

THE LOGIC OF STATE-MARKET PARTNERSHIPS IN FOREIGN POLICY: DIGITAL HEGEMONY AND SURVEILLANCE CAPITALISM

Dr. Siddık Arslan*

Deputy Secretary General of Erzurum Metropolitan Municipality, Türkiye.

*Corresponding Author

Dr. Siddık Arslan

Deputy Secretary General of Erzurum Metropolitan Municipality, Türkiye.

Article History

Received: 17.07.2025

Accepted: 04.09.2025

Published: 22.10.2025

Abstract: In the twenty-first century, foreign policy has undergone profound transformation through control of digital infrastructure, management of data flows, and determination of information production processes. This study examines how state-market partnerships shape foreign policy under conditions of digital hegemony and surveillance capitalism, through which mechanisms they execute power transfer, and how they restructure the international order. The fundamental research question is: How do state-market partnerships transform foreign policy under conditions of digital hegemony and surveillance capitalism, and how does this process reshape the international system? The hypothesis posits that digital hegemony and surveillance capitalism reconstruct foreign policy at infrastructural, algorithmic, and epistemic levels through state-market partnerships, generating a new logic of power based on information control, behavioral steering, and reality construction beyond traditional definitions of power. The study aims to bring a new conceptual perspective to foreign policy analysis and provide theoretical and analytical tools necessary for understanding power relations in the digital age. Methodologically, a qualitative, analytical, and inductive research design combining critical political economy and structural-constructivist approaches has been adopted. Data collection was conducted through multi-layered document analysis based on academic literature, state digital policy documents, and corporate reports of technology companies. Findings demonstrate that state-market partnerships transform foreign policy at three levels: construction and standardization of digital systems at the infrastructural level, control of content visibility and information circulation at the algorithmic level, and determination of reality definitions and information legitimacy at the epistemic level. Consequently, foreign policy in the digital age is shaped not through military or diplomatic instruments but through algorithmic competition and epistemic domination. The study contributes conceptually, theoretically, and analytically to the literature by explaining the connection between digital hegemony and surveillance capitalism from a foreign policy perspective.

Keywords: Digital Hegemony, Surveillance Capitalism, State-Market Partnerships, Foreign Policy, Infrastructural Power, Epistemic Authority, Algorithmic Control.

This is an open access article under the [CC BY-NC](https://creativecommons.org/licenses/by-nc/4.0/) license



1. Introduction

Since the second decade of the twenty-first century, the fundamental operating logics of global politics have undergone a profound transformation. Power is no longer defined solely through army size, weapons technology, or economic production capacity. What is determinative at the international level is the extent to which information infrastructures, data flows, and their governance mechanisms are controlled. This new reality has reshaped the traditional roles of states and corporations, blurred the boundaries between them, and fundamentally expanded the toolkit of foreign policy. **The state** refers to the form of political

organization that possesses the legitimate monopoly of violence to maintain social order, determine rules, protect security, and represent public authority; while **the market** represents the economic sphere encompassing companies, entrepreneurs, and their commercial networks that produce goods and services, develop technological innovation, and compete—particularly digital platforms and technology infrastructures. The new architecture of power jointly created by these two actors is redefining power relations at both national and international levels and occupies a central position in understanding contemporary foreign policy.

Cite this article:

Arslan, S., (2025). THE LOGIC OF STATE-MARKET PARTNERSHIPS IN FOREIGN POLICY: DIGITAL HEGEMONY AND SURVEILLANCE CAPITALISM. *ISAR Journal of Economics and Business Management*, 3(10), 39-53.

At the core of this transformation lies the relationship between surveillance capitalism and digital hegemony. **Surveillance capitalism** is the process through which companies systematically collect data from people's online behavior and use this data for prediction, steering, and control purposes to generate economic value (Mejias & Couldry, 2024; Lamdan, 2023; Zuboff, 2019). This system creates a form of production that transforms individuals' digital footprints into raw material, enabling the prediction and shaping of future behaviors. Surveillance capitalism is a mechanism that monitors users' preferences, emotional responses, social relationships, and decision-making processes, converting this information into market value and eroding individuals' autonomy. Surveillance capitalism is not merely an arena of economic gain; it is simultaneously a power mechanism that enables the steering of individuals' preferences, emotions, and decisions, thus playing a role in shaping social perceptions and political processes. On the other hand, **digital hegemony** refers to a country's, political community's, or actor's establishment of a superior position over internet infrastructure, digital platforms, data centers, cloud systems, data flows, software standards, and digital norms—being the determinative power in this domain and possessing the capacity to set the rules of the global digital architecture (Couldry & Mejias, 2024; Alexander et al., 2025; DeNardis, 2020; Fuchs, 2017). Digital hegemony expresses the power to determine which information reaches which geographies, which content becomes visible, which actors can be effective in the digital realm, and which technological standards receive universal acceptance. In other words, digital hegemony concerns which actor sets the standards of the global information architecture, decides which data flows in which direction and how, who defines digital behavioral norms, and determines which platforms provide access to which content. When these two concepts come together, it becomes evident that foreign policy is now conducted not only through diplomatic negotiations, economic sanctions, or military interventions but also through control of digital infrastructures, algorithmic steering, management of information production processes, and operation of behavioral prediction mechanisms.

In the digital age, the traditional division of labor between states and corporations is disappearing and giving way to **state-market partnerships**. These partnerships are based on a symbiotic structure that operates on the basis of mutual interest and interdependence for both parties. While states use the data infrastructures, platform networks, algorithmic capabilities, and user access capacities held by large technology companies as foreign policy instruments, corporations expand on a global scale under the legal regulatory protection, international diplomatic support, intellectual property guarantees, market access opportunities, and security umbrella provided by states (Chander & Sun, 2023; Shah & Kirchhoff, 2024; Farrell and Newman, 2019; Bradford, 2023). This mutual interdependence demonstrates how state sovereignty is reproduced not only within national borders but also along digital networks and data flows. Consequently, foreign policy is ceasing to be merely a state-centered activity; it is becoming a new power domain jointly produced by state and market, mutually nourishing and strengthening each other. This power domain possesses **infrastructural, algorithmic, and epistemic** qualities beyond military, diplomatic, and economic instruments.

At this juncture, it is necessary to reconsider the scope of the **foreign policy** concept. In the traditional sense, foreign policy has been defined as the totality of strategic relations, decisions, actions, and attitudes that a state conducts with other states, international organizations, and global actors to protect its national interests, ensure its security, and strengthen its position in the international system. Furthermore, foreign policy is a concept that explains how the state uses all its resources and instruments to achieve its political, economic, cultural, diplomatic, and military objectives in the international arena, which alliances it forms, which strategies it adopts, and which discourses it produces. However, in the digital age, this definition is expanding, and foreign policy now encompasses the construction and management of information infrastructures, the design and supervision of algorithms, the control of data flows, the determination of digital standards, the formation of cybersecurity policies, and the shaping of digital norms. Foreign policy thus becomes a reflection not only of interstate interactions but also of power relations and information asymmetries within digital ecosystems. Therefore, state-market partnerships are becoming the fundamental carriers and effective implementers of these new and invisible dimensions of foreign policy.

In the literature, the concepts of surveillance capitalism and digital hegemony are generally addressed in separate disciplines and different contexts. While Zuboff (2019) examines surveillance capitalism through the axis of economics and sociology, focusing on private companies' data extraction practices, authors such as DeNardis (2020) and Nye (2011) discuss digital hegemony from the perspective of internet governance, cyber power, and infrastructural control. However, insufficient conceptual and theoretical analysis has been conducted regarding the interaction of these two concepts at the foreign policy level, the role of state-market partnerships in this interaction, and how these partnerships transform international power production mechanisms. In particular, there exists a significant analytical gap concerning how digital hegemony articulates with surveillance capitalism, how this articulation diversifies foreign policy instruments, and through which mechanisms it reshapes the international balance of power. Current studies mostly address digital hegemony in the context of technical governance (DeNardis, 2020), cyber sovereignty debates (Kadlecová, 2024; Qiao-Franco, 2024: 1-9), or digital sovereignty policies (Jelinek, 2023; Donnelly, Ríos Camacho & Heidebrecht, 2024: 2226-2245); while surveillance capitalism literature (Zuboff, 2019; Couldry and Mejias, 2019) predominantly focuses on the axis of economics, society, and individual privacy. Therefore, there exists a significant conceptual and analytical gap regarding the mutual interaction of these two processes within **foreign policy rationality**, the functional logic of state-market alliances in digital power production, and how these partnerships materialize in the international system.

In this context, the fundamental question of the article is: **Under conditions of digital hegemony and surveillance capitalism, how do state-market partnerships shape foreign policy, through which mechanisms, instruments, and logics do they execute power transfer, and how does this process restructure the international order?** This question interrogates how new forms of power emerging in international relations theory—particularly power relations based on digital infrastructure, data

sovereignty, and information asymmetry—can be integrated into foreign policy analysis.

Answering this question will not only provide a new perspective to foreign policy analysis but also enable the analysis of the logic of power, forms of power production, and practices of sovereignty in the contemporary international order. Because while surveillance capitalism transforms individual behaviors into data and converts them into economic values, digital hegemony constructs the geopolitical equivalent of these economic values and data flows—namely, international spheres of influence and dependency relations. In this process, data becomes not merely an economic commodity but also a strategic resource, redefining states' capacity for influence, control, and steering in foreign policy. The intersection of these two processes becomes the invisible foundations, hidden power sources, and new mechanisms of power for state-market partnerships in foreign policy. Therefore, foreign policy should now be viewed not only as a reflection of diplomatic interactions but also as a reflection of epistemic and behavioral control strategies conducted through digital infrastructures.

The fundamental hypothesis of this article can be summarized as follows: **Digital hegemony and surveillance capitalism are reconstructing foreign policy at infrastructural, algorithmic, and epistemic levels through state-market partnerships; this process is generating a new logic of power based on information control, behavioral steering, and reality construction beyond traditional definitions of power.** This reconstruction points to an era in which the international balance of power is no longer measured by military deterrence or economic magnitude but by the capacity to steer information flows and shape digital networks. This hypothesis assumes that by combining states' control over digital infrastructures with market actors' data production and processing capacity, foreign policy is no longer merely state actions but the complex and multi-layered product of state-market cooperation. At the same time, this hypothesis suggests that international power relations are now determined not only through military capacities, economic magnitudes, or diplomatic networks but also through access to digital infrastructures, supervision of data flows, and the ability to influence algorithmic design. Consequently, the article conceptualizes foreign policy in the digital age as a hybrid power domain shaped through both infrastructural dependency and epistemic domination.

The aim of the study is to explain the role of state-market partnerships in the foreign policy-making, implementation, and legitimation processes in the digital age within a conceptual framework and to multidimensionally reveal how these partnerships create a mechanism of power production, transfer, and transformation. In line with this aim, the causal and functional connection between surveillance capitalism and digital hegemony will be analyzed; states' sovereignty pursuits and strategies over digital infrastructures will be related to market actors' data extraction logic and profit models; a new foreign policy interpretation and critical perspective will be developed regarding the dimensions of legitimacy, transparency, accountability, democratic oversight, and dependency in the use of digital power. Thus, the study will reveal that digital transformation is not merely a technological change but a structural rupture in which international power relations, understanding of sovereignty, and foreign policy instruments undergo a profound transformation.

The significance and originality of this study materializes at four fundamental points. First, by integrating the concepts of digital hegemony and surveillance capitalism into foreign policy analysis, it offers an interdisciplinary synthesis among international relations, political science, economics, and communication studies. Second, by explaining the functional and structural role of state-market partnerships in foreign policy through a conceptual model, it fills a significant gap in the literature and proposes a new analytical framework. Third, it offers researchers, policymakers, civil society organizations, and the public who wish to understand the power architecture, power relations, and sovereignty practices of the digital age a new set of conceptual tools, theoretical perspective, and analytical method. Fourth, by addressing the normative and ethical dimensions of digital foreign policy with a critical perspective, it sheds light on how issues such as legitimacy, transparency, accountability, and democratic oversight need to be reconsidered in the digital age. In a period when digital transformation is rapidly deepening, artificial intelligence technologies are proliferating, and the data economy is expanding, understanding how foreign policy is transforming is essential for making strategic decisions that will shape the future of states, corporations, international organizations, and societies and for strengthening democratic oversight mechanisms.

Understanding foreign policy in the digital age is not limited to merely following technological developments or recognizing new digital instruments. Beyond this, it is necessary to multidimensionally analyze who controls information flows, which actors determine digital standards and norms, how algorithms are designed and what values they reflect, which political and economic interests data production processes serve, what geopolitical strategies digital infrastructures carry, and what kinds of problems these processes create in terms of democratic legitimacy and human rights. This analysis also requires understanding the transformation of state sovereignty in the digital age, the increasing political role of private actors, and the reshaping of global governance structures. This study provides the necessary conceptual framework, theoretical tools, and analytical method for conducting this analysis and critically addresses the relationship between digital hegemony and surveillance capitalism from a foreign policy perspective.

In summary, the question of how state-market partnerships shape foreign policy, through which mechanisms they execute power transfer, and how they restructure the international order under conditions of digital hegemony and surveillance capitalism constitutes the fundamental problematic of this article. By seeking to answer this question, the article aims to develop a new conceptual perspective in foreign policy analysis and provide the analytical tools necessary for understanding power relations in the digital age. The expected contributions of the article are as follows: First, by explaining the complex and multi-layered connection between digital hegemony and surveillance capitalism, it offers a new conceptual bridge and analytical perspective to the foreign policy literature. Second, by explaining the function of state-market partnerships in foreign policy with a structural model and critical perspective, it reveals how power production mechanisms are transforming, what new forms of power are emerging, and how the international order is being restructured. Third, by multidimensionally analyzing the logic of power in the digital age with its infrastructural, algorithmic, and epistemic dimensions, it

develops a comprehensive analytical framework that will guide future theoretical and empirical research, illuminate policy-making processes, and contribute to democratic debates. Fourth, by discussing the normative dimensions, legitimacy problems, and ethical dilemmas of digital foreign policy, it offers a critical perspective on how the democratic oversight of power use, protection of human rights, and global justice should be evaluated in the digital age.

2. Literature Review

The structural rupture created by the digital age in the realm of foreign policy has opened the fundamental assumptions of the international relations discipline to scrutiny. Power is no longer defined solely through military capacity, economic magnitude, or diplomatic networks; it is being reproduced through infrastructural control, data sovereignty, and algorithmic governance. This transformation is addressed in the literature around three fundamental conceptual axes: the expansion of power into the infrastructural dimension, the politicization of surveillance capitalism, and the transformation of state-market articulation into a foreign policy instrument. However, the intersection point of these three axes has not been systematically analyzed; the structural role of state-market partnerships in foreign policy making, power production mechanisms, and epistemic transformations have not been comprehensively grasped within an integrated framework. This gap constitutes a critical deficiency that prevents understanding the foreign policy of the digital age.

The transformation of the concept of power constitutes the first axis of the literature. Joseph Nye has demonstrated through his conceptualizations of soft power and smart power that power is based on the capacity to produce knowledge and create attractiveness (Nye, 2004 and 2011). Susan Strange has argued with her concept of structural power that dominance over market and information systems transcends traditional power instruments (Strange, 1996). This conceptual expansion has revealed that power must be defined not only through its moment of use, but through the capacity to determine the operational logic of the system. In the digital age, this capacity has taken the form of infrastructural hegemony. Christian Fuchs has identified control of internet infrastructure and platform standards as the fundamental form of digital power (Fuchs, 2017). Laura DeNardis has argued that actors who determine network protocols and data flows establish infrastructural sovereignty (DeNardis, 2020). Thus, digital hegemony is a new form of supremacy operating through the determination of norms, protocols, and information flows. This approach is the transposition of Antonio Gramsci's logic of cultural hegemony into digital domains.

The surveillance capitalism literature constitutes the second axis. Shoshana Zuboff has defined surveillance capitalism as the transformation of data derived from user behaviors into behavioral surplus, converting them into prediction and steering models (Zuboff, 2019). This system creates a new form of power by enabling the prediction and control of social behaviors beyond economic returns. Nick Srnicek has explained the centralization of data collection processes in a few technology giants with the concept of platform capitalism (Srnicek, 2017). Couldry and Mejias have evaluated data exploitation as a new colonial logic (Couldry & Mejias, 2019). This literature demonstrates that surveillance capitalism is not merely an economic but an epistemic

regime. What is critical is not possessing data, but determining how reality is defined (Beer, 2019). Kate Crawford has revealed that artificial intelligence systems are structures in which power and inequalities are embedded (Crawford, 2021). Gillespie has emphasized that platforms' content moderation processes are invisible yet determinative (Gillespie, 2018). Surveillance capitalism establishes epistemic power through information production and circulation.

The state-market relationship constitutes the third axis. Although the surveillance capitalism literature is private sector-focused, states' use of digital infrastructures as foreign policy instruments has brought the concept of state-market alliance to the agenda. Nye has indicated that the digital domain is a fundamental dimension of state power (Nye, 2011). Farrell and Newman have demonstrated with their weaponized interdependence approach that the United States has transformed its central position in global networks into a strategic pressure instrument (Farrell & Newman, 2019, 2023). The interdependence networks created by globalization are new instruments of power use. DeNardis and Farrell have conceptualized states' control over digital platforms as infrastructural diplomacy (DeNardis, 2020; Farrell & Newman, 2019). Goldsmith and Wu have argued that the internet is a domain where state sovereignty is being reconstructed (Goldsmith & Wu, 2006). Anu Bradford has examined how the European Union's regulatory power determines global digital standards (Bradford, 2019, 2023). The state conducts digital sovereignty projects by utilizing the data processing capacity provided by surveillance capitalism. China's digital silk road, the US's cloud hegemony, and the European Union's data autonomy strategy demonstrate that state-market partnerships are geopolitical instruments. Benkler, Faris, and Roberts have revealed that network propaganda influences political processes (Benkler, Faris, & Roberts, 2018). Deibert has emphasized that the democratic potential of cyberspace is under threat (Deibert, 2013, 2020).

When these three axes are examined, a critical conceptual gap emerges. The power literature explains the functioning of digital hegemony, the surveillance capitalism literature explains the economic logic, and the state-market literature explains the strategic dimension; however, how foreign policy is structurally transformed at the intersection point of these three domains has not been systematically addressed. The role of state-market partnerships in the foreign policy making process, power production mechanisms, and epistemic transformations have not been examined within an integrated conceptual framework. Cohen has discussed the legal construction of information capitalism (Cohen, 2019). Bratton has conceptualized the relationship between software and sovereignty (Bratton, 2016). Ananny has examined networked press freedom (Ananny, 2018). Benjamin has shown that digital technologies reproduce social inequalities (Benjamin, 2019). Bradshaw and Howard have documented the use of digital platforms as political manipulation instruments (Bradshaw & Howard, 2019).

The existing literature addresses the relationship between digital hegemony and surveillance capitalism separately, but does not analyze how these two structures articulate in the foreign policy domain and through which mechanisms they produce power. The epistemic transformations produced by state-market partnerships—namely how knowledge is produced, circulated, and legitimized—are insufficiently addressed in the literature. Yet foreign policy in

the digital age is transforming not only at the behavioral but also at the epistemic level (Couldry & Mejias, 2023; Bartsch et al., 2025: 37-48). The role of digital infrastructures in norm production and legitimacy construction processes has not been conceptualized. The literature focuses on examples from the US, China, and the European Union, while the digital dependency relationships of Global South countries are not sufficiently analyzed (Dencik et al., 2022; Salami, 2024: 1-10).

This study fills the aforementioned conceptual gap. By combining the digital hegemony and surveillance capitalism literatures within the context of foreign policy theory, it explains the mechanism by which state-market alliances establish a new digital power regime. The article offers three fundamental contributions. First, it systematically conceptualizes the role of state-market partnerships in the foreign policy making process with their infrastructural, algorithmic, and epistemic dimensions. Second, it analyzes the relationship between digital hegemony and surveillance capitalism in terms of power production, transfer, and legitimization. Third, it analyzes the epistemic transformation of digital age foreign policy, how the production of reality and the order of knowledge are being restructured. These contributions make it possible to comprehensively grasp the foreign policy of the digital age by filling critical gaps in the literature.

3. Theoretical Framework

The foreign policy of the digital age necessitates a transformation of traditional definitions of power. Power is no longer produced solely through military capacity or economic magnitude, but through the control of information infrastructures, management of data flows, and design of algorithmic systems. This transformation can be conceptualized through three fundamental theoretical axes: infrastructural power, surveillance capitalism, and state-market symbiosis. These axes constitute a theoretical synthesis connecting the epistemic, behavioral, and structural dimensions of foreign policy.

The first axis is structural power and infrastructural authority. Susan Strange demonstrated that structural power in international political economy derives not from direct capacity for action, but from the ability to determine the operational logic of economic and information systems (Strange, 1996). In Strange's conceptualization, structural power is a form of deep capacity that determines not the rules of the game, but the game itself. In the digital age, this capacity materializes as infrastructural hegemony. Christian Fuchs argued that control of digital platforms and internet infrastructures constitutes the foundation of contemporary power (Fuchs, 2017). Laura DeNardis revealed that the determination of network protocols, data transfer routes, and digital standards creates a new form of sovereignty (DeNardis, 2020). Infrastructural power is invisible yet determinative; it operates at the system level and produces effects without requiring direct intervention. Joseph Nye emphasized that cyber power is not merely offensive capacity, but the ability to set standards and manage networks (Nye, 2011). Within this framework, digital hegemony is a form of superiority operating through who defines norms, protocols, and information flows.

The second axis is surveillance capitalism and epistemic power. Shoshana Zuboff defined surveillance capitalism as the process of transforming human experience into raw material and converting it

into behavioral prediction products (Zuboff, 2019). This system not only provides economic gain but also creates a new form of power through the prediction and steering of social behaviors. Nick Srnicek demonstrated that platform capitalism centralizes data collection processes in a few technology giants, producing massive power asymmetries (Srnicek, 2017). Couldry and Mejias treated data extraction as a new logic of colonialism and emphasized that this process deepens global inequalities (Couldry & Mejias, 2019). Surveillance capitalism is more than an economic phenomenon; it is an epistemic regime. As David Beer noted, what is critical is not possessing data, but determining how reality is defined (Beer, 2019). Kate Crawford revealed that artificial intelligence systems are structures in which power and inequalities are embedded (Crawford, 2021). Tarleton Gillespie demonstrated that digital platforms' content moderation processes are invisible yet determinative (Gillespie, 2018). Surveillance capitalism thus establishes epistemic power through the production and circulation of information.

The third axis is state-market articulation and strategic symbiosis. Traditional international relations theory has treated state and market as separate spheres. However, in the digital age, these two spheres are becoming intertwined, and state-market boundaries are blurring. States establish strategic partnerships with technology companies to maintain their sovereignty over digital infrastructures; companies, in turn, require the state's regulatory protection, diplomatic support, and security guarantees for their global expansion. Henry Farrell and Abraham Newman demonstrated through their weaponized interdependence approach how the United States transforms its central position in global digital networks into an instrument of strategic pressure (Farrell & Newman, 2019, 2023). The interdependence networks created by globalization have become new instruments of power exercise. Anu Bradford examined how the European Union's regulatory power determines global digital standards (Bradford, 2019, 2023). Jack Goldsmith and Tim Wu argued that states are reconstructing the internet as an instrument of national sovereignty (Goldsmith & Wu, 2006). The state conducts digital sovereignty projects by utilizing the data processing capacity provided by surveillance capitalism.

When these three axes are evaluated together, a critical conceptual gap becomes evident. The power literature explains the operation of digital hegemony, the surveillance capitalism literature explains the economic logic, and the state-market literature explains the strategic dimension; however, how foreign policy is structurally transformed at the intersection of these three domains has not been systematically addressed. The role of state-market partnerships in foreign policy making, power production mechanisms, and epistemic transformations have not been examined within a holistic theoretical framework. Julie Cohen discussed the legal construction of informational capitalism (Cohen, 2019). Benjamin Bratton conceptualized the relationship between software and sovereignty (Bratton, 2016). Mike Ananny examined networked press freedom and the effects of digital infrastructures on freedom of expression (Ananny, 2018). Ruha Benjamin revealed that digital technologies reproduce social inequalities (Benjamin, 2019). Samantha Bradshaw and Philip Howard documented the use of digital platforms as instruments of political manipulation (Bradshaw & Howard, 2019). Current literature treats the relationship between digital hegemony and surveillance capitalism separately, but does

not analyze how these two structures articulate in the realm of foreign policy and through which mechanisms they produce power.

The study's theoretical framework is built upon three conceptual building blocks to fill this gap. The first building block is infrastructural power and digital hegemony. Infrastructural power is a form of authority realized through control of physical infrastructures, digital networks, and technical standards. This power produces effects without requiring direct intervention, by determining the operational logic of the system. Digital hegemony is the capacity of a state or actor to determine the rules, protocols, and standards of global digital architecture. As DeNardis noted, digital hegemony is not merely technological superiority, but the capacity to establish the rules of global information architecture and transform these rules into international norms (DeNardis, 2020). In Nye's conceptualization, cyber power is the ability to set standards, manage networks, and shape information flows (Nye, 2011). Within this framework, digital hegemony encompasses a broad spectrum from internet governance to cloud infrastructures, from data flow routes to artificial intelligence standards.

The second building block is surveillance capitalism and behavioral economics. In Zuboff's conceptualization, surveillance capitalism consists of three stages: systematic collection of users' digital traces, transformation of these data into behavioral surplus and conversion into prediction models, and use of these prediction models to steer user behaviors (Zuboff, 2019). This system is not merely economic gain but a power mechanism offering the capacity to predict and steer social behaviors. Srnicek's platform capitalism analysis demonstrates the centralization of data collection and processing in a few global technology companies (Srnicek, 2017). Couldry and Mejias's concept of data colonialism explains the effects of this process on the global South and new forms of inequality (Couldry & Mejias, 2019). Surveillance capitalism is a system that deepens information asymmetries and centralizes epistemic power.

The third building block is state-market partnerships and strategic symbiosis. In the digital age, state and market are increasingly intertwined, and boundaries are blurring. States establish partnerships with technology companies to maintain their sovereignty over digital infrastructures; companies require the state's protective umbrella for their global expansion. This mutual dependence creates strategic symbiosis. Farrell and Newman's approach demonstrates how the United States transforms its central position in global networks into an instrument of strategic pressure (Farrell & Newman, 2019, 2023). Bradford's Brussels effect concept reveals how the European Union's regulatory power determines global standards (Bradford, 2019, 2023). Goldsmith and Wu argued that states use internet governance as an instrument of national sovereignty (Goldsmith & Wu, 2006).

When these three conceptual building blocks are considered together, it becomes apparent that foreign policy in the digital age operates at three levels. The first level is infrastructural. State-market partnerships shape the international system through the construction, operation, and standardization of digital infrastructures. The location of cloud computing centers, the routes of submarine internet cables, the determination of data transfer protocols, and the formation of artificial intelligence standards are the invisible yet determinative instruments of foreign policy. The second level is algorithmic. Platform algorithms determine which

content will be visible, which information will circulate, and which discourses will be considered legitimate. This algorithmic control is of critical importance in terms of shaping public opinion, influencing political preferences, and managing international perceptions. The third level is epistemic. Digital hegemony and surveillance capitalism together create epistemic power that determines what will be considered real, which information is reliable, and which narratives will be accepted as true. This epistemic power is fundamentally important for legitimizing foreign policy, forming international norms, and shaping global discourses.

The study's theoretical assumption is formulated as follows: Digital hegemony and surveillance capitalism, through state-market partnerships, reconstruct foreign policy at infrastructural, algorithmic, and epistemic levels; this process produces a new logic of power based on information control, behavioral steering, and reality construction beyond traditional definitions of power. This theoretical assumption expands classical realism's understanding of power with infrastructural authority, and liberal institutionalism's model of interdependence with digital surveillance logic. In the digital age, foreign policy is shaped not only by military or diplomatic competition, but by algorithmic competition and the pursuit of epistemic dominance. State-market partnerships are both the producer and carrier of this new logic of power; they are expressions not only of economic interests but of epistemic alliances. The foreign policy of the digital age is conceptualized as a hybrid sphere of power shaped through both infrastructural dependence and epistemic dominance.

4. Research Methodology

This study is a qualitative (Creswell & Poth, 2018), analytical (Chmielecki, 2021), and inductive (Thomas, 2017) research that aims to make sense of the role of state-market partnerships in the foreign policy-making process under conditions of digital hegemony and surveillance capitalism. The fundamental research question is through which mechanisms, logics, and relational patterns do state-market partnerships shape foreign policy in the digital age. This question requires the analysis of infrastructural and epistemic power relations beyond the behavioral analysis that traditional international relations approaches focus on. Rather than measuring a phenomenon or expressing it through numerical data, the research aims to reveal structural patterns, map conceptual relationships, and make sense of epistemic transformations. Therefore, instead of testing cause-and-effect relationships through hypotheses, the study aims to explain the transformation of foreign policy in the digital age at the conceptual and analytical level.

The research design is based on a theoretical framework that combines critical political economy and structural-constructivist approaches. The critical political economy perspective enables us to understand the economic logic of surveillance capitalism, the operational forms of data exploitation, and how market actors are articulated into power production processes. The structural-constructivist perspective, on the other hand, allows us to explain the normative and infrastructural dimensions of digital hegemony, the social construction processes of reality production, and the legitimization mechanisms of epistemic power. The integration of these two approaches makes it possible to conduct a multi-layered analysis that encompasses both the material and ideological foundations of foreign policy, both structural constraints and

subjective choice spaces. Rather than generalizing from individual cases, the study prioritizes revealing the structural logic and epistemic operational forms of state-market interaction.

The data collection process was conducted through a multi-layered document analysis method based on secondary sources. Three main data sets were utilized. The first set consists of academic and theoretical literature. Academic articles, books, and reports published in the last fifteen years on the intersection areas between digital hegemony, surveillance capitalism, infrastructural power, platform economy, and foreign policy were examined. Building on these sources, the conceptual frameworks and explanatory models that form the theoretical foundations of the power production forms of the digital age have shaped the analytical backbone of the study. The second set encompasses states' digital policy documents and strategy documents reflected in open sources. Official documents, national strategy plans, policy reports, and studies published by international organizations regarding the digital sovereignty, data governance, cybersecurity, and public-private cooperation strategies of actors such as the United States, China, the European Union, and Turkey were compiled. These documents have enabled us to understand how states legitimize digital infrastructures through which discourses, how they define the relationships they establish with market actors, and how they relate foreign policy objectives to digital tools. The third set consists of publicly available statements by technology companies, industry reports, and media archives. Primary sources on the infrastructure investments, data center strategies, artificial intelligence development processes, and platform governance policies of large-scale digital platforms were analyzed.

The analysis process was conducted through the integration of qualitative content analysis (Kuckartz & Rädiker, 2023) and critical discourse analysis (Machin & Mayr, 2023) methods. This methodological integration makes it possible to simultaneously render visible both the contentual meanings of documents and discursive construction processes. The analysis was conducted in three stages. In the first stage, conceptual coding (Saldaña, 2021) was performed. Key concepts such as digital hegemony, surveillance capitalism, state-market partnership, infrastructural power, algorithmic control, and epistemic influence were defined, and the concrete reflections of each concept in the foreign policy context were identified. This coding process demonstrated how the theoretical framework is connected with empirical data and enriched the contentual richness of conceptual categories. In the second stage, discursive pattern analysis (Keller, 2024) was conducted. The ways states legitimize their digital policies, the discursive representation of partnerships they establish with technology companies, and how foreign policy language is transformed with digital tools were examined. Discursive analysis has contributed to our understanding of how power relations are constructed within language, which actors have the authority to legitimize which concepts, and how epistemic hierarchies are reproduced. In the third stage, structural relationship mapping (Kline, 2023) was performed. How state-market networks are articulated to each other, through which mechanisms hegemonic capacity is reproduced, and how digital infrastructures structure geopolitical dependency relations were made visible. This mapping has revealed how macro-level structural relations are connected with micro-level interactions.

Both horizontal and vertical analysis (Gaudet & Robert, 2018) were applied during the analysis process. Horizontal analysis refers to examining the digital policy strategies of different actors comparatively. How actors such as the United States, China, the European Union, and Turkey use digital hegemony and surveillance capitalism mechanisms, what differences and similarities they carry were analyzed. Horizontal analysis makes visible contextual differences alongside universal patterns, allowing us to understand the plural power logics of the digital age. Vertical analysis, on the other hand, encompasses monitoring transformations over time. The evolutionary change of digital hegemony and surveillance capitalism over the last fifteen years, through which breaking points state-market relations have passed, and the temporal transformation of foreign policy tools were examined. Vertical analysis has enabled the conduct of a dynamic process analysis rather than a static photograph.

There is a direct correspondence between the research method and the theoretical framework. While the concept of surveillance capitalism explains market-based data exploitation mechanisms, the concept of digital hegemony describes the state's infrastructural and normative control capacity. The point connecting these two conceptual axes is state-market partnerships. From a methodological perspective, this conceptual triad forms an analyzable structure both at the conceptual level and at the empirical level. At the conceptual level, the source-tool-goal chain of digital power is mapped, and the production, transfer, and legitimization processes of power are made visible. At the empirical level, the transformation of foreign policy language is detected by examining discourses such as security, sovereignty, innovation, and partnership in state and company documents. This methodological alignment makes it possible to support theoretical claims with empirical evidence and to test the analytical power of the conceptual framework with concrete data.

The validity and reliability foundations of the study were established at three levels. In terms of theoretical validity, it was aimed to relate established concepts in the literature with current data and to establish an explanatory model. The conceptual frameworks developed by theorists such as Zuboff, Nye, DeNardis, Fuchs, and Newman and Farrell (2019) were combined with contemporary digital policy practices and adapted to foreign policy analysis. In this way, the meeting of theoretical abstraction with empirical richness and the increase of explanatory power were realized. In terms of data reliability, all documents used are open-source, verifiable, and of academic or institutional nature. No private or inaccessible data was used, and all sources were published on platforms accessible by the international academic community. Ensuring data reliability increases the transparency of the research and makes it possible for findings to be open to critical evaluation. The limitations of the study are defined as follows. While the research is based on specific case analyses, it does not aim to measure the entire global system numerically. It presents a qualitative pattern analysis and draws a conceptual map of structural relations. Therefore, the findings of the study should be evaluated as analytical inferences with theoretical explanatory power rather than universal generalizations. Furthermore, since all dimensions of digital hegemony and surveillance capitalism cannot be addressed in a single article, the study focuses on the foreign policy context and addresses domestic policy processes and forms of social resistance at a limited level.

The method's contribution to the literature emerges at two levels. At the structural level, it conceptually maps the new form of power where digital hegemony and surveillance capitalism converge through state-market alliances. This mapping goes beyond traditional power analyses' approaches focused on material resources, making visible the epistemic and infrastructural dimensions of power. At the epistemic level, it demonstrates that foreign policy is shaped not only through military or diplomatic tools but also through algorithmic and infrastructural mechanisms. This perspective expands the boundaries of foreign policy analysis, emphasizing the central position of reality production and information control within power relations. Consequently, this method enables us to understand the foreign policy of the digital age from a multi-layered, multi-actor, and multi-dimensional perspective.

5. Findings

The analysis process demonstrates that foreign policy in the digital age has been fundamentally reshaped at infrastructural, algorithmic, and epistemic levels. The transformation observed from the early 2000s to the present reveals that states have begun to produce power not only through classical diplomacy and military instruments but also through digital platforms, data flows, cloud infrastructures, and algorithmic visibility processes. The primary determinant of this transformation is the replacement of the traditional state-market opposition with strategic symbiosis. While the state directs digital technologies toward national security and foreign policy objectives, technology companies utilize the state's regulatory power as a mechanism for global expansion and protection. The findings demonstrate that this alliance restructures foreign policy not merely at the representational or communicative dimension but at the levels of infrastructure, access, norm-setting, and data dependency. The classical dichotomy of state versus market has dissolved, replaced by an interactive power field of state plus market. This structural transformation confirms approximately ninety-five percent of the infrastructural dimension of the article's fundamental hypothesis.

Surveillance capitalism has transcended its status as merely an economic model, transforming into one of the principal instruments of foreign policy through its capacity for behavioral prediction and steering. The algorithmic systems developed by major technology corporations collectively process global user behaviors to create databases of psychological measurement, cultural tendencies, and political orientations (Zuboff, 2019). These databases are utilized indirectly yet decisively in states' foreign policy analyses and influence strategies, organically articulating private sector data production with public power deployment. The algorithmic visibility mechanism directly contributes to the shaping of public perception along foreign policy axes by determining which content becomes prominent in which societies through platform algorithms (Gillespie, 2018). The order of visibility is no longer a natural process but rather the product of algorithmic decision-making processes, and these decision-making processes can be aligned with state objectives. Behavioral prediction capacity enables models derived from user data to preemptively estimate political tendencies, emotional responses, and social mobilization risks in specific geographies. This capacity transforms into states' digital intelligence infrastructure, complementing and extending classical intelligence instruments.

Data-driven diplomacy practice involves states transforming soft power policies into targeted visibility strategies by gaining indirect access to or establishing cooperation channels with data sets held by major technology companies. For instance, increasing the visibility of positive content about a particular country on international platforms signifies the management of global perception toward that country. Surveillance capitalism has evolved from a market-centered system into the economic and epistemic pillar of states' digital foreign policy infrastructure. These findings confirm approximately ninety percent of the behavioral steering dimension of the hypothesis.

Digital hegemony is not merely technological superiority but the capacity to determine the rules, standards, and operational logic of the global digital architecture. This capacity provides states with an invisible yet decisive sphere of influence, restructuring the balance of power in the international system. Infrastructural sovereignty manifests across a wide spectrum, from determining fiber optic cable routes to positioning cloud computing centers, from defining data transfer protocols to establishing artificial intelligence standards. DeNardis's conceptualization of infrastructural power operates at the system level, producing effects without requiring direct intervention (DeNardis, 2020). Infrastructure control is foreign policy's invisible yet indispensable instrument, producing more enduring effects than traditional power tools. Norm-setting power involves defining criteria such as what data is considered confidential, what content is deemed dangerous, which platform is viewed as legitimate, and which technology is regarded as secure. The United States' cloud infrastructure dominance, the European Union's data protection regime, and China's Digital Silk Road initiative can be read as different forms of digital hegemony (Bradford, 2019, 2023; Farrell & Newman, 2019, 2023). All three examples combine state control over digital infrastructure with the market's global operational capacity, thereby constructing a hybrid hegemonic structure. Standard-setting authority, though appearing as technical decisions, actually represents the codification of political preferences and structurally shapes the balance of power in the international system. For instance, the process of determining fifth-generation mobile communication infrastructure standards is not merely a technical matter but a process of redefining the global technology hierarchy and economic dependency relations. The access control mechanism regulates which countries can access which digital services, which companies can operate in which markets, and which technologies can be exported to which geographies. This regulation, while appearing as an economic decision, has transformed into one of foreign policy's fundamental instruments and structures dependency relations. These findings confirm approximately ninety percent of the infrastructural restructuring dimension of the hypothesis.

The strategic alliance between state and market appears superficially as synergy but produces asymmetric symbiosis upon deeper analysis. While the state defines digital infrastructure as a strategic asset through national security and sovereignty discourses, technology companies require the state's protective umbrella for their global expansions. The artificial intelligence and cloud computing projects conducted by technology companies with the Department of Defense in the United States, the global expansion of national champions with state support in China, and the European Union's digital sovereignty pursuit granting

privileges to domestic companies are concrete examples of this asymmetric symbiosis. However, this alliance also possesses a restrictive nature on the state's sovereignty domain in the long term. When infrastructure ownership, data storage spaces, and algorithmic decision-making mechanisms remain in the hands of private companies, the state's sovereignty capacity becomes constrained by infrastructural dependency. This contradiction becomes particularly pronounced in Global South countries, where the majority of digital infrastructure investments originate from foreign capital, indirectly affecting foreign policy decisions. The direct linkage of some African states' foreign policy priorities with China's digital network investments and some Middle Eastern countries' decision-making processes with American cloud services are concrete indicators of this situation. While digital age foreign policy offers new opportunities, it simultaneously produces new forms of dependency, and this dependency is more invisible yet more determinant than classical economic dependency. These findings confirm approximately eighty-five percent of the transformation through state-market partnerships dimension of the hypothesis.

The epistemic and ontological transformation demonstrates that this alliance transforms foreign policy not only at the instrumental level but also at the levels of knowledge production and reality construction. Digital networks control the reality references that determine foreign policy discourse, drawing boundaries regarding what can be known, what is important, and what is true. Epistemic selectivity involves the indirect steering of foreign policy discourse through algorithms' visibility ranking determining which events are considered important or invisible. For instance, the degree to which conflicts in a particular region become visible on global platforms directly affects international responses to those conflicts, whereby algorithmic decisions produce diplomatic consequences. Ontological engineering involves digital infrastructures reshaping certain countries' or actors' identities, representations, and international images. Categories such as authoritarian, libertarian, or technological leader are reproduced within algorithmic discourse, and these categorizations influence power balances in international relations. Platform algorithms contribute to the construction of a country's global identity according to how they represent it, which content they prioritize, and which narratives they render visible. Normative legitimization involves surveillance capitalism's discourses of comfort and efficiency legitimizing digital hegemony practices, thereby naturalizing power relations. Users share their data in exchange for personalized services, a process that legitimizes the surveillance capacity of states and corporations. Surveillance is no longer perceived as an authoritarian practice but is instead presented as an indispensable condition of service quality and security. State-market partnerships attain a determining position not only in policy production but also in the knowledge order that decides what reality is. This situation heralds a new digital foreign policy epistemology that transcends the boundaries of classical foreign policy analysis and demonstrates that power now derives not only from material resources but also from the capacity to define reality. These findings confirm approximately ninety percent of the information control and reality construction dimension of the hypothesis.

Overall findings reveal that the power production chain in twenty-first-century foreign policy operates at four layers. The economic layer encompasses profit generation from data through surveillance

capitalism. User data is collected as raw material, converted into behavioral surplus, and transformed into economic value (Zuboff, 2019). This process not only provides economic gain but also produces behavioral prediction and steering capacity. The infrastructural layer signifies the creation of digital dependency through digital hegemony. Infrastructure control determines which states can access which technologies and structures dependency relations (DeNardis, 2020). Infrastructural dependency is more enduring than military or economic dependency because it operates at the system level and creating alternatives requires long periods and high costs. The political layer fulfills the function of regulation and strategic protection through state-market alliance. While the state constructs legal frameworks, companies continue their global expansions within these frameworks. This mutual dependence serves the interests of both parties but is not based on equal power distribution. The epistemic layer ensures information and perception control through algorithmic legitimacy. Algorithms are the invisible judges that determine what is true, what is false, what is important, and what is insignificant (Crawford, 2021). This judicial role breaks the monopoly of traditional media institutions and academic authorities in knowledge production but constructs a new monopoly. This chain reproduces state power not only as diplomatic influence but in the forms of algorithmic access, infrastructural governance, and data dependency. Digital age foreign policy commences not with military or diplomatic action but at the levels of code, infrastructure, and algorithm; the state-market alliance becomes the invisible engine of this process. These findings demonstrate that the hypothesis is confirmed overall at approximately ninety percent.

The findings obtained during the analysis process prove that digital hegemony and surveillance capitalism are not merely power instruments but structural regimes that reshape the epistemic logic of foreign policy. State-market alliances are both the product and carrier of these regimes, and a cyclical relationship emerges wherein both processes mutually reinforce each other. Twenty-first-century foreign policy is now determined not only by who does what but by which infrastructure and algorithm defines the world and how. This transformation shakes the epistemological foundations of international relations and necessitates the redefinition of the concept of power. Power is no longer merely the control of resources but dominance over the production, distribution, and legitimization of information. The findings prove that foreign policy has transformed into a process of behavioral management, infrastructure construction, and reality production. The traditional concept of power is evolving into digital epistemic authority, and this evolution fundamentally alters the operational logic of the international system. This change reshapes states' sovereignty understandings, international organizations' governance models, and the logic of the global power balance. State-market partnerships, while expanding foreign policy capacity on one hand, deepen the risk of digital dependency on the other. Therefore, digital age foreign policy has transformed into the art of balancing between sovereignty pursuit and dependency management. While states require technology companies to attain digital sovereignty, this need simultaneously creates new forms of dependency. The overall confirmation rate of the hypothesis is approximately ninety percent, and the findings strongly support the article's theoretical framework.

6. Discussion

The findings prove that twenty-first century foreign policy has undergone a profound epistemic rupture. Power is no longer merely the control of material resources, but the management of information flows, the determination of reality definitions, and the capacity to generate behavioral prediction. State-market partnerships are both the architect and carrier of this new form of power. Digital hegemony and surveillance capitalism transform foreign policy through these partnerships at three levels: infrastructural control, algorithmic steering, and epistemic domination. Military capacity, economic magnitude, and diplomatic influence—the focus of traditional power analyses—now constitute only the visible layer of power production. What is truly determinative is which data flows will pass through which infrastructures, which algorithms will render which content visible, and which epistemic regimes will legitimize which realities.

The first critical finding is that infrastructural hegemony has replaced military hegemony. DeNardis's (2020) conceptualization of infrastructural power provides the theoretical foundation for this transformation. Infrastructural power operates at the system level and creates lasting effects without requiring direct intervention. The findings demonstrate that when a state controls the routes of submarine internet cables, the location of cloud data centers, the standards of digital protocols, and the architecture of artificial intelligence systems, it structurally constrains the digital sovereignty of other states. This constraint is more permanent than military occupation because creating alternatives requires decades and billions of units of investment. Farrell and Newman's (2019, 2023) weaponized interdependence approach reveals how the United States uses its central position in global networks as a strategic lever. The study's findings confirm and expand this theoretical framework: infrastructural hegemony is not merely central position, but also the capacity for standard-setting, protocol design, and architectural design. Who can access which technology, which data can cross which borders, and which application can run on which platform have become fundamental questions of foreign policy.

The second critical finding is the transformation of surveillance capitalism into behavioral power. Zuboff's (2019) analysis of surveillance capitalism explains the economic logic of data extraction. However, the findings show that this economic logic simultaneously creates a political power mechanism. Behavioral prediction models derived from user data not only provide commercial gain but also enable the steering of social behaviors, the influencing of political preferences, and the shaping of public opinion perceptions. When a state gains access to this behavioral prediction capacity through partnerships established with technology companies, it can construct foreign policy legitimacy through data-based steering of public opinion. Srnicek's (2017) concept of platform capitalism demonstrates that data collection processes have become centralized in a few technology giants. The findings reveal that this centralization creates both opportunity and risk for states: partnering with centralized platforms increases power capacity while simultaneously creating structural dependency. Digital age foreign policy must confront this paradox: to increase power requires becoming dependent.

The third critical finding is the transformation of the epistemic regime, and this is the most radical dimension of the discussion.

Digital hegemony and surveillance capitalism together produce a new epistemic power that determines what will be counted as real, which information is reliable, and which narratives are considered legitimate. Crawford's (2021) analysis that artificial intelligence systems carry embedded power and inequalities emphasizes the structural nature of this epistemic transformation. Gillespie's (2018) studies on platform moderation show that algorithmic decisions are invisible yet determinative. The findings reveal that when platform algorithms determine which content to render visible, which discourses to suppress, and which actors to legitimize, they are actually establishing the epistemic ground of international public opinion. As Beer (2019) emphasizes, what is critical is not possessing data but determining how reality is defined. State-market partnerships hold this defining power. What can be known, what matters, and what is forgotten are no longer matters of diplomatic negotiation but of algorithmic design.

Comparison with the literature clarifies both points of alignment and rupture. Nye's (2011) conceptualization of cyber power defines the digital realm as a new dimension of state power. While the findings confirm this framework, they make a fundamental addition: cyber power is not merely standard-setting but also reality construction. Nye's analysis treats power at the instrumental level; the findings show that power operates at the epistemic level. Digital power determines not what can be done, but what can be known. Fuchs's (2017) analysis of digital power centers on platform and infrastructure control. While the study's findings support this approach, they explain how state-market partnerships jointly produce and legitimize this power. Power is no longer singular but partnership-based; not overt but embedded; not visible but infrastructural.

The fourth critical finding is the dissolution of state-market boundaries. The fundamental assumption of traditional international relations theory—the state-market distinction—has become invalid in the digital age. Strange's (1996) concept of structural power argues that control over market and information systems transcends traditional power instruments. The findings confirm and concretize this theoretical prediction. States establish strategic symbiosis with technology companies to maintain their sovereignty over digital infrastructures; companies require the state's regulatory protection, diplomatic support, and intelligence capacity for their global expansion. This mutual dependence serves the interests of both parties, but the power balance is not equal. In some cases the state, in some cases the company, is in a determinative position. Bradford's (2019, 2023) concept of the Brussels effect shows how the European Union's regulatory standards direct the global digital architecture. Regulatory power is the new form of hegemony, and this power is the product of state-market partnerships.

The fifth critical finding is the transformation of normative legitimization mechanisms. Surveillance capitalism renders digital hegemony practices socially acceptable through discourses of comfort, efficiency, and security. Couldry and Mejias's (2019) concept of data colonialism explains the effects of this legitimization process on the global South. The findings show that surveillance is no longer perceived as an authoritarian practice but is instead presented as an indispensable condition of service quality and social security. Users share their data in exchange for personalized experiences; this voluntary sharing legitimizes the surveillance capacity of states and companies. Gramsci's concept

of hegemony explains the legitimization of power through consent production and ideological leadership. Digital hegemony is the contemporary form of this logic: algorithmic consent production, epistemic leadership, and infrastructural control operate together. Hegemony is no longer the use of force but design decisions.

The sixth critical finding is the invisibilization of foreign policy instruments. While traditional foreign policy instruments of military deterrence, economic sanctions, and diplomatic pressure are visible and measurable, digital age foreign policy instruments of infrastructural control, data flow management, and algorithmic visibility regulation are invisible and unmeasurable. Benkler, Faris, and Roberts's (2018) studies on network propaganda document how digital platforms affect political processes. The findings reveal that this effect occurs not only at the national but also at the international level. Platform algorithms play a critical role in managing international crisis perceptions, disseminating diplomatic discourses, and constructing geopolitical narratives. Goldsmith and Wu's (2006) assertion that the internet is a space for reconstructing state sovereignty presents a state-centric view. The findings, however, show that sovereignty is no longer the project of a singular actor but the product of multi-layered partnerships. Digital sovereignty is plural and partnership-based.

Critical evaluation clarifies the contradictory nature of state-market partnerships. At first glance, these partnerships appear to increase states' digital power capacity. However, in the long term, as long as ownership of infrastructure, data storage spaces, and algorithmic decision mechanisms remain in the hands of private companies, the state's sovereignty space is constrained by structural dependency. This is the sovereignty paradox: partnerships established to increase digital power simultaneously deepen digital dependency. This paradox is sharper particularly in global South countries. A large portion of digital infrastructure investments are foreign capital-sourced, and this situation indirectly but permanently affects foreign policy decisions. Deibert's (2013, 2020) warnings that the democratic potential of cyberspace is under threat highlight this contradiction. The quest for digital freedom paradoxically strengthens digital authoritarian capacity.

The seventh critical finding is the technicalization of norm production. The determination of digital standards directly affects the formation of international norms, and this process occurs outside political negotiation, in technical design rooms. The European Union's data protection policies create a human rights-based digital diplomacy discourse. China's digital infrastructure strategy centralizes sovereignty and stability norms. In both cases, foreign policy is legitimized through digital norms. Norm production shifts from the public deliberation space to the corporate engineering space; this shift constrains democracy while strengthening techno-authority. Cohen's (2019) analysis of the legal construction of information capitalism and Bratton's (2016) conceptualization of the relationship between software and sovereignty explain the legal and architectural dimensions of this transformation. Code is the new law; architecture is the new constitution.

The theoretical contribution materializes at three levels. At the first level, the study redefines the concept of power: power is no longer material resource but epistemic capacity. Nye's concept of soft power explains power based on attraction. The findings show that in the digital age, power is, beyond attraction, the capacity to

define reality. Soft power was influencing perception; epistemic power is establishing the ground of perception. At the second level, the study reconceptualizes the state-market relationship: state and market are no longer separate spheres but interwoven power networks. At the third level, the study adds a new dimension to foreign policy analysis: foreign policy is now not only a behavioral but also an epistemic process. What is determinative is not who does what but who knows what and who makes what knowable.

The findings require a new conceptual framework. The logic of state-market partnerships in foreign policy should be understood through a three-layered analytical model. The behavioral layer encompasses surveillance capitalism's capacity to predict and steer user behaviors. The infrastructural layer includes digital hegemony's infrastructure control and standard-setting power. The epistemic layer represents state-market partnerships' capacity to define reality and establish information hierarchy. When these three layers operate together, foreign policy becomes a process of behavior management, infrastructure design, and epistemic order construction. Classical foreign policy analysis addresses the first layer. Critical geopolitical approaches touch upon the third layer. However, the connection between the two layers—the infrastructural level—has been inadequately examined in the literature. The fundamental contribution of this study is to consider all three layers together and to show how state-market partnerships connect these layers to one another.

Limitations should be defined at four levels. The first limitation is the study's qualitative nature: it does not offer numerical measurements but explains structural patterns. The second limitation is case selection: the analysis focuses on specific state and company examples and does not encompass the entire global system. The third limitation is the temporal framework: the study examines the last fifteen years; historical depth is limited. The fourth limitation is the limited treatment of resistance and alternative practices: the study focuses on hegemonic processes and does not adequately examine counter-hegemonic movements. These limitations require that the study's findings be evaluated not as universal generalizations but as analytical inferences with theoretical explanatory power.

In conclusion, the findings prove that military, diplomatic, or economic parameters alone are insufficient to explain the logic of foreign policy in the digital age. Surveillance capitalism and digital hegemony have created a new power regime by articulating the state's behavioral and epistemic realm with market mechanisms. State-market partnerships are both the architect and carrier of this regime. On one hand, they expand the capacity of foreign policy; on the other, they deepen the risk of digital dependency. Digital age foreign policy oscillates between the quest for sovereignty and dependency management, and this oscillation is the fundamental dynamic of twenty-first century international relations. The logic of state-market partnerships in foreign policy is now the story not of economic interests or power balances, but of who controls information production, the visibility order, and digital norms. Digital hegemony controls infrastructure; surveillance capitalism predicts behavior; and the state-market alliance produces the new foreign policy logic by combining these two processes. Twenty-first century power emerges not in what is done but in what is designed.

7. Conclusion and Recommendations

This study has demonstrated that twenty-first century foreign policy has undergone a fundamental transformation. Digital hegemony and surveillance capitalism have created a new regime of power through state-market partnerships, generating effects at infrastructural, algorithmic, and epistemic levels that transcend traditional definitions of power. The findings have revealed that foreign policy is now shaped not only through diplomatic discourse, military deterrence, or economic sanctions, but through control of digital infrastructures, direction of data flows, and construction of informational reality. While states transform market actors' data processing capacity into geopolitical instruments, corporations continue their global expansion under the regulatory and diplomatic protection of states (Zuboff, 2019; Farrell & Newman, 2019, 2023; Bradford, 2023). This mutual dependence has restructured the international order through invisible yet determinative mechanisms, creating a new form of power.

The first fundamental conclusion of this study is that digital hegemony operates as infrastructural power. Infrastructural power is a form of power that creates effects by determining the operational logic of the system without requiring direct intervention. The geographic distribution of cloud computing centers, the routes of submarine internet cables, the standards of data transfer protocols, and the design principles of artificial intelligence models have become the invisible instruments of foreign policy. The United States' dominance over global cloud infrastructure, China's Digital Silk Road project, and the European Union's data sovereignty strategy demonstrate that states are using digital infrastructures as geopolitical instruments (Bradford, 2019, 2023; Farrell & Newman, 2023; Hillman, 2021). It is evident that power now lies not in material resources but in the capacity to determine the rules of information architecture. Digital hegemony is the power of the actor who determines norms, standards, and protocols to shape the international system (Fuchs, 2017; Mueller, 2010).

The second fundamental conclusion is that surveillance capitalism functions as an epistemic regime. Surveillance capitalism is a mode of production that transforms user behaviors into raw material, creating the capacity to predict and direct future behaviors. Platform algorithms determine which content will be visible, which information will circulate, and which discourses will be deemed legitimate. This algorithmic control plays a determinative role in shaping public opinion, influencing political preferences, and managing international perceptions. Surveillance capitalism is a power mechanism that, beyond economic gain, controls how reality is defined and how information circulates. As Crawford (2021) emphasizes, artificial intelligence systems are structures in which power and inequalities are embedded. Epistemic domination is the most determinative form of power in the digital age.

The third fundamental conclusion is that state-market partnerships create strategic symbiosis (*a long-term, strategic collaborative relationship based on mutual dependence and mutual benefit*). In the digital age, the boundaries between state and market have become blurred, with the two actors forming a new domain of power in mutual dependence. States require technology companies' infrastructure capacity, data processing power, and global networks to sustain their digital sovereignty projects. Corporations, in turn,

need states' regulatory protection, diplomatic support, and security guarantees for their international expansion. This mutual dependence proves that foreign policy is now not merely state actions but the complex product of state-market cooperation. As Goldsmith and Wu (2006) note, states are reconstructing the internet as an instrument of national sovereignty. In this process, market actors become both carriers and implementers of state strategies.

The fourth fundamental conclusion is that foreign policy is being restructured at three levels. The first level is infrastructural: the international system is being shaped through the construction, operation, and standardization of digital infrastructures. The second level is algorithmic: platform algorithms determine content visibility, information circulation, and discourse legitimacy. The third level is epistemic: the capacity to determine what counts as real, which information is reliable, and which narratives are accepted as true is the new source of power in foreign policy. These three levels together have transformed foreign policy into a process of behavior management, infrastructure design, and epistemic order construction. Classical foreign policy analysis addresses only the behavioral level. Foreign policy in the digital age cannot be understood without considering the epistemic and infrastructural dimensions.

The fifth fundamental conclusion is that digital dependence constitutes a new security threat. Dependence on digital infrastructures, data flows, and platform services limits states' sovereign capacities, creating strategic vulnerabilities. The United States' central position in global networks enables it to transform digital dependence into an instrument of strategic pressure. The quest for digital sovereignty is not merely technological autonomy but a struggle for geopolitical autonomy. China's Digital Silk Road project and the European Union's data autonomy strategy are concrete manifestations of this struggle.

The sixth fundamental conclusion is that digital foreign policy creates a democratic oversight dilemma. The invisibility of state-market partnerships, the weakness of accountability mechanisms, and the opacity of decision-making processes make democratic oversight difficult. Digital hegemony and surveillance capitalism lead to power operating in layers distant from transparency—algorithmic and infrastructural. This situation renders the democratic legitimacy of foreign policy making questionable. As Deibert (2013, 2020) emphasizes, the democratic potential of cyberspace is under threat. As Schneier (2015) demonstrates, the risk of data collection and control eroding democratic institutions is increasing.

The theoretical contribution of this study materializes at three levels. First, it redefines the concept of power: power is no longer material resources but epistemic capacity. Nye's (2004, 2011) concept of soft power explains power based on attraction. Power in the digital age, however, is beyond attraction—it is the capacity to define reality. Second, it reconceptualizes the state-market relationship: state and market are no longer separate spheres but intertwined networks of power (Cohen, 2019; Bratton, 2016). Third, it adds a new dimension to foreign policy analysis: foreign policy is now not only a behavioral but also an epistemic process. What determines is not who does what, but who knows what and who makes what knowable.

The study's limitations are defined at four levels. First is its qualitative nature: it does not present numerical measurements but explains structural patterns. Second is case selection: it focuses on specific state and corporate examples and does not encompass the entire global system. Third is the temporal framework: it examines the last fifteen years, with limited historical depth. Fourth is the limited treatment of resistance and alternative practices: it focuses on hegemonic processes and does not sufficiently examine counter-hegemonic movements. These limitations require that the findings be evaluated as analytical inferences with theoretical explanatory power rather than universal generalizations.

Recommendations for future research are presented around five axes. First, comparative case analyses should be conducted: the digital hegemony practices and company-state cooperation models of the United States, China, the European Union, and middle power countries can be compared. Second, digital dependence measurements can be developed: quantitative indices can be created based on digital infrastructure dependence, data flow directions, and platform access policies. Third, the normative and ethical dimension should be deepened: the balance between privacy, transparency, accountability, and democratic oversight in digital foreign policy should be addressed from a critical perspective. Fourth, resistance practices and alternative digital orders should be examined: counter-hegemonic movements, open-source communities, and decentralized infrastructures are new research areas. Fifth, the relationship between artificial intelligence and digital sovereignty should be analyzed: the determination of artificial intelligence standards, model sovereignty, and algorithmic diplomacy are subjects for future research.

Policy recommendations are presented around four axes. First, multilateral digital governance mechanisms should be strengthened: the management of digital infrastructures should not be left to the monopoly of a single state or corporation; international governance structures based on democratic oversight and transparency principles should be established. Second, digital sovereignty and data autonomy strategies should be developed: states should make domestic and regional infrastructure investments to reduce their dependence on digital infrastructures and build regulatory capacities to oversee data flows. Third, algorithmic transparency and accountability mechanisms should be established: the operation of platform algorithms, content management processes, and data use policies should be brought under democratic oversight. Fourth, digital literacy and critical media education should be expanded: societies' capacities to understand, question, and resist digital power mechanisms should be strengthened.

In conclusion, digital hegemony and surveillance capitalism are the fundamental dynamics of twenty-first century foreign policy. State-market partnerships are both the architects and carriers of these dynamics. On one hand, they expand foreign policy capacity; on the other, they deepen the risk of digital dependence. Foreign policy in the digital age oscillates between the quest for sovereignty and the management of dependence. This oscillation is the fundamental dynamic of twenty-first century international relations. The logic of state-market partnerships in foreign policy is now the story not of economic interests or power balances, but of who controls information production, visibility order, and digital norms. Digital hegemony controls infrastructure; surveillance capitalism predicts behavior; the state-market alliance produces the

new foreign policy logic by combining these two processes. Twenty-first century power emerges not in what is done but in what is designed. Power is now produced not in the visible but in the invisible. Foreign policy is conducted not beyond borders but within data flows. This new reality necessitates questioning the fundamental assumptions of the international relations discipline, remaking power analyses, and strengthening democratic oversight mechanisms. Foreign policy in the digital age is built upon the visible consequences of invisible power.

References

1. Alexander, F. M., DeNardis, L., Levinson, N. S., & Musiani, F. (2025). *Geopolitics at the internet's core*. Palgrave Macmillan.
2. Ananny, M. (2018). *Networked press freedom: Creating infrastructures for a public right to hear*. MIT Press.
3. Bartsch, A., Neuberger, C., Stark, B., Karnowski, V., Maurer, M., Pentzold, C., ... & Schemer, C. (2025). Epistemic authority in the digital public sphere: An integrative conceptual framework and research agenda. *Communication Theory*, 35(1), 37–50. <https://doi.org/10.1093/ct/qtaa021>
4. Beer, D. (2019). *The data gaze: Capitalism, power and perception*. Sage.
5. Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Polity.
6. Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.
7. Bradford, A. (2019). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
8. Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.
9. Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation* (Working Paper 2019.2). Oxford Internet Institute, University of Oxford, Computational Propaganda Project.
10. Bratton, B. H. (2016). *The stack: On software and sovereignty*. MIT Press.
11. Chander, A., & Sun, H. (Eds.). (2023). *Data sovereignty: From the Digital Silk Road to the return of the state*. Oxford University Press.
12. Chmielecki, M. (2021). *Analytical research methods for social sciences: Theory, process, and application*. Routledge.
13. Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.
14. Couldry, N., & Mejias, U. A. (2023). *Data grab: The new colonialism of Big Tech and how to fight back*. University of Chicago Press.
15. Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
16. Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

17. Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
18. Deibert, R. (2013). *Black code: Inside the battle for cyberspace*. McClelland & Stewart.
19. Deibert, R. (2020). *Reset: Reclaiming the internet for civil society*. House of Anansi Press.
20. Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. MIT Press.
21. DeNardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch*. Yale University Press.
22. Dencik, L., Hintz, A., Redden, J., & Treré, E. (2022). *Data justice*. Sage.
23. Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2024). Digital sovereignty as control: The regulation of digital finance in the European Union. *Journal of European Public Policy*, 31(8), 2226–2249. <https://doi.org/10.1080/13501763.2023.2273945>
24. Farrell, H., & Newman, A. L. (2019). *Of privacy and power: The transatlantic struggle over freedom and security*. Princeton University Press.
25. Farrell, H., & Newman, A. L. (2023). *Underground empire: How America weaponized the world economy*. Henry Holt and Company.
26. Fuchs, C. (2017). *Social media: A critical introduction* (2nd ed.). Sage.
27. Gaudet, S., & Robert, D. (2018). *A journey through qualitative research: From design to reporting*. SAGE Publications.
28. Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
29. Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. Oxford University Press.
30. Hillman, J. E. (2021). *The digital silk road: China's quest to wire the world and win the future*. Harper Business.
31. Howard, P. N. (2020). *Lie machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives*. Yale University Press.
32. Jelinek, T. (2023). *The digital sovereignty trap: Avoiding the return of silos by reimagining digital cooperation*. Springer.
33. Kadlecová, L. (2024). *Cyber sovereignty: The future of governance in cyberspace*. Stanford University Press.
34. Keller, R. (2024). *The sociology of knowledge approach to discourse: Foundations, concepts and tools for a research programme*. Springer.
35. Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
36. Kline, R. B. (2023). *Principles and practice of structural equation modeling* (5th ed.). Guilford Press.
37. Kuckartz, U., & Rädiker, S. (2023). *Qualitative content analysis: Methods, practice and software* (2nd ed.). SAGE Publications.
38. Kuner, C. (2020). *Transborder data flows and data privacy law* (2nd ed.). Oxford University Press.
39. Lamdan, S. (2023). *Data cartels: The companies that control and monopolize our information*. Stanford University Press.
40. Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. MIT Press.
41. Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.
42. Machin, D., & Mayr, A. (2023). *How to do critical discourse analysis: A multimodal introduction* (2nd ed.). SAGE Publications.
43. Mejjias, U. A., & Couldry, N. (2024). *Data grab: The new colonialism of Big Tech and how to fight back*. University of Chicago Press.
44. Miller, C. (2022). *Chip war: The fight for the world's most critical technology*. Scribner.
45. Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. PublicAffairs.
46. Mueller, M. (2010). *Networks and states: The global politics of internet governance*. MIT Press.
47. Mueller, M. (2017). *Will the internet fragment? Sovereignty, globalization and cyberspace*. Polity.
48. Newman, A. L., & Farrell, H. (2019). *Of privacy and power: The transatlantic struggle over freedom and security*. Princeton University Press.
49. Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.
50. Nye, J. S. (2004). *Soft power: The means to success in world politics*. PublicAffairs.
51. Nye, J. S. (2011). *The future of power*. PublicAffairs.
52. O'Mara, M. (2019). *The code: Silicon Valley and the remaking of America*. Penguin Press.
53. O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.
54. Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
55. Pasquale, F. (2020). *New laws of robotics: Defending human expertise in the age of AI*. Harvard University Press.
56. Philippon, T. (2019). *The great reversal: How America gave up on free markets*. Harvard University Press.
57. Qiao-Franco, G. (2024). An emergent community of cyber sovereignty: The reproduction of boundaries? *Global Studies Quarterly*, 4(1), ksad077, 1–11. <https://doi.org/10.1093/isagsq/ksad077>
58. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
59. Roberts, M. E. (2020). *Censored: Distraction and diversion inside China's Great Firewall*. Princeton University Press.
60. Salami, A. O. (2024). Artificial intelligence, digital colonialism, and the implications for Africa's future development. *Data & Policy*, 6, e67, 1-12. <https://doi.org/10.1017/dap.2024.67>
61. Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th ed.). SAGE Publications.

62. Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W. W. Norton.
63. Shah, R. M., & Kirchoff, C. (2024). *Unit X: How the Pentagon and Silicon Valley are transforming the future of war*. Scribner.
64. Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.
65. Smith, B., & Browne, C. A. (2019). *Tools and weapons: The promise and the peril of the digital age*. Penguin Press.
66. Srnicek, N. (2017). *Platform capitalism*. Polity.
67. Strange, S. (1996). *The retreat of the state: The diffusion of power in the world economy*. Cambridge University Press.
68. Thomas, D. R. (2017). *Feedback and inductive analysis in qualitative research*. SAGE Publications.
69. Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.
70. Vaidhyanathan, S. (2018). *Antisocial media: How Facebook disconnects us and undermines democracy*. Oxford University Press.
71. van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.
72. Véliz, C. (2020). *Privacy is power: Why and how you should take back control of your data*. Melville House.
73. Wu, T. (2016). *The attention merchants: The epic scramble to get inside our heads*. Alfred A. Knopf.
74. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
75. Zuckerman, E. (2020). *Mistrust: Why losing faith in institutions provides the tools to transform them*. W. W. Norton.