

Table 1. Evolutionary shift in institutional coordination models

Criteria	Traditional model (hierarchical)	Collaborative model (network-centric)
Dominant logic	Compliance and enforcement (Ex-ante)	Innovation and investment facilitation (Ex-post / Sandbox)
Key instrument	Rigid licensing and fines	Memorandums of Understanding (MoU) and Co-investment
Information flow	Asymmetric (state requests reporting)	Bilateral (data exchange and real-time monitoring)
Spectrum management	Administrative allocation / fiscal revenue focus	Dynamic spectrum sharing / efficiency focus
Crisis response	Directive-based mobilization	Voluntary resource pooling and public safety alignment

Despite the evident efficacy of collaborative models, the deepening integration between operators and the state engenders specific institutional risks, described in the scientific literature as "regulatory capture" (Dal Bó, 2006). As the state increasingly relies on the expertise and data of private entities for decision-making (for instance, in the development of 6G standards or cybersecurity), a danger emerges regarding the displacement of the public policy vector to the benefit of dominant market players.

This creates a coordination paradox: excessive distance between stakeholders leads to the bureaucratic inhibition of innovation, where excessive proximity threatens market oligopolization and the erection of entry barriers for new technological startups.

Consequently, the efficacy of the interaction model is gauged not by the speed of decision-making, but by the existence of transparent public oversight mechanisms that prevent the privatization of the regulatory function (Figure 1).

Regulatory frameworks governing civilian telecommunications infrastructure

The regulatory framework governing civilian telecommunications infrastructure constitutes a complex institutional matrix determining the sector's economic efficiency and technological agility. Unlike other utility sectors (water supply, energy), telecommunications are characterized by a high rate of technological obsolescence, which requires exceptional adaptability from frameworks. Static laws here become an impediment to innovation faster than in any other sphere.

The foundation of regulation in most developed jurisdictions is the concept of technological neutrality (Maxwell & Bourreau, 2015). It implies that legal norms should regulate the service functionality (for example, voice or data transmission) and not the specific technology of its implementation (whether fiber optics, copper or a satellite channel). This permits avoiding the necessity to rewrite legislation for every new generation of connectivity (from 4G to 5G and beyond).

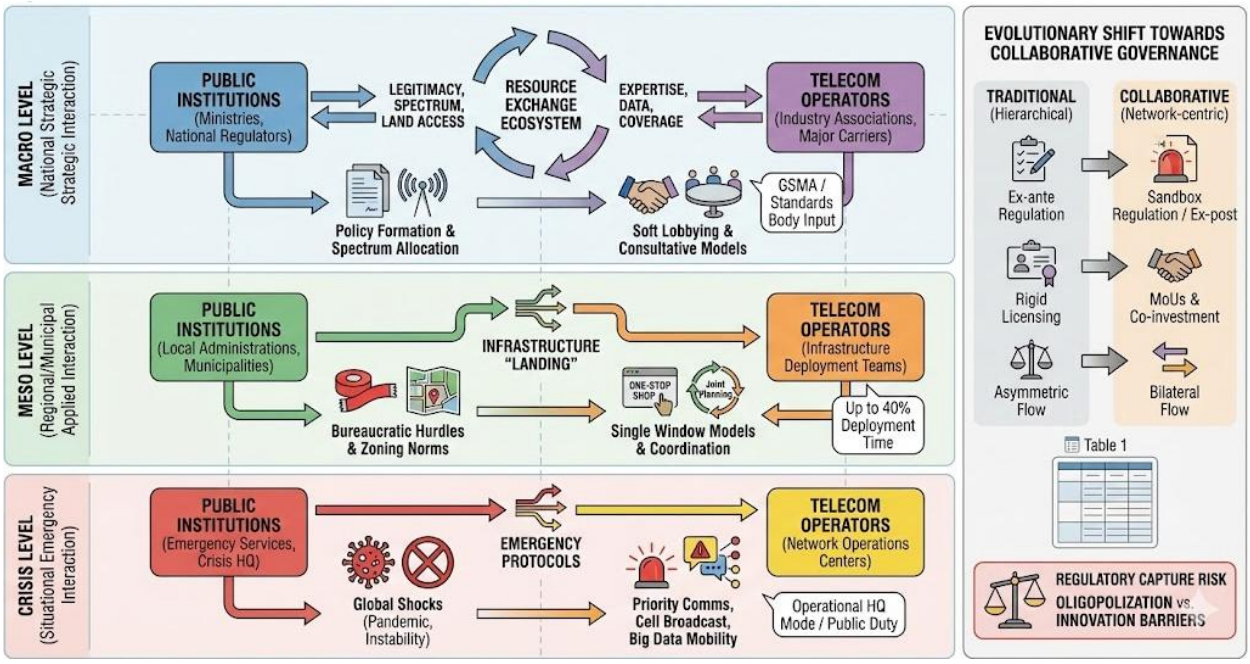

Figure 1. Multiplayered institutional coordination ecosystem in telecommunications (Generative artificial intelligence was used for creation scheme)

A central element of the regulatory landscape is spectrum management. Spectrum is a scarce natural resource and the efficiency of its allocation directly influences the country's GDP. Modern regulatory approaches are shifting from administrative allocation ("command and control") to market mechanisms, primarily auctions (Kwerel & Williams, 2002). However, a regulatory dilemma arises here: fiscal maximization (selling frequencies as expensively as possible to replenish the budget) often comes into conflict with investment goals (a high license price deprives the operator of funds for tower construction). Advanced legal regimes resolve this through the implementation of the "use-it-or-lose-it" principle and the authorization of a secondary frequency market (spectrum trading), which enhances the overall liquidity of the asset.

The second regulatory block concerns access to infrastructure and competition. Since the construction of duplicate networks is economically inexpedient (especially the "last mile"), regulators introduce obligations for non-discriminatory access to passive infrastructure (ducts, poles, masts). Key here is the concept of SMP (Significant Market Power) (Baldwin et al., 2012). Operators recognized as dominant (usually former state monopolies) fall under rigid ex-ante regulation. They are obliged to provide competitors access to their networks at regulated tariffs (the LLU - Local Loop Unbundling model). This prevents market monopolization and lowers the entry barrier for alternative providers (Figure 2).

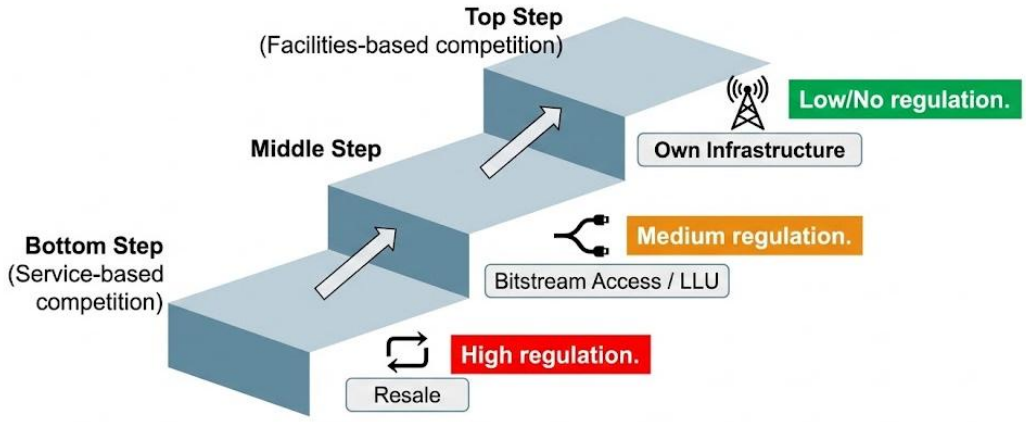

Figure 2. The ladder of investment: regulatory progression from service-based to facilities-based competition

The regulation of network sharing warrants particular attention (see: Figure 3. Taxonomy of mobile network sharing) (Mölleryd et al., 2014). Amidst escalating capital expenditures (CAPEX) for 5G, legislation in many jurisdictions has begun to encourage sharing models. Passive Sharing constitutes the joint utilization of masts and sites (this model is the least regulated). Active Sharing involves the shared use of antennas and transceivers (requiring rigorous antitrust analysis). Core Network Sharing implies the consolidation of network cores (the most risky and frequently prohibited due to considerations of national security and network resilience).

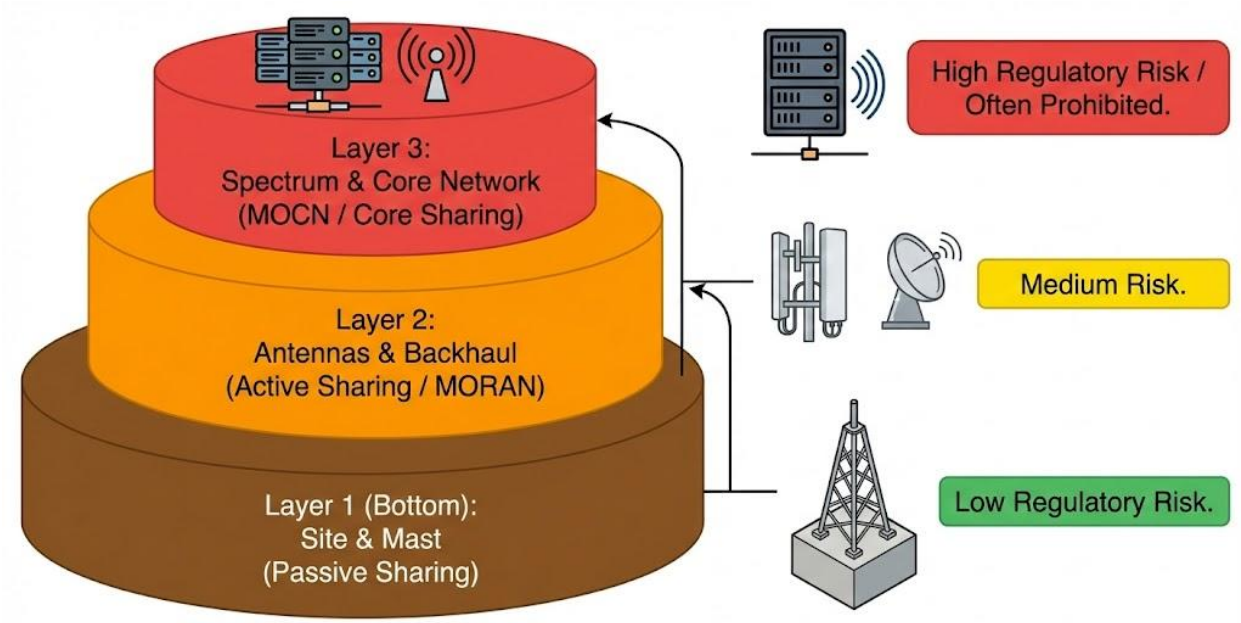

Figure 3. Taxonomy of mobile network sharing

Finally, the regulatory framework encompasses obligations regarding Universal Service Obligation (USO) (Falch & Henten, 2018). This constitutes a social contract between the state and operators. In exchange for the right to operate in high-yield urban markets, operators are obliged (or subsidized through special funds) to provide connectivity in economically unattractive rural areas. Modern legal frameworks are transforming USO from the provision of a simple "payphone" to the guarantee of broadband internet access (Broadband USO) as a fundamental human right, enshrining minimum data transmission speeds at the legislative level.

Thus, modern regulatory frameworks are evolving from the role of a "policeman" to the role of a "market architect", creating conditions wherein competition stimulates investment, while infrastructural monopolies remain under strict control to obviate market failures.

Public-private partnership models in telecommunications

Public-Private Partnership (PPP) models in telecommunications emerge as a response to classic market failure. In zones characterized by low population density and complex topography, capital expenditures (CAPEX) for network deployment are disproportionately high compared to projected average revenue per user (ARPU) (Nucciarelli et al., 2010. At this juncture, the purely market-driven model ceases to function and a digital divide arises. In this context, PPP serves as an instrument for hedging investment risks, rendering otherwise unprofitable projects marginally viable for the private operator.

Global practice has elaborated three unique baseline architectures for such partnerships, distinguished by the degree of state involvement in operational activities (Figure 4).

The "Gap Funding" model (subsidy for the viability gap). This is the least invasive approach, where the state does not become the owner of the infrastructure. The private operator retains full ownership rights and management of the network, but receives a one-time subsidy (grants) to cover a portion of the capital expenditures during the construction phase. The distribution mechanism for such subsidies is typically implemented through reverse auctions (World Bank, 2018). The state

announces target coverage indicators (for example, a gigabit channel in a remote settlement) and the contract is awarded to the operator requesting the minimum amount of state support to realize the project. This model predominates in the European Union, as it minimizes the distortion of competition and incentivizes operators to optimize costs.

Model Type	Infrastructure Ownership	Operational Management	Investment Risk	Commercial Risk
Private DBO (Gap Funding)	Private	Private	Shared (State subsidies)	Private
Public Outsourcing (Concession)	Public	Private	Public	Shared
Joint Venture	Shared (SPV)	Shared	Shared	Shared

Figure 4. Allocation of responsibilities in telecom PPP models

The Concession model (Public DBO - Design, Build, Operate). In this scenario, the state assumes the role of investor in passive infrastructure. A municipality or state agency finances the laying of "dark fiber" and the construction of towers, retaining ownership thereof. Subsequently, this asset is transferred for long-term operation to a private partner (a wholesale-only operator), who installs active equipment, "lights up" the network, and sells services to retail providers. The economic rationale of the model lies in the state assuming the "heavy" risks of construction recoupment (an investment return period of approximately 15–20 years), allowing private business to concentrate on service provision and traffic management (a cycle of 5-7 years). This is particularly effective for creating neutral backbone networks to which all market players enjoy equal access.

The "Anchor Tenant" model (demand aggregation/anchor tenancy) (Gómez-Barroso & Feijóo, 2010). Here, the state does not invest in construction directly, but utilizes its purchasing power. Public institutions (schools, hospitals, administrative centers) act as a guaranteed "anchor" client, concluding long-term service contracts with the operator prior to the commencement of network construction. The aggregated demand of the public sector mitigates the commercial risk of demand uncertainty (demand risk). Cognizant of a guaranteed revenue stream from budgetary institutions for 5-10 years in advance, the operator can justify investments in constructing the "last mile" for the entire locality, including households.

However, notwithstanding its attractiveness, PPP in telecommunications entails the risk of the "crowding out effect" on private investment (Wallsten, 2000). Should the state commence subsidizing network construction in a region where private enterprise intended independent development (so-called "grey zones"), this disrupts market incentives. Consequently, a critically important stage of any PPP project is preliminary mapping - a detailed territorial analysis for the precise delineation of zones, where support is requisite ("white zones") and where it is detrimental ("black zones").

Thus, contemporary PPP models are evolving from direct state construction towards complex financial instruments for risk redistribution, where the state purchases not cable and concrete, but social impact in the form of digital service accessibility.

Data protection, transparency and compliance in telecom operations

In the digital epoch, the role of telecommunications operators has undergone substantial modification. From mere "signal transmitters", they have evolved into global custodians of human digital identity. Every click, call or movement leaves a "digital footprint" (metadata), which frequently reveals far more about an individual's behavior and habits than the actual content of their

conversations (Hongladarom & Zuboff, 2023). In this context, data protection and compliance have ceased to be a mundane legal formality. Today, it constitutes a central element of business architecture, determining directly whether users place trust in the digital ecosystem or harbor fear towards it.

Institutional coordination here resembles a tightrope walk, as operators are compelled to balance between the rigid privacy imperative and the equally stringent security imperative (see: Figure 5. The "Gatekeeper" mechanism: lawful interception + data disclosure process).

On one side of the scale lie user interests and the law. The European GDPR regulation has become the global benchmark here. It mandates not merely "not losing" data, but constructing networks according to the privacy by design principle: collecting a minimum of information, encrypting traffic and being prepared to "forget" the subscriber at any moment upon their request. An error here comes at a high cost: fines of up to 4% of global turnover and instantaneous reputational loss (Voigt & Von dem Bussche, 2017).

On the other side of the scale lie the interests of the state. Legislation (for instance, SALI procedures - lawful interception) obliges operators to cooperate with law enforcement agencies. Here, a most complex engineering and ethical paradox arises: the operator is obliged to build a system impregnable to hackers (cyber resilience), yet simultaneously leave a "backdoor" within it for intelligence services possessing a judicial warrant. Managing this conflict requires surgical precision and transparent protocols to exclude the risk of transforming lawful interception into an instrument of mass surveillance.

The industry's response to this pressure has been "corporate diplomacy" in the form of Transparency reports (Parsons, 2019). Market giants such as Vodafone, Orange and Deutsche Telekom annually publish detailed statistics regarding how many times intelligence agencies requested data and, more importantly, how many times they were refused. This serves as an important banner for all concerned about their confidentiality: "- We are not blind executors, we filter requests and protect your rights if the authorities' demands are legally incorrect".

The situation is further complicated by geopolitics. Under conditions of hybrid warfare, communication networks have become a primary target and new directives (NIS2 in the EU) impose responsibility upon operators for the security of the entire supply chain. Now, the operator must conduct a rigorous audit of its vendors, excluding equipment from "high-risk" jurisdictions. Effectively, the hardware procurement process has become a political act.

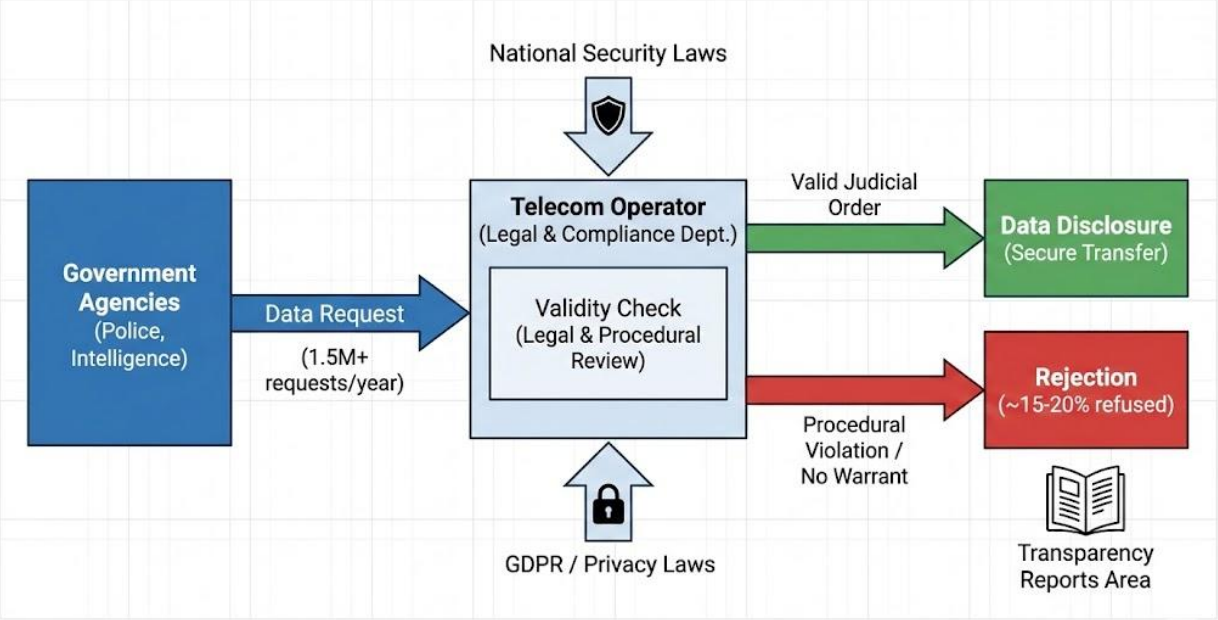

Figure 5. The "Gatekeeper" mechanism: lawful interception + data disclosure process

The scale of this pressure is corroborated by dry statistical figures. Interaction with state authorities has reached industrial proportions. According to aggregated data from leading operators (Verizon,

Vodafone, Orange), the sector processes over 1.5 million government requests globally per annum. It is noteworthy that corporate legal teams operate effectively: according to Vodafone data, approximately 15-20% of requests are rejected as non-compliant with procedural norms. Compliance constitutes a matter of financial survival. According to the IBM Cost of a Data Breach Report, the average cost of a data breach in the telecommunications sector exceeds $4 million per incident, surpassing average market indicators (IBM, 2024). Since the enactment of GDPR, EU operators have incurred fines totaling over €150 million. Illustrative is the case of the Italian regulator against TIM (a fine of €27.8 million), which demonstrated that penalties are now imposed not for technical failures, but for aggressive marketing and negligence in data processing.

Telecommunications serves as a "lightning rod" for attacks. According to ENISA data, the industry consistently ranks among the top three most targeted sectors, absorbing 25% of all high-magnitude DDoS attacks aimed at destabilizing national infrastructure (ENISA, 2023).

Thus, modern compliance in telecommunications has long transcended the level of mere "instruction adherence". It now represents a dynamic risk management system, where the operator is compelled to continuously maneuver between the protection of civil rights, national security requirements and the physical resilience of its own networks.

International best practices for civilian telecommunications governance

Analysis of the global landscape indicates that effective telecommunications governance has ceased to be a nationally isolated process. In the context of a cross-border digital economy, a pool of universal managerial solutions is forming, having proven their efficacy across various jurisdictions. Comparative analysis facilitates the identification of key regional models demonstrating diverse approaches to the balance between state control and market freedom (Figure 6).

The European Union offers a reference model for managing a fragmented market (27 national regulators) through harmonization and rights protection, where the priority is the creation of a single digital market and consumer protection. A key achievement was the mandatory abolition of roaming charges ("Roam like at home", 2017), which required complex coordination of wholesale tariffs between operators of different countries (European Commission, 2017). Another core mechanism is the "EU Connectivity Toolbox". This is a set of recommendations for member states on the unification and acceleration of permit granting procedures for construction, which is critical for 5G network densification. Stringent regulation stimulates operators to seek efficiency at scale. Companies such as Deutsche Telekom and Vodafone actively lobby for "in-market consolidation" (mergers within a single country, such as the attempted merger of Orange and MásMóvil in Spain) to compensate for the decline in roaming revenues and high compliance costs. In response to GDPR, initiatives such as Utiq have emerged - a joint venture of major European operators to create an ethical advertising identifier.

The experience of leading Asian economies demonstrates the efficacy of a proactive industrial policy (the state as a strategist), where the regulator acts not as an arbiter, but as a visionary and co-investor directing the market towards long-term technological goals. In South Korea, the "K-Network 2030" strategy entails direct state investment in R&D for 6G and tax incentives for operators implementing advanced networks (Ministry of Science and ICT, 2023). In China, the state directively resolved the issue of infrastructure duplication by forcibly merging the tower assets of three state operators into China Tower Corporation - the world's largest infrastructure company, which allowed for the deployment of 5G at unprecedented speed. The Singaporean regulator IMDA finances pilot zones jointly with operators Singtel and StarHub for testing autonomous transport and port logistics based on 5G, creating guaranteed demand for new technologies prior to their commercial maturity.

The USA demonstrates a model of market innovations and dynamic spectrum, where the state sets minimal frameworks, relying on competition and private sector innovation, particularly in the management of scarce resources. The primary breakthrough is the transition from static auctions to dynamic spectrum access. The CBRS (Citizens Broadband Radio Service) system in the USA allows civilian operators to utilize military frequencies (3.5 GHz), when they are not occupied by the navy. This is a three-tiered priority system managed by automated databases, which allows for the unfreezing of a vast volume of scarce resource. Light-touch regulation allowed hyperscalers (AWS, Google, Microsoft Azure) to actively enter the telecom sector, offering operators (Dish Network or

AT&T) the option to migrate network cores to the public cloud, which radically reduces CAPEX and accelerates service deployment. Furthermore, new players have emerged - spectrum administrators, such as Federated Wireless, ensuring the technical operation of the CBRS system.

The effectiveness of this liberalized approach is exemplified by the operational case of City Cable USA. As a Director of Operations within this framework, the author observed that minimizing ex-ante bureaucratic barriers allowed the company to optimize its coordination with public stakeholders. Instead of lengthy permitting procedures characteristic of rigid hierarchical models, the market-centric approach enabled City Cable to utilize existing municipal infrastructure more efficiently and respond rapidly to shifts in local demand. This serves as empirical proof that the US model of institutional coordination fosters not only competition, but also operational agility for mid-sized operators

Feature	EU Model (Consumer-Centric & Harmonized)	Asian Model (Industrial-Centric & Strategist)	US Model (Market-Centric & Innovative)
Primary Goal	Single Digital Market & Consumer Rights	Tech Leadership & Industrial Output (Industry 4.0)	Innovation, Competition & Market Efficiency
State Role	Harmonizer & Regulator (e.g., BEREC)	Strategist & Co-investor (Direct R&D)	Arbiter (Light-touch), Enabler
Spectrum Policy	High Auction Fees (fiscal focus)	Administrative Allocation / Low Fees	Dynamic Sharing (CBRS), Market-driven
Key Strategy Example	“Roam like at Home”, GDPR	"K-Network 2030" (KR), China Tower Corp (CN)	Dynamic Spectrum Access (CBRS)
Corporate Examples	Deutsche Telekom, Vodafone, Cellnex	Singtel, StarHub, China Mobile	AT&T, Dish Network, Federated Wireless, Hyperscalers (AWS/Google)

Figure 6. Comparative matrix of global telecommunications governance models

Irrespective of the specific regional model, the structural separation of passive infrastructure into independent business entities has emerged as a universal best practice. This facilitates the mitigation of inefficient infrastructure redundancy (three distinct towers belonging to three operators situated on a single hill). The European entity Cellnex acquires tower assets from operators across the continent, thereby establishing itself as a neutral host. In Africa, IHS Towers assumes the critical function of power provisioning (utilizing solar panels and generators) amidst grid instability, delivering a turnkey “Power-as-a-Service” solution to operators.

International experience attests that the most successful jurisdictions are transitioning from a fiscal perspective on telecommunications (prioritizing the maximization of budgetary revenues from spectrum auctions) to an infrastructural perspective, where the regulator is prepared to forego immediate fiscal gains in favor of the long-term growth of the digital economy.

Conclusion

The conducted research on institutional coordination models within the telecommunications sector substantiates the assertion that the traditional dichotomy of “state-regulator” vs “business-operator” has definitively transmuted into a complex ecosystem of interdependence. Telecommunications operators have de facto assumed quasi-state functions regarding the assurance of cyber resilience and the management of critical data, where the state is compelled to integrate into market processes via mechanisms of co-investment and risk-sharing. The transition from “command and control” management to collaborative governance and the utilization of “regulatory sandboxes” constitutes an imperative prerequisite for the deployment of 6G and AI technologies.

Analysis of the funding gap demonstrates that market mechanisms are incapable of independently securing ubiquitous digital coverage. PPP models (Gap Funding, Concessions, Anchor Tenant) have ceased to be optional instruments and have become the cornerstone of infrastructural development. Successful global experience validates the efficacy of structural asset separation (TowerCos) and the transition from the fiscal maximization of spectrum value to the incentivization of capital expenditures.

Interaction within the data sphere is characterized by an institutionalized conflict between the right to privacy and national security imperatives. Telecommunications operators act as "Gatekeepers", whose efficacy is measured by the capacity to filter illegitimate state requests through transparent compliance protocols. The proliferation of cyber threats and the politicization of supply chains render security issues a dominant factor in the selection of technological partners.

Comparative analysis of regional models (EU, Asia, USA) indicates that, despite divergences in approaches (consumer protection vs industrial policy vs market innovations), a convergence is observable towards dynamic spectrum access and the unification of construction standards.

Thus, the resilience of the national digital economy in the coming decade will be determined by the quality of the institutional environment ("institutional agility") capable of harmonizing the interests of private capital and the public good under conditions of high uncertainty.

References

5G PPP. (2021). *5G Infrastructure Public Private Partnership*. European Commission. https://5g-ppp.eu/wp-content/uploads/2021/10/5GInfraPPP_10TPs_Brochure2021_v1.0.pdf

Analysys Mason. (2020). *Reducing barriers to 5G deployment: The role of local government*. https://www.analysysmason.com/contentassets/6ce9b6fbc48f410db7482906ab88adff/analysys_mason_first_phase_5g_deployment_aug2020_rdns0.pdf

Attrey, A., Lesher, M., & Lomax, C. (2020). *The role of sandboxes in promoting flexibility and innovation in the digital age* (OECD Going Digital Toolkit Notes, No. 2). OECD Publishing. https://doi.org/10.1787/cdf5ed45-en

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding Regulation: Theory, Strategy, and Practice*. Oxford University Press. https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001

Bauer, J. M., & Bohlin, E. (2022). Regulation and innovation in 5G markets. *Telecommunications Policy, 46*(4), 102260. https://doi.org/10.1016/j.telpol.2021.102260

Cave, M. (2006). Encouraging infrastructure competition via the ladder of investment. *Telecommunications Policy, 30*(3–4), 223–237. https://doi.org/10.1016/j.telpol.2005.09.001

Cave, M., & Nicholls, R. (2017). The use of spectrum auctions to attain multiple objectives: Policy implications. *Telecommunications Policy, 41*(5–6), 367–378. https://doi.org/10.1016/j.telpol.2016.12.010

Dal Bó, E. (2006). Regulatory capture: A review. *Oxford Review of Economic Policy, 22*(2), 203–225. https://doi.org/10.1093/oxrep/grj013

ENISA. (2023). *ENISA Threat Landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

European Commission. (2017). *Roam like at home as of summer 2017*. EU Publications. https://epthinktank.eu/2017/08/07/roam-like-at-home-as-of-summer-2017-what-is-europe-doing-for-its-citizens/

Falch, M., & Henten, A. (2018). Universal service in a digital world: The demise of postal services. In *22nd ITS Biennial Conference, Seoul 2018: Beyond the boundaries: Challenges for business, policy and society* (Paper 190416). International Telecommunications Society (ITS). https://ideas.repec.org/p/zbw/itsb18/190416.html?utm_source=chatgpt.com

Freeman, R. E. (2010). *Strategic Management: A Stakeholder Approach*. Cambridge University Press. https://doi.org/10.1017/cbo9781139192675

Gómez-Barroso, J. L., & Feijóo, C. (2010). A conceptual framework for public-private interplay in the telecommunications sector. *Telecommunications Policy, 34*(9), 487–495. https://doi.org/10.1016/j.telpol.2010.01.001

GSMA. (2023). *The Mobile Economy 2023*. GSMA Intelligence. https://www.gsmaintelligence.com/research/the-mobile-economy-2023

Hongladarom, S., & Zuboff, S. (2023). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *AI & Society*, (38), 2359–2361. https://doi.org/10.1007/s00146-020-01100-0

IBM. (2024). *Cost of a Data Breach Report 2024*. IBM Security. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

ITU. (2023). *Facts and Figures 2023: Measuring digital development*. ITU Publications. https://www.itu.int/itu-d/reports/statistics/wp-content/uploads/sites/5/2023/11/Measuring-digital-development-Facts-and-figures-2023-E.pdf

Kwerel, E., & Williams, J. (2002). *A proposal for a rapid transition to market allocation of spectrum*. FCC Office of Plans and Policy. https://docs.fcc.gov/public/attachments/DOC-228552A1.pdf

Maxwell, W., & Bourreau, M. (2014). Technology neutrality in Internet access. *Computer and Telecommunications L. Rev.*, (2014). https://dx.doi.org/10.2139/ssrn.2529680

Ministry of Science and ICT. (2023). *K-Network 2030 Strategy*. Republic of Korea Government. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=783

Mölleryd, B. G., Markendahl, J., & Sundquist, M. (2014, June 22–25). Is network sharing changing the role of mobile network operators? [Paper presentation]. In *25th European Regional Conference of the International Telecommunications Society (ITS) "Disruptive Innovation in the ICT Industries: Challenges for European Policy and Business"*. Brussels: International Telecommunications Society (ITS). https://hdl.handle.net/10419/101392

North, D. C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511808678

Nucciarelli, A., Sadowski, B. M., & Achard, P. O. (2010). Emerging models of public-private interplay for European broadband access: Evidence from the Netherlands and Italy. *Telecommunications Policy, 34*(9), 513–527. https://doi.org/10.1016/j.telpol.2010.07.004

OECD. (2020). *Keeping the Internet up and running in times of crisis*. OECD Policy Responses to Coronavirus (COVID-19). https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/05/keeping-the-internet-up-and-running-in-times-of-crisis_f7ea0978/4017c4c9-en.pdf

Parsons, C. (2019). The (In)effectiveness of Voluntarily Produced Transparency Reports. *Business & Society, 58*(1), 103–131. https://doi.org/10.1177/0007650317717957

Pfeffer, J. and Salancik, G.R. (2003). *The External Control of Organizations: A Resource Dependence Perspective*. Stanford Business Books, Stanford. https://www.scirp.org/reference/referencespapers?referenceid=1728829

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide* (1st ed.). Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Wallsten, S. J. (2000). The effects of government-industry R&D programs on private R&D: The case of the Small Business Innovation Research Program. *RAND Journal of Economics, 31*(1), 82–100. https://ideas.repec.org/a/rje/randje/v31y2000ispringp82-100.html

World Bank. (2018). *Innovative Business Models for Expanding Broadband Infrastructure and Services*. World Bank Group. https://documents1.worldbank.org/curated/en/674601544534500678/pdf/Main-Report.pdf