ASSAM
INTERNATIONAL REFEREED JOURNAL
ASSAM ULUSLARARASI HAKEMLİ DERGİ
e-ISSN: 2148-5879

https://dergipark.org.tr/en/pub/assam
Issue/ Special Issue (2025)

ARAŞTIRMA MAKALESİ | RESEARCH ARTICLE

Siber Güvenlik Söylemleri ve Toplumsal Güç İlişkileri: Dijital Güvenliğin Politik ve Stratejik Boyutları

Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security

Rashad MAMMADOV[1]

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.* Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

[1]Master Degree Istanbul Kultur University, Turkiye
E-Posta: rewad2000.rm@gmail.com
https://orcid.org/0009-0001-1213-938X

Özet

Dijital çağda siber güvenlik, yalnızca bilgi sistemlerini koruma pratiği olmaktan çıkarak, siyasal otorite, yönetişim ve toplumsal düzenin temel belirleyicilerinden biri haline gelmiştir. Başlangıçta teknik bir gereklilik olarak ele alınan bilgi güvenliği, günümüzde davranışların düzenlenmesi, dijital yurttaşların gözetimi ve ulusal–küresel bilgi akışlarının kontrolüyle doğrudan ilişkilidir. Bu çalışma, siber güvenlik söylemlerinin nasıl inşa edildiğini, dolaşıma sokulduğunu ve güç ilişkilerini meşrulaştırmak amacıyla nasıl kullanıldığını eleştirel bir perspektifle incelemektedir. Eleştirel güvenlik çalışmaları literatürü ve Foucault'nun iktidar–söylem kuramı çerçevesinde, "siber tehdit" kavramının nasıl bir varoluşsal tehlike olarak çerçevelendiği ve bu yolla devletlerin olağanüstü güvenlik önlemlerini nasıl meşrulaştırdığı analiz edilmiştir. Devlet strateji belgeleri, ulusal siber güvenlik politikaları ve medya söylemleri üzerinde gerçekleştirilen nitel söylem analizi, siber güvenlik söylemlerinin çoğu zaman "güvenliklendirme" işlevi gördüğünü ortaya koymaktadır. Bu süreçte teknik riskler, toplumsal korkulara dönüştürülerek, dijital alanlarda artan gözetim, denetim ve düzenleyici müdahaleler rasyonelleştirilmektedir. Böylece siber güvenlik, yalnızca koruma sağlayan bir araç değil, aynı zamanda kimlerin tehdit, kimlerin korunmaya değer olduğu üzerine toplumsal kararları şekillendiren bir iktidar diline dönüşmektedir. Elde edilen bulgular, siber güvenliğin dijital altyapıları koruma amacının ötesine geçerek, çağdaş toplumlarda yeni kontrol biçimlerini ve asimetrik güç yapılarını yeniden ürettiğini göstermektedir. Güvenlik, bilgi ve yönetişim arasındaki bu ilişki, dijital çağın yeni bir "teknopolitik düzen" inşasının temel dinamiğini oluşturmaktadır.

Anahtar Kelimeler: *Siber güvenlik, Güç ilişkileri, Söylem analizi, Dijital egemenlik, Gözetim, Eleştirel güvenlik çalışmaları*

Abstract

In the digital age, cybersecurity has evolved from merely a practice of protecting information systems into one of the fundamental determinants of political authority, governance, and social order. Initially approached as a technical necessity, information security today is directly linked to the regulation of behaviors, the surveillance of digital citizens, and the control of national and security studies and Foucault's theory of power–discourse, it analyzes how the concept of "cyber threat" is framed as an existential danger and how this framing legitimizes extraordinary security measures by states.A qualitative discourse analysis of state strategy documents, national cybersecurity policies, and media narratives reveals that cybersecurity discourses often serve a "securitizing" function. In this process, technical risks are transformed into social fears, thereby rationalizing increased surveillance, control, and regulatory interventions in digital domains. Thus, cybersecurity becomes not merely a tool of protection but also a language of power that shapes social decisions about who constitutes a threat and who is deemed worthy of protection.The findings indicate that cybersecurity goes beyond the goal of safeguarding digital infrastructures, reproducing new forms of control and asymmetric power structures in contemporary societies. The relationship between security, information, and governance constitutes the fundamental dynamic of constructing a new "technopolitical order" in the digital ageglobal information flows. This study critically examines how cybersecurity discourses are constructed, circulated, and employed to legitimize power relations. Within the framework of critical.

Keywords: *Cybersecurity, Power Relations, Discourse Analysis, Digital Sovereignty, Surveillance, Critical Security Studies*

Article Type	**Application Date**	**Admission Date**
Research Article	November 06 2025	December 12 2025

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.* Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

1. INTRODUCTION

In the information age, the concept of security has gone beyond the prevention of merely military or physical threats; it now encompasses the protection of data produced, stored, and transmitted in digital environments. This transformation has made information security a fundamental security paradigm of modern societies (Castells, 2010). As digitalization has rendered economic and political processes increasingly dependent on information, it has transformed information security into both a technical and a political issue. Today, even the smallest cyberattack targeting areas such as national security, energy infrastructure, or public administration is regarded as a factor threatening the sovereignty capacity of states (Nye, 2017).

Although the concept of information security primarily aims to protect the confidentiality, integrity, and availability of information produced in digital environments, its use carries not only a technical but also an ideological and discursive dimension (Solms & Niekerk, 2013). Through discourses such as "cyber threat" or "national interest," states and institutions transform security into a means of legitimization, thereby reinforcing both social order and control over the digital sphere. Foucault's (1977) approach to the relationship between power and discourse provides an explanatory framework for understanding that information security discourses are not solely aimed at ensuring security but also at producing and reconstructing power relations.

Today, information security has evolved from a technical line of defense into a strategic field at the center of national policies. Cyberattacks, data manipulation, disinformation campaigns, and threats to critical infrastructures have created a new arena of competition in international relations (Carr, 2016). In this context, information security discourses redefine the concept of state sovereignty in the digital age, bringing forth the notion of "digital sovereignty" that extends beyond national borders (DeNardis, 2020). This sovereignty is measured not only by the capacity for technical control but also by the ability to regulate information flows and determine normative power over digital infrastructures.

Another significant aspect of information security discourses is their influence on social perceptions of security. The way cyber threats are presented in media and political discourse shapes society's sense of security needs and fears (Hansen & Nissenbaum, 2009). Particularly, the discursive emphasis on incidents such as "data breaches," "personal information leaks," or "national cyberattacks" strengthens the social legitimacy of security policies and facilitates the public's acceptance of digital surveillance (Lyon, 2018). This situation turns information security into not merely a technological necessity but also a tool for generating social consent.

This research aims to analyze how information security discourses are constructed, by which actors they are produced, and how these discourses are related to mechanisms of political legitimacy, power, and control. The main assumption of the study is that the concept of information security is not merely a "technical necessity" but rather a discursive field through which power is reproduced in the digital age. Therefore, the study approaches information security discourses not only from a protection-oriented perspective but also through the lenses of power, surveillance, and sovereignty.

Drawing on critical security theories (Buzan, Wæver & de Wilde, 1998) and Foucault's (1977, 1980) discourse-based approach to power, the research analyzes the political functions of information security discourses. In this context, national cybersecurity strategies, state policies, and media narratives will be examined to discuss how "information security" is defined, through which threats it is legitimized, and what kinds of security perceptions it generates at the societal level.

2. CYBERSECURITY TECHNOLOGIES, INFRASTRUCTURAL POWER, AND THE DIGITAL DEFENSE ECONOMY

Cybersecurity in the contemporary world is not merely a security policy but also a field of power production grounded in technology. The protection of digital infrastructures, prevention of cyber threats, and maintenance of data integrity have become directly dependent on the technical capacities of states and the private sector. Therefore, information security today is not only an issue of "computer

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.*
Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

engineering" but also a matter of national defense and economic sovereignty (Carr, 2016). While cybersecurity technologies aim to enhance the resilience of digital systems, they also redefine global power distribution and economic dependency relations.

The technical dimension of cybersecurity is generally addressed along three main axes: network security, data protection, and critical infrastructure security. Network security relies on technologies such as encryption, firewalls, intrusion detection/prevention systems (IDS/IPS), and secure protocol architectures to ensure the integrity of communication between systems. Although these systems appear to provide technical solutions, decisions about which threats are deemed "priority" or which user activities are considered "suspicious" are entirely political (Deibert, 2013). For example, large-scale traffic monitoring systems implemented by states (such as Deep Packet Inspection) not only block malicious software but also become tools that categorize user behaviors and deepen surveillance infrastructures.

Data protection technologies are similarly as ideological as they are technical. Encryption systems are viewed both as tools that protect individual privacy and as potential security threats from the perspective of states. The 2016 Apple–FBI case is one of the most concrete examples of this duality. The FBI, citing counterterrorism concerns, demanded that Apple create a "backdoor" to bypass iPhone's security protocols; Apple refused, arguing the need to protect user security. This example clearly demonstrates that technical infrastructures are simultaneously arenas of political decision-making (DeNardis, 2020). Information security technologies, by determining who can access which information, contribute to the reproduction of power relations.

Critical infrastructure security is one of the most strategic dimensions of information security. Sectors such as power grids, energy distribution systems, healthcare networks, and financial systems have become fully dependent on digital networks. A cyberattack on any of these systems can turn not only into a technical malfunction but into a national security crisis. The Stuxnet virus, discovered in 2010, went down in history as the first industrial sabotage software targeting Iran's nuclear program. This incident demonstrated that the technical dimension of cybersecurity could directly transform into a form of geopolitical power projection (Rid, 2020). Stuxnet proved that information security infrastructures could be used not only for defense but also as offensive tools.

At this point, the political aspect of technical infrastructures can be understood through the concept of "infrastructural power." Developed by Mann (1984), this concept refers to the state's capacity to organize and control society through technical systems. In the digital age, this power is being reproduced through cybersecurity networks, data centers, cloud infrastructures, and AI-driven monitoring systems. Infrastructure is not merely technological but also a governmental instrument of power. Examples such as China's "Great Firewall" or the U.S. "PRISM" surveillance program clearly illustrate how technical systems can be transformed into political control mechanisms. These systems, while normalizing social surveillance through technical legitimacy, simultaneously reinforce digital sovereignty.

Another critical dimension of cybersecurity technologies involves AI- and machine learning–based security systems. In recent years, the use of AI systems in areas such as anomaly detection, behavioral analysis, and threat intelligence has grown rapidly. These systems attempt to predict potential threats by classifying billions of user behaviors through big data analytics. However, their opaque decision-making mechanisms bring with them risks of "algorithmic surveillance" and "digital bias" (Zuboff, 2019). Artificial intelligence is used not only to enhance security but also to monitor user behavior, collect data for economic interests, and enable social manipulation. This situation significantly weakens the democratic accountability of technical security systems.

From an economic perspective, the cybersecurity industry has become an expanding digital defense economy. By the mid-2020s, the global cybersecurity market exceeded an annual value of 250 billion dollars, and it now constitutes a strategic component of state budgets (Floridi, 2022). Cybersecurity technologies lie at the heart of not only national security strategies but also private sector

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.*
Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

investments. Defense contractors, technology giants, and private software developers directly benefit economically from the discursive reproduction of security threats. Therefore, the technical aspect of the "cyber threat" discourse is also a component of economic and political interests. In line with Beck's (1992) "risk society" approach, the definition and management of security risks have become an "economic sector" in themselves.

The proliferation of cybersecurity technologies has also brought about the problem of digital dependency. Many countries are dependent on the products of a small number of global corporations for security software, hardware infrastructure, or cloud services. This dependence weakens national digital sovereignty while reinforcing technological hierarchies on a global scale. DeNardis (2020) defines this situation as "infrastructural geopolitics," since the control of technical standards, data flows, and software protocols constitutes a new form of power. Thus, information security technologies not only ensure the protection of systems but also enable the reconfiguration of global power relations through digital codes.

The human and ethical consequences of technical security systems must not be overlooked. Systems developed to enhance security often restrict user freedom. In particular, biometric authentication systems, facial recognition algorithms, and location-based tracking technologies constrain individual autonomy in the name of "security" (Lyon, 2018). These technologies invisibly structure public space, determining who is classified as "trustworthy" and who is seen as a "potential threat." This process reveals that security technologies are not only technical but also ethical domains of debate. As Han (2017) notes, individuals in the digital age voluntarily surrender their privacy in exchange for the convenience of security. This is the fundamental paradox of the modern surveillance society.

3. THE DISCURSIVE CONSTRUCTION OF INFORMATION SECURITY, DIGITAL SOVEREIGNTY, AND CONTEMPORARY POWER STRATEGIES

In the digital age, information security has evolved far beyond a technical concern and has become a central mechanism through which states exercise sovereignty, construct national identity, and regulate social behavior. Cybersecurity technologies now constitute essential instruments for expanding state authority, maintaining economic competitiveness, and deepening systems of surveillance and control (Carr, 2016). As digital infrastructures increasingly underpin political, economic, and social life, the discourse of information security has emerged as a powerful framework that legitimizes new forms of governance, risk management, and geopolitical strategy.

Although information security is often conceptualized as a neutral technical practice, its technical infrastructures—network security, data protection, and critical infrastructure defense—are deeply embedded within political and ideological choices. Network security technologies such as firewalls, encryption protocols, and intrusion detection systems are presented as objective protective mechanisms. Yet decisions regarding which data is considered valuable, which behaviors are labeled suspicious, and which traffic should be monitored reflect political calculations as much as technical assessments (Deibert, 2013). Actions framed as cyber threats in one political context may fall under freedom of expression in another, demonstrating how cybersecurity constructs its own normative boundaries.

This political dimension becomes even more visible in debates on data security. Encryption technologies, designed to guarantee confidentiality and privacy, often come into conflict with national security objectives. The well-known Apple–FBI dispute revealed how technical infrastructures become arenas of power struggles, raising fundamental questions about who holds legitimate authority over data access—states or private corporations (DeNardis, 2020). Consequently, cybersecurity functions not merely as a shield against threats but as a mechanism through which data sovereignty and informational power are contested.

The stakes rise further in the realm of critical infrastructure security. Power grids, transportation systems, financial networks, and energy infrastructures are now fully digitized, making them vulnerable

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.*
Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

to cyberattacks that can trigger national-level crises. The Stuxnet incident, which caused physical damage to Iran's nuclear facilities in 2010, stands as a defining example of the geopolitical implications of cybersecurity technologies (Rid, 2020). This convergence of digital and physical domains has transformed cyberspace into the "fifth domain of warfare," where states pursue both defensive and offensive strategies.

In this context, Mann's (1984) concept of infrastructural power provides an important framework for understanding how cybersecurity expands state authority. Digital infrastructures such as cloud systems, data centers, 5G networks, and AI-driven monitoring architectures enhance the state's capacity to organize and regulate society. Surveillance programs such as China's Great Firewall and the U.S. PRISM project illustrate how technical infrastructures become political instruments that shape the flow of information and the contours of social life (Lyon, 2018). While these systems are presented as necessary for security, they simultaneously normalize practices of monitoring and control.

AI-based cybersecurity systems intensify these dynamics. By analyzing vast quantities of behavioral data and identifying anomalies, they promise predictive security but also raise concerns about algorithmic bias, digital discrimination, and opaque decision-making (Zuboff, 2019). These systems may inadvertently reproduce existing social hierarchies or classify certain groups as inherently risky, transforming technical tools into mechanisms of political surveillance. As such, ethical oversight and transparency have become pressing issues for democratic governance.

The rapid expansion of cybersecurity has also produced a growing digital defense economy. As of 2024, the cybersecurity market exceeded $250 billion globally (Floridi, 2022). This industry thrives on the discursive amplification of digital risks, echoing Beck's (1992) notion of the "risk society," in which modern economies increasingly depend on the continuous identification and management of new risks. Cybersecurity thus becomes both an economic engine and a generator of political narratives that justify technological intervention.

Moreover, the global distribution of cybersecurity capacities has produced new forms of inequality. A handful of dominant corporations—Cisco, Huawei, Microsoft, and others—define infrastructural standards and influence national security policies, creating a structure akin to digital colonialism (DeNardis, 2020). Dependence on foreign technologies constrains national autonomy, particularly in developing countries, limiting their ability to regulate their digital ecosystems.

The interplay between information security and digital sovereignty demonstrates how cybersecurity has become a fundamental dimension of state power. States now claim sovereignty not only over physical territories but also over data flows, network infrastructures, and the digital identities of their citizens. Policy initiatives emphasizing "cyber independence," "data localization," or "digital resilience" show how technical infrastructures are leveraged to strengthen national authority (Nye, 2017). These policies also enable the expansion of domestic surveillance and governance capacities, recalling Foucault's (1980) insight that knowledge and power mutually reinforce one another. As states manage digital risks, they simultaneously shape the behavior of digital populations through norms, standards, and regulatory frameworks.

Within this digital polity, information security discourse contributes to the construction of national identity. References to "cyber homeland defense" or "protecting the digital nation" frame cybersecurity as a patriotic duty, mobilizing public support and fostering what may be termed digital nationalism. This discursive strategy binds technical security practices to symbolic narratives of unity, sovereignty, and national strength.

Yet these developments raise significant democratic concerns. Measures adopted in the name of national security often limit privacy, restrict freedom of expression, and centralize informational power in state institutions. Authoritarian regimes may use cybersecurity rhetoric to suppress dissent, while democratic governments may expand surveillance under claims of public safety (Bauman & Lyon, 2013). As a result, the balance between security and civil liberties becomes increasingly precarious.

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.* Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

At the international level, cybersecurity policies shape global power relations. Cyberspace is both a domain of cooperation and conflict, where states attempt to establish normative power through standards, regulatory frameworks, and cyber diplomacy. However, these processes reproduce global asymmetries. Western states often promote their own norms as universal, while developing countries face structural pressures to conform (Deibert, 2013). This dynamic reflects Nye's (2017) concept of information power, whereby control over knowledge production and circulation becomes a decisive element of geopolitical influence.

In sum, the discursive construction of information security cannot be reduced to technological imperatives. Rather, cybersecurity operates as a multifaceted field through which power is exercised, legitimized, and contested. It shapes digital sovereignty, defines national interests, facilitates surveillance, and structures global hierarchies. Analyzing cybersecurity discourse from this integrated perspective reveals its role as a central mechanism of authority in the digital age—a technology of power that governs individuals, societies, and international orders alike.

4. FOUCAULT'S POWER–DISCOURSE FRAMEWORK AND THE THEORETICAL POSITIONING OF DIGITAL SECURITY

Foucault's power–discourse framework provides a robust theoretical foundation for understanding how modern societies construct knowledge, regulate behaviors, and legitimize security practices. In Foucault's perspective, power is not merely repressive or prohibitive; rather, it is productive, operating through the creation of knowledge, norms, and subjectivities (Foucault, 1977; 1980). This view is essential for analyzing cybersecurity, a field where technical narratives, political interests, and social control mechanisms are deeply intertwined. Cybersecurity discourse does not simply describe digital risks; it actively shapes the ways in which threats, vulnerabilities, and protective measures are socially, politically, and institutionally defined.

For Foucault, discourse is not a neutral representation of reality but a system that produces truth claims and organizes what can be thought, said, and governed (Foucault, 1980). Within this framework, terms such as "cyber threat," "critical digital infrastructure," "digital sovereignty," and "national cyberattack" are not purely technical concepts; they are discursive constructs produced by states, expert communities, and technology corporations. These constructs define which behaviors are seen as risky, which actors are labeled as potential threats, and which interventions become legitimate in the name of national security (Hansen & Nissenbaum, 2009). In this sense, cybersecurity becomes a "regime of truth" that generates authoritative knowledge and establishes a normative understanding of digital order.

Foucault's notion of disciplinary power further clarifies how modern security operates through continuous surveillance, normalization, and the regulation of individual conduct (Foucault, 1977). In the digital environment, these mechanisms intensify through big data analytics, behavioral monitoring systems, biometric authentication, and algorithmic profiling. Cybersecurity infrastructures classify user activities as "normal," "risky," or "suspicious," thereby producing a digital normativity that shapes how individuals behave online. Much like the panopticon, the awareness of constant visibility induces self-regulation, rendering cybersecurity not only a technical safeguard but a disciplinary technology that molds digital subjectivity (Lyon, 2018). Users modify their practices in accordance with standards set by security protocols, risk metrics, and algorithmic evaluations, which operate as subtle forms of behavioral governance.

Foucault's concept of biopolitics adds another layer to understanding how cybersecurity discourse governs populations. Biopolitics refers to techniques for managing life, regulating populations, and controlling collective risks (Foucault, 1977). Cybersecurity discourse extends this logic to the digital domain by constructing categories such as "digital citizens," "critical users," and "high-risk groups." National cybersecurity strategies increasingly emphasize notions of "cyber hygiene," "user awareness," and "responsible digital behavior," all of which function as biopolitical techniques disciplining the digital population (DeNardis, 2020). Through these practices, the state assumes a

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.*
Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

managerial role over digital life, aiming to control not only infrastructures but the behaviors and competencies of entire populations.

Seen through this Foucauldian lens, cybersecurity emerges as a field where technical systems, political agendas, and social regulation converge. Cybersecurity discourse legitimizes the expansion of surveillance systems, the restructuring of state authority, and the normalization of data extraction and monitoring. It shapes the conditions under which power is exercised in the digital age, determining who is protected, who is monitored, and which forms of control are justified. As such, cybersecurity is not merely a defensive measure; it is a discourse that produces new configurations of power and restructures the relationship between individuals, technology, and the state.

This study adopts Foucault's theoretical framework to examine how cybersecurity discourse is constructed, which actors produce it, and how it legitimizes new forms of digital governance. By situating cybersecurity within the broader power–knowledge nexus, the analysis highlights its role not only as a technical necessity but as a foundational mechanism that structures authority, shapes public perceptions, and reproduces asymmetrical power relations in contemporary digital societies.

5. INFORMATION SECURITY, THE SURVEILLANCE SOCIETY, AND THE REDEFINITION OF PRIVACY

In contemporary societies, information security is not merely a technical practice of protection, but a determining element of a new social order and form of power. As digital technologies penetrate every aspect of daily life, individuals' behaviors, modes of communication, and identity constructions have become bound to a data-driven system of traceability. Within this process, the discourse of information security has become one of the most powerful ideologies that legitimizes the surveillance society under the claim of "protecting the individual." The boundary between security and privacy is no longer merely technical but has turned into a political field of negotiation.

As Foucault (1977) argued in his analysis of the disciplinary society, modern forms of power discipline individuals not only through punishment but through continuous surveillance. The panopticon metaphor explains how individuals, feeling themselves constantly watched within an invisible mechanism of control, automatically regulate their own behavior. In the digital age, this model has been reproduced through information security infrastructures. However, this new panopticon is no longer based on the architectural design of prisons or schools, but on the algorithmic order of data flows. Digital panopticism operates through the constant recording, analysis, and classification of individuals' online behaviors, communication histories, and social relations (Lyon, 2018).

Today, information security policies appear to be implemented for the protection of individuals' online existence, yet these practices of protection often result in the restriction of individual privacy. As Bauman and Lyon (2013) describe in their concept of "liquid surveillance," modern forms of surveillance are no longer anchored in fixed institutions or centralized authorities; rather, they produce a dispersed logic of monitoring embedded within the digital infrastructure itself. Liquid surveillance refers to a structure in which individuals continuously supply data both to the state and to private sector actors. Users' social media interactions, location data, purchasing preferences, and even health information are collected as "anonymized" data under the framework of information security, yet this anonymity is often merely symbolic.

This condition lies at the heart of Zuboff's (2019) concept of "surveillance capitalism." Surveillance capitalism is a system that generates economic value from individuals' digital traces. In this system, security technologies function simultaneously as tools that protect the user and as instruments that measure, classify, and predict their behavior. Information security systems do not merely provide defense against attacks; they also establish a data-mining infrastructure designed to anticipate and influence user behavior. Therefore, while information security performs a technically protective function, it simultaneously becomes a tool of economic and political control. As Zuboff notes,

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.*
Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

data collected "in the name of security" often circulates across a wide spectrum of uses from targeted advertising to political manipulation.

In this process, the conceptual meaning of privacy has also undergone transformation. Privacy is no longer an absolute state of secrecy but has turned into a "negotiable" value. Individuals voluntarily share their personal data in order to benefit from digital services, gaining in return access, convenience, or social visibility. Han's (2017) concept of the "transparency society" explains this transformation: the modern individual no longer rejects surveillance but internalizes it as a productive form of social relation. The act of "self-disclosure" in social media practices shows that privacy is now linked not to individual autonomy but to performative identity construction. In this sense, information security functions not as a mechanism that protects privacy but as a normative system that determines which forms of disclosure are considered "safe" or "legitimate."

This normative system also reveals how the forms of digital power have been transformed. Within the framework of Foucault's concept of biopolitics, information security has become a technical form of power that governs not only individuals but entire populations. Through cybersecurity policies, states monitor digital populations, identify risk groups, construct threat models, and use this data in national security strategies. This process can be explained through Deleuze's (1992) notion of the "control society." Whereas in disciplinary societies power regulates individuals through specific institutions, in the control society power is continuous, timeless, and operates invisibly. Information security technologies constitute the technical infrastructure of this continuous control.

With the digitalization of surveillance society, the classical tension between security and freedom has acquired a new dimension. States and private corporations use the discourse of digital security to manufacture individuals' consent. The statement "If you have nothing to hide, you have nothing to fear" serves to morally legitimize surveillance. Consequently, individuals come to accept the loss of privacy as the price of security. However, this consent is often less a conscious choice than a reflection of the inescapable nature of technological infrastructures. Since avoiding digital services would mean social exclusion, individuals share their data under a form of voluntary coercion. This condition strengthens the "subjectifying" character of modern power; individuals are no longer merely the objects of surveillance but also its agents (Han, 2017).

Within this framework, information security policies perform a dual function. On one hand, they claim to protect individuals from cyber threats; on the other, this very claim of protection generates a mechanism of constant traceability and accountability. This mechanism gives rise to what Lyon (2018) calls a "logic of digital surveillance": individuals must authenticate their identities on digital platforms, record their transactions, and document their behaviors through algorithmic systems. Although this digitalization appears to promote transparency and safety, it simultaneously eliminates individual anonymity.

The pervasive expansion of information security technologies has transformed individual privacy from merely a legal concern into an ontological one. Privacy is now defined not through the distinction between public and private spaces but through data access and data control. In this context, "information sovereignty" should be considered a right belonging not only to states but also to individuals. Yet, in practice, this sovereignty often functions in favor of states or corporations. Users' control over their personal data is restricted by complex privacy policies and platform agreements. This asymmetric structure weakens the individual's digital autonomy and makes institutional surveillance permanent under the guise of security.

This regime of surveillance also reproduces social inequalities. The power to access and process data is directly related to economic and political resources. Major technology companies, by controlling global data flows, have gained the power to define information security standards. This situation influences state information security policies and blurs the boundaries between public safety and private interest (Deibert, 2013). Consequently, information security becomes a discursive field that mediates the centralization of power in both public and private domains.

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.* Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

In an environment where digital surveillance has become the norm, the redefinition of privacy emerges not merely as an ethical necessity but as a political imperative. Privacy must be approached within a broad framework that includes individuals' control over their digital identity, the boundaries of consent, and the social consequences of information sharing. In traditional security approaches, privacy was equated with the protection of secrecy; today, privacy signifies "data autonomy." In other words, the right to determine not only what information is hidden but also how it is used has become an integral part of security itself.

The future of information security policies, therefore, depends on the creation of ethical and legal frameworks that can redefine the balance between surveillance and privacy. The European Union's General Data Protection Regulation (GDPR) represents a significant step in this direction, yet the equal implementation of such regulations on a global scale remains extremely difficult. This is because information security is, at its core, a power relation: questions such as whose data is protected, whose data is shared, who watches, and who is watched are not technical but political in nature. Hence, the critical examination of information security discourse is essential to making visible the boundaries of freedom in the digital society.

Foucault's (1980) emphasis on the productive nature of power should be recalled here. Security technologies are designed not only to suppress threats but also to produce new forms of behavior and subjectivity. Information security defines the modern subject as a "digital citizen" a citizen who continuously authenticates their identity, shares their data, and remains accountable and traceable. Thus, security is not merely a practice of defense but also a production of subjectivity.

6. CONCLUSION

In the digital age, information security has evolved beyond a mere technical practice of protection to become one of the most dynamic forms of modern power. Cybersecurity technologies not only redefine the sovereignty of states but also reshape the boundaries of individual privacy. Security today is no longer confined to defending against external threats; it operates as a mode of social organization that governs data flows, regulates behaviors, and legitimizes surveillance. Thus, information security should be understood as both a technical and an epistemological–ideological category.

At the technical level, systems such as network defense, data encryption, and critical infrastructure protection ostensibly serve the purpose of safeguarding digital assets. Yet, behind this protective function lies a political apparatus of information control and surveillance. These infrastructures enhance the infrastructural power of states (Mann, 1984), while simultaneously constraining the autonomy of digital subjects. Particularly, AI-driven threat detection systems, due to their opacity, introduce new ethical dilemmas and extend governance into algorithmic domains. The technologization of security has therefore created a new coded form of politics.

At the societal level, the discourse of information security produces the ideological legitimacy of the surveillance society. Foucault's panopticon model has been reconstituted in the form of a digital panopticon operating through data centers and algorithms. Individuals are continuously monitored, measured, and classified in the name of protection. This mode of surveillance forms the core mechanism of what Zuboff (2019) terms "surveillance capitalism," where personal data are transformed into economic value. Information security technologies thus function as the technical infrastructure through which both the state and capital reproduce power.

In this context, the tension between security and privacy emerges as the central paradox of digital society. Individuals willingly surrender their privacy in exchange for access and security; privacy has ceased to be an inherent right and has become a managed privilege. This transformation necessitates a redefinition of freedom itself. In contemporary digital life, freedom is no longer measured by one's ability to escape surveillance but by one's capacity to maintain autonomy even under its constant gaze.

Therefore, the future of information security policies must be shaped not only by technical solutions but also by ethical, legal, and political principles. Genuine digital security requires a

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.* Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

framework that guarantees not only the resilience of systems but also the sovereignty of individuals over their own data. This calls for a redefinition of security from a mechanism that merely protects individuals to one that empowers them.

Ultimately, information security stands as one of the most powerful forms of authority in the digital era. Through its dual function of protection and control, it embodies the central contradiction of modernity. Hence, information security should not be perceived solely as a technical issue but as a constitutive axis of social order, freedom, and digital citizenship. Only by approaching it in this way can the balance between surveillance and liberty be ethically reestablished in the digital age.

Information About Ethics Committee Approval: Ethics committee approval was not required.
Research And Publication Ethics Statement: The authors declare that the ethical rules are followed in all preparation processes of this study. In the event of a contrary situation, the ASSAM International Refereed Journal has no responsibility and all responsibility belongs to the author of the study.
Conflict Of Interest Statement: There is no conflict of interest among the authors and/or any institution.
Contribution Rate Statement: The authors contributed equally to the work.

REFERENCES

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Carr, M. (2016). US power and the internet in international relations: The irony of the information age. Palgrave Macmillan.

Castells, M. (2010). The rise of the network society (2nd ed.). Wiley-Blackwell. https://doi.org/10.30935/cedtech/6177

DeNardis, L. (2020). The Internet in everything: Freedom and security in a world with no off switch. Yale University Press.

Foucault, M. (1977). Discipline and punish: The birth of the prison. Vintage Books.

Foucault, M. (1980). Power/Knowledge: Selected interviews and other writings 1972–1977. Pantheon Books.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. International Studies Quarterly, 53(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity Press. https://doi.org/10.4000/communication.11962

Nye, J. S. (2017). Cyber power. Harvard Kennedy School.

Solms, B. von, & Niekerk, J. van (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Nye, J. S. (2017). Soft Power and Public Diplomacy Revisited. The Hague Journal of Diplomacy, 12(1-2), 1–6. https://doi.org/10.1163/1871191X-14101013

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs. https://doi.org/10.1007/s00146-020-01100-0

Lacy, M., & Prince, D. (2018). Media framing of cyber threats: The social construction of security. Journal of Information Warfare, 17(2), 1–14.

Bauman, Z., & Lyon, D. (2013). Liquid surveillance: A conversation. Polity Press. https://doi.org/10.22230/CJC.2014V39N3A2843

Deibert, R. (2013). Black code: Inside the battle for cyberspace. McClelland & Stewart.

Floridi, L. (2022). The ethics of information (2nd ed.). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199641321.001.0001

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Deleuze, G. (1992). Postscript on the societies of control. October, 59(1), 3–7.

Atıf/Citation: Mammadov, R. (2025). **Cybersecurity Discourses and Social Power Relations: The Political and Strategic Dimensions of Digital Security**. *ASSAM International Refereed Journal.* Special Issue, 111-121.
https://doi.org/10.58724/assam.1818761

Foucault, M. (1980). Power/knowledge: Selected interviews and other writings, 1972–1977 (C. Gordon, Ed.). Harvester Press.

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. Alternatives: Global, Local, Political, 27(1_suppl), 63–92. https://doi.org/10.1177/03043754020270S105

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR)relevant theory? International Political Science Review, 27(3), 221–244. https://doi.org/10.1177/0192512106064462

Duffield, M. (2019). Post-humanitarianism: Governing precarity in the digital world. Polity Press.

Beck, U. (1992). Risk society: Towards a new modernity. Sage Publications. https://doi.org/10.2307/3341155