Robotics & Automation Engineering Journal
ISSN: 2577-2899

Juniper Publishers
key to the Researchers

Research Article
Volume 6 Issue 5 - September 2025
DOI: 10.19080/RAEJ.2025.06.555698

Robot Autom Eng J

Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge

Loubna Ali1*, Anna Rostomyan2, Ali Ali3

[1]*Faculty of Computer Science and Informatics, Berlin School of Business and Innovation, Germany*

[2]*Department of Psychology, Media University of Applied Sciences, Germany*

[3]*Chairman of the ARISPA Cybersecurity Committee, Beirut, Lebanon*

Submission: August 10, 2025; **Published:** September 02, 2025

***Corresponding author:** Loubna Ali, Faculty of Computer Science and Informatics, Berlin School of Business and Innovation, Germany

Abstract

In an era of global connectivity and dataization, cybersecurity is often viewed as a value-neutral technical bulwark against cyber risks. By contrast, the present article argues that cybersecurity functions as a governmental apparatus-one rooted in the power and knowledge systems of our time. Drawing on Michel Foucault's concepts of panopticism, disciplinary power, and good governance, it critically examines how cybersecurity technologies not only protect digital objects, but also categorize, normalize, and regulate them. Drawing on case studies such as the Pegasus spyware scandal, social credit systems in East Asia, and the algorithmic surveillance practices of big tech companies, the paper demonstrates the ways in which cybersecurity has evolved into a subtle and pervasive tool for psychological and behavioral control. The main theoretical argument is thus supported by an original dataset from an empirical user survey, explored using Principal Component Analysis (PCA) and k- means clustering. The findings present two key user personas: (i) cautious adherents, who embrace behaviors of surveillance and self-governance, and (ii) resistant freelancers, who exhibit distrust and resist the influence of algorithms. Together, these findings describe how cybersecurity systems participate in shaping digital subjectivity, determining who is visible, trusted, and heard online. The article concludes with a call to reframe cybersecurity as a political and philosophical issue that requires an ethical examination of how digital infrastructure constructs identity, access, and the limits of freedom in the information age.

Keywords: Cybersecurity; Foucauldian theory; Surveillance; Disciplinary power; Governmentality; Digital subjectivity; Social credit; Algorithmic governance; Data politics; Technopolitics

Introduction

In a digitally interconnected world, cybersecurity has become a cornerstone of contemporary governance, institutional policy, and personal protection. It is generally introduced as a technical or legal safeguard-a depoliticized shield against external threats such as hacking, data breaches, or cyberterrorism. But this framing risks concealing a more complex and politically charged truth: cybersecurity also functions as a technology of power, shaping digital behaviour of the users, enforcing norms, and producing compliant subjects.

This article, thus, argues that cybersecurity is not merely a security practice, but a productive force involved in the production of contemporary subjectivity and the exercise of power. Drawing on Michel Foucault's power/knowledge theory, the study locates cybersecurity within the broader paradigm of disciplinary societies, where not only are individuals secured, but they are being surveilled, controlled, evaluated, and normalized by algorithmic assemblages and data-driven classification.

The guiding question here is: When does cybersecurity turn from being less of a protective measure to more of a controlling mechanism? And how does this shift manifest in real-world applications? To explore this tension, the paper examines three critical case studies:

- The use of Pegasus spyware as a covert surveillance tool;
- The Social Credit System in parts of East Asia as a framework for behavioral normalization;
- And the data surveillance regimes of Big Tech corporations, whose algorithmic architectures subtly discipline users through visibility, scoring, and recommendation systems.

With the complement of theoretical analysis, this research draws on empirical data collected from a survey of participants

using Principal Component Analysis (PCA) and K-Means clustering. The objective is to identify not only the abstract logic behind control inherent in cybersecurity systems, but also how these mechanisms are experienced, embodied, and contested by individuals in their quotidian online activity, as well as taking into account the psychological aspect.

Lastly, this paper seeks to redefine cybersecurity as a political and philosophical matter rather than a legal or technical one. Through its examination of the ethical, epistemological, and disciplining dimensions of cybersecurity, the research contributes to our understanding of how digital power operates in the age of data.

Related Works in the Literature

In recent times, scholars across disciplines have come to consider cybersecurity on a broader non-technical foundation more and more, seeing the wider social, ethical, psychological, legal, and political stakes at issue. Disciplines of critical security studies, digital sociology, and political theory alike have all made strides that cybersecurity possesses substantial embedded connections to power relations, governance, and social ordering [1-2]. These are criticisms that indicate a growing worry that cybersecurity, instead of being used to safeguard users, may result in the growth of surveillance regimes and novel forms of control by states and non-state actors alike, also in case of data breaches, damaging the psycho-emotional well-being of the affected users leaving them with social anxiety and diminished self-value because of the caused breaches of data and damaged security.

The work of Michel Foucault, specifically, studying power, knowledge, and surveillance, has most directly established the aim of this trend. His ideas of panopticism, disciplinary power, biopolitics, and governmentality have come to be most intensely called upon to treat digital space [3-4]. This line of scholarship assumes that control in contemporary societies happens not merely through formalized institutions and statutory code, but diffuse and usually unobtrusive systems of regulation embedded in normal technology use.

Some academics have attempted to link Foucault's work directly with the internet. For instance, Boyle [5] explores the concept of "Foucault in cyberspace" and how apparently diffuse digital technology can inscribe disciplinary and sovereign forms of exercising power. Wichum (2013) employs Foucault's later work on dispositifs to analyse security as a more than merely a response to risk, but as a rationality of government that creates and governs populations. Similarly, Askari and Sheikh [6] apply the panopticon model to U.S. cybersecurity and intelligence systems, illustrating how mass surveillance infrastructure exercises a new form of soft, yet totalizing, control. Lysova [7] examines video surveillance in public spaces, contrasting "surveillance society" with "security state," using Foucauldian tools to understand normalization and internalized discipline.

However, despite these valuable contributions, much of the existing literature treats Foucault's concepts either metaphorically or selectively. Many studies focus narrowly on the metaphor of the panopticon without grounding the analysis in Foucault's broader theoretical system-particularly the interplay between knowledge production, normalization, and subject formation. Furthermore, few works directly interrogate the specific role of cybersecurity infrastructures in producing forms of knowledge that define, manage, and act upon digital subjects. Thus, there is still a gap in understanding cybersecurity as a regime of power/knowledge that actively shapes behaviours and identities through technical systems, policies, and practices.

Moreover, Foucault in his 1954 works connected the human mind and psyche to a broader social, cultural, economic, political, and environmental influence to promote a positive change, mental health, and solid protection and empowerment, at individual and systemic organizational and governmental levels [8]. Furthermore, in his earliest works devoted to human psychology, Foucault believed that psychology, as a discipline, could have an important function in improving people's well-being and in overcoming challenges in everyday life [9], therefore, it should be taken into account while analyzing any aspect of human activity, including digital behavior.

This paper seeks to fill that gap by offering a focused Foucauldian reading of cybersecurity as a technology of governmentality. Rather than viewing cybersecurity merely as a neutral framework for risk mitigation, it will be analysed as a system that produces compliant subjects through the normalization of digital monitoring, self-regulation, and algorithmic governance. By bringing Foucault's full theoretical apparatus into dialogue with concrete cybersecurity practices-such as spyware, credit systems, and platform-based data tracking- this paper contributes to contemporary debates on digital authority, surveillance capitalism, emotional and psychological well-being, and the ethics of power in the information age.

Theoretical Framework: Power, Knowledge, Psychology, and Surveillance in Foucault

Michel Foucault's work offers a difficult analytical framework for understanding modern societies' rule-not by coercive domination, but by complex webs of surveillance, normalization, and knowledge production. Challenging traditional assumptions about power as a space possessed by individuals or groups, Foucault [10], Foucault [11] redefines power as relational, diffuse, and productive. According to the author, thus, power not only represses, it produces realities, categories, and truths. At the heart of this perspective, therefore, lies the thesis that power and knowledge are not autonomous domains but inter-constitutive: all knowledge is constituted by power relations, and power is enacted by means of the production and distribution of knowledge.

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

Power/Knowledge

Foucault argues that knowledge systems-medical, legal, or computational-are imbued with power relations. These systems do not represent the world in a neutral manner; they actually make it by mapping what is true, normal, or deviant [11]. To this extent, cybersecurity, with its classificatory logics (e.g., safe vs. risky practice, trusted vs. suspect behaviour), can be read as a regime of power/knowledge. Through threat modelling, risk assessment, and behaviour prediction, cybersecurity makes digital subjects and enacts normative expectations.

Psychological Perspectives

Foucault's work encourages a critical examination of the assumptions, practices, and power dynamics within the field of psychology, claiming a more nuanced, socially-aware and self- aware approach to our understanding of the human mind, human psyche, and overt human verbal and non-verbal behaviour [8]. To Foucault, in psychology, formerly there used to be a tendency to neglect the cultural, social, and situational context perspectives in favour of the medical and natural science perspective. Yet, he strongly believed that a deeper understanding of the psychological phenomena (including human behavior) also implies a solid understanding of the accompanying social and cultural phenomena, which we should also take into account while analyzing the aspect of cybersecurity, where the protection of the users' "safe" psychology (being social and cultural entities), including psychological and emotional well-being of the users has to be of paramount significance.

Surveillance and Disciplinary Power

In Discipline and Punish [10], Foucault describes how institutions such as schools, prisons, and hospitals exercise power-through watching, training, and correcting, not through violence. The metaphor of the old panopticon, a prison design that provides permanent visibility without physical force, describes how observing leads to the involved parties' self- regulation. The panoptic model has thus been at the heart of critical studies of digital surveillance [4]. Thence, in virtual space, subjects internalize surveillance logic, self-regulating their conduct in anticipation of being watched-a Foucauldian "docile bodies" reminded of perpetual visibility. This brings us to the ultimate assumption that the ability of an emotional and operational self-regulation of the users is of high vitality with the knowledge that they are being surveilled. Moreover, it can be reinforced to a higher level by means of surveillance.

Governmentality and Population Management

In subsequent work, Foucault uses the notion of governmentality-the "conduct of conduct"-to describe how modern states and institutions manage populations less through legality and more through decentered means that affect human decision-making and behaviour [12]. Cybersecurity policies, particularly if enacted at scale (e.g., national firewalls, social credit systems, predictive policing), are a classic manifestation of this type of power. They govern by promoting certain types of behaviour, delegitimating others, and integrating mechanisms of control into the design of everyday digital life. Rather than depending on direct repression, cybersecurity is thus a practice of preemption, prevention, protection, and algorithmic intervention.

From Panopticism to the Surveillant Assemblage

Building on Foucault's observations, scholars such as Haggerty and Ericson [4] have conceptualized the "surveillant assemblage" as a dispersed, networked system of data collection beyond the spatial limitations of the panopticon. Through big data and AI-enabled surveillance in current times, individuals become "data doubles", which are readable, knowable, and actionable in ways unknown to them. This post-panoptic account is in line with Foucault's notion that power in contemporary times does not operate through visibility, but through the constant production and investigation of knowledge.

In a nutshell, Foucault's theory of power/knowledge, discipline mechanisms, psychology, and governmentality provide a solid theoretical base for seeing cybersecurity as more than a technical neutral sphere, but as a control regime producing digital subjects via circulation of risk, surveillance, and normalizing norms. Throughout this research, these concepts will be applied to explain actual cybersecurity practices and technology and how digital infrastructures normalize surveillance and condition user behaviour, as well as protect psychological and emotional well-being therein, in subtle yet meaningful ways.

Cybersecurity as a Modern Apparatus of Power

In Foucauldian theory, an apparatus (dispositif) is a diverse collection of discourses, institutions, laws, administrative measures, and technical mechanisms that respond to an immediate problem or need at a particular historical moment [11]. Apparatuses are not merely repressive instruments; they are strategic deployments that produce specific types of subjectivity, conduct, and knowledge. Cybersecurity-even most broadly conceived as a technically reactive project aimed at deterring digital violence-is viewed to operate as a new technology of power that demands mastery over populations, as well as over subjects by introducing apparatuses of surveillance, control, and overall shaping of behaviour.

The Problematization of Threat

All apparatus begins from a problematization. For cybersecurity, the virtual environment is envisioned as inherently insecure, characterized by constant danger: malware, data breaches, foreign cyberattacks, disinformation, and insider threats. This atmosphere of fear and ambiguity legitimates the enlargement of cybersecurity controls and the delegation of power to state and corporate agencies [1-2]. These actors not only respond to threats, but also constitute them-constructing knowledge about what constitutes "risky" behavior, data "breach",

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

"suspicious" users, or "legitimate" security practices. In doing so, cybersecurity is an epistemological framework that builds reality rather than mirrors it.

Surveillance as a Normalized Condition

As cybersecurity infrastructures expand, continuous monitoring is a normalized state of digital life. From endpoint detection programs to behavioral monitoring and threat intelligence software, security tech collects and inspects massive volumes of user data, including private data. This view is blind-eyed-it happens invisibly, silently, algorithmically behind the scenes. Post-Foucault's investigation into the panopticon, this condition draws forth self-discipline. Users come to appreciate the logic of taking care of oneself (including psychological and emotional self-care), policing the behavior that might be caught and punished even absent overt force [4]. This self-governing dynamic recapitulates the shift away from external enforcement towards internal regulation and self- protection.

Risk, Classification, and Digital Subjectivity

Cybersecurity is a classification system. Users are always profiled based on patterns of access, device activity, communication activity, and compliance with security policies. These two categories-trusted and untrusted, high-risk and low-risk-are not technical but extremely political. They dictate access, visibility, and legitimacy in digital spaces. In doing so, cybersecurity becomes a player in the creation of digital subjectivity: it enacts what it means to be a "secure" user, a "safe" platform, a "compliant" employee, or an "inside potential threat". Such categories are not politically neutral ones; they are generated from and regenerate particular relations of power [11].

Governmentality and Governance of Populations

Cybersecurity policy today extends beyond the subject and into governance of populations. National cyber policies, digital identity systems, and AI-powered risk analyses not only aim to secure systems, but also to shape behavior at scale. With predictive analytics, automated prompt decision-making, and regulatory mandates, cybersecurity is a form of governmentality [12]. Cybersecurity shapes behavior by embedding norms into platforms, protocols, and infrastructures. This is pre-emptive management, not reactive management-it foresees threats ahead of their occurrence and treats users as potential threats to be eliminated. The result is a world in which freedom and trust are recoded into the vocabulary of compliance, auditability, safety, protection, and regulation.

Case Studies

This section presents three case studies that illustrate how digital surveillance technologies and cybersecurity software are contemporary instruments of power. Extending Foucault's writings on surveillance, discipline, normalization, and governmentality, the cases illustrate how digital infrastructures discipline conduct, produce knowledge, and govern individuals and populations-often in ways that are unseen and beyond traditional legal controls.

Pegasus Spyware and Political Surveillance

Pegasus, a zero-click spyware developed by the Israeli firm NSO Group, can penetrate smartphones without the need for any user action. Once activated, it has the capacity to drain messages, emails, audio, video, and location data, converting personal devices into real-time surveillance devices [13]. This can really be very beneficial for protecting users from phishing (fraudulent emails), smishing (sms phishing) and vishing (voicemail phishing). Despite being labeled as a counterterrorism tool, investigative journalism has untangled its use in the surveillance of journalists, political opponents, and human rights activists across areas in Europe, the Middle East, and South Asia. Therefore, we believe that it can be also very efficient in protecting users within various companies, organisations, and institutions across the Globe.

From a Foucauldian perspective, Pegasus is a hypermodern form of panopticism [10], where surveillance is no longer bound by physical space or institutional architecture. The power of these tools lies not only in their ability to monitor, but in their ability to induce self-regulation-individuals may modify their behavior at the mere suspicion of being under surveillance. This is consistent with Foucault's formulation of disciplinary power, which produces docile bodies not through coercion, but through normalization and internalization. In addition, the deployment of Pegasus amounts to what Foucault [11] characterized as a dispositif-a strategic constellation of state power, private industry, and legal ambiguity that enables the exercise of power through technologically mediated visibility.

Social Credit Systems and Mass Normalization

In East Asia, particularly in the Chinese setting, Social Credit Systems (SCS) have appeared to measure individuals' trustworthiness by consolidating behavioral, financial, legal, and social data. The systems rank citizens according to digital behavior, with decisions on access to services, loans, mobility, and public welfare [14-15]. Good scores are rewarded, and bad scores result in social sanctions such as restricted travel or even exclusion from work.

This technology functions as a modality of governmentality, whereby populations are managed not through explicit repression, but by predictive analytics and behavioral scoring [12]. Thus, SCS programs promote conformity and discourage deviance, writing normative values into algorithmic feedback loops. Subjects thus become self-managing, aligning their behavior with state-defined standards of "good" behavior. In Foucauldian terms, this is a classic case of normalization, whereby normative behavior is defined, measured, and policed not by law, but by a socio-technical system that pervades everyday life.

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

Big Tech and the Invisible Discipline of Algorithms

Large platform corporations-like Google, Meta (née Facebook), Amazon, and TikTok- hold immense influence over online communication and culture. These companies harvest and process user data en masse, using algorithmic systems to filter content, personalize experience, and commodify behavior. Shoshana Zuboff's model of surveillance capitalism (2019) is a well-suited description of this apparatus, in which human behavior is made a predictable commodity for targeted persuasion and profit.

Although not traditionally associated with state power, these sites exercise a form of algorithmic governance that aligns with Foucault's understanding of *disciplinary power*. Thus, instead of explicit coercion, users are managed through code, metrics, and algorithms-they modify their behavior to adhere to platform norms, optimize visibility, or avoid deplatforming. Haggerty and Ericson [4] have referred to this as the "*surveillant assemblage*"-a decentralized, data-driven assemblage of observation and classification that acts upon the individual without needing physical presence or legal authority.

In fact, this is an invisible and internalized discipline. The users adapt to algorithmic systems that are not transparent either in their operation or in their capacity to shape preferences, attitudes, and decisions. As a result, the platforms are norm-producing infrastructures that nudge the behavior, while preserving the illusion of freedom and neutrality.

Analysis and Empirical Findings: Cybersecurity as a Foucauldian Apparatus

To complement the theoretical framework, an empirical survey was also conducted to study how individuals perceive and internalize cybersecurity and surveillance methods in online environments. The survey was designed using Google Forms and distributed on multiple social media sites. Participants were recruited through convenience sampling and came from various countries and cultures. While the sample is not statistically representative, it provides insightful information regarding digital attitudes and behavioral responses to cybersecurity initiatives by regions.

The survey findings, as read and interpreted in context with the theory of Michel Foucault's ideas, set the stage for the central argument of this paper: namely, that information security infrastructures are increasingly fewer protective systems in the classical sense, but advanced apparatuses of governance. This sub-section proceeds to outline the theoretical elements of this very argument, and synthesises the most salient empirical information from the survey. Each discussion is followed by a corresponding figure.

From Protection to Governance

In the course of the above case studies, we witness a shift in the work of cybersecurity-from a technical response to online threats, to a form of anticipatory governance. Spyware like Pegasus operates behind the scenes, instilling self-censorship; social credit systems write codes of conduct by means of scores and incentives; and algorithmic infrastructures within Big Tech platforms discipline users through managing their exposure, visibility, and reputation.

This shift is in line with Foucault's theory of governmentality, wherein subjects are not merely protected, but actually regulated by norms embedded within technical systems [12]. As indicated in (Figure 1), only 18.6% of the respondents were absolutely at ease with automated classification systems. 70.9% of the respondents indicated discomfort or opposition-31.4% believing that such systems exercised too much power with no one to answer for it, and 10.5% indicating outright opposition in the belief that they were mechanisms of control. Even among the 39.5%, who were moderately comfortable, the majority indicated an uncompromising call for transparency. We believe that such results register an expanding public awareness that risk classification is not a politically neutral exercise of protection, but a vivid practice of social ordering.

As we can see from the (Figure 1) above, the vast majority of the respondents are either "uncomfortable" or "somewhat comfortable" with the automated classification systems, which brings us to the assumption that people are uneasy with being constantly surveilled and further digital transparency.

Surveillance Without Walls

Foucault's [10] panopticon as metaphor, previously architectural, has become ambient. Digital surveillance pervades public and private space: smartphones, social media, bank systems, and workplace platforms. The logic of ubiquitous visibility still underlies but is now written into infrastructures that operate algorithmically and twenty-four hours a day-albeit sometimes beneath users' radar.

Survey results reflect internalization of power during the Internet age. As can be seen from (Figure 2), over 71% of respondents reported they had changed their behavior due to perceived online monitoring. More specifically, 41.9% reported avoiding posting or sharing sensitive opinions, and 29.1% reported that they have become more cautious overall in their use of the Internet. As low as 19.8% reported that they are not influenced by surveillance, and only a minority (9.3%) even try to hide or avoid their activity. These findings strongly support Foucault's panopticism theory, showing the shift from coercive surveillance to self-regulation, as users begin to internalize surveillance and control their expression under ambient visibility conditions.

As it can be detected in (Figure 2), the vast majority of the respondents reported a change in their digital behavior on various platforms becoming more cautious with their digital activity. This very finding brings us to the assumption that people have started

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

self-regulating their behavior in line with the advancement in science and technologies and have become more self-aware and socially-aware to be able to protect themselves from resultant data breaches.

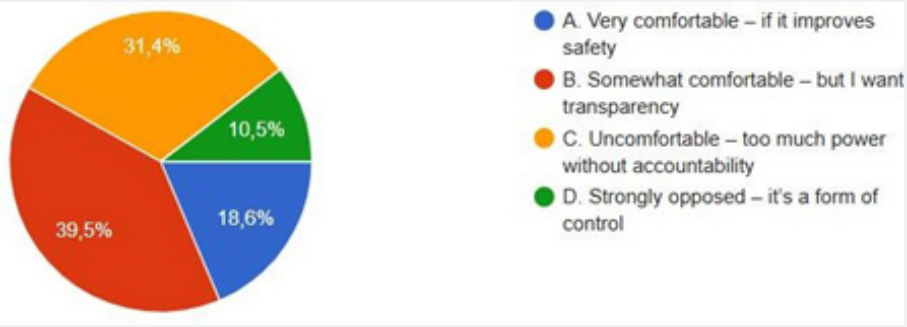

Figure 1: Respondents' comfort with automated risk classification systems.

Source: Creation of the authors.

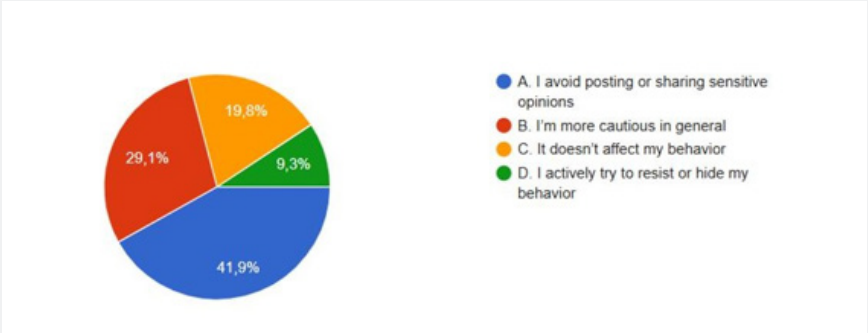

Figure 2: Behavioral change due to perceived online monitoring.

Source: Creation of the authors.

Knowledge as a Means of Control

It is our firm belief that cybersecurity technologies do not merely protect; they also make knowledge. They categorize individuals into threats or assets, secure or suspect, compliant or deviant. By doing so, they perform Foucault's [11] power/knowledge, in which epistemological control is never neutral, but always intimately linked with governance. The labeling of a user is a political action with the power to determine that person's access, opportunity, protection, regulation, and freedom.

As can be seen in (Figure 3), only 36% of respondents were unconditional in accepting being provided with a platform-based trust score. A larger number-47.7%-accepted it conditionally, on the proviso that the scoring needed to be transparent and understandable. A further 11.6% actively disagreed with the suggestion as being unfair or manipulative, and 4.7% were undecided. These findings point to pervasive distrust of algorithmic classification, particularly when it is neither visible nor under user control. This agrees with Foucault's power/knowledge theory, in which rating and classifying systems are never neutral-they are tools of governmentality, shaping access, trust, digital literacy, and digital legitimacy.

The results of the answers speak for themselves pointing out to the fact that they mostly feel at ease accepting being provided with a platform-based trust score. Though it should be highlighted that of course raising the awareness of the users of its profitability can increase their interest and engagement rates.

Subject Formation and Normalization

Power, as Foucault [10] sees it, is not merely repressive-productivity. It creates subjects that internalize norms and adapt accordingly. On the internet, users of the net are subjects and also acts of surveillance: they learn how to act in accordance with platform norms, become visible as much as possible, and get accordingly disciplined by the algorithms.

Empirical evidence strongly pinpoints towards the process of digital normalization. As can be seen in (Figure 4), nearly 45% of respondents (8.1% always, 37.2% sometimes) reported that they consciously modify their tone, content, or behavior to

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

align with algorithmic expectations. This shows that users are not just using platforms-they are being subtly shaped by them. Conversely, 31.4% reported never altering their behavior, and 23.3% responded that they rarely do. These results confirm Foucault's argument that power works best when internalized: users learn what is encouraged, tolerated, or punished, and adapt accordingly to remain visible and included in algorithmically governed systems.

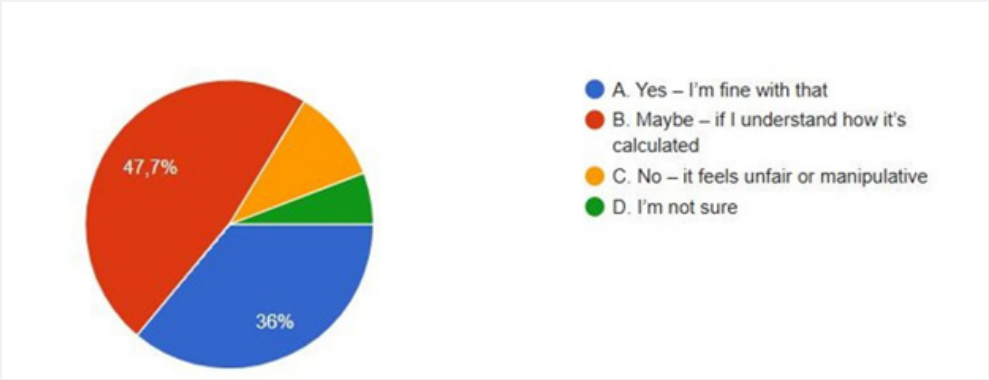

Figure 3: User acceptance of automated trust scores in exchange for services.

Source: Creation of the authors.

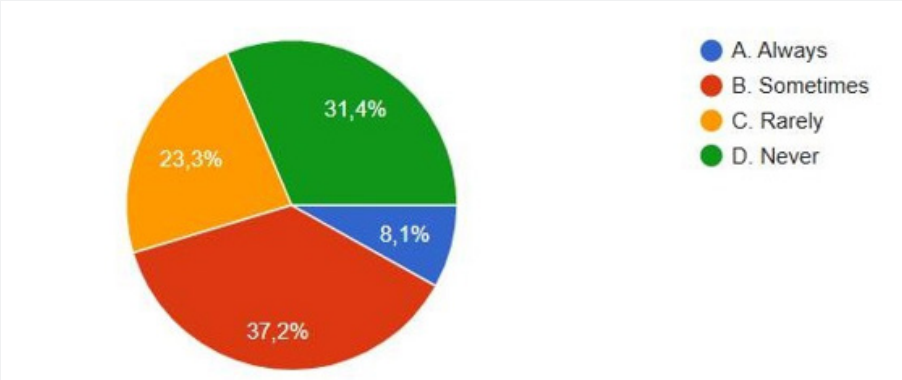

Figure 4: Frequency of user behavior adjustment to align with algorithms.

Source: Creation of the authors.

This very finding comes to suggest that people are highly inclined towards adjusting their behavior (including digital behavior) when being aware that they are being surveilled. The same holds true to real-world life scenarios when we adjust our overt behavior when being surveilled.

Diffuse and Decentralized Power

One of the features of cybersecurity now is that it is diffused. Power is no longer centralized in the state or in traditional institutions. Instead, it is spread out across a network of actors: states, tech companies, private contractors, and automated systems. This decentralization is consistent with Foucault's perspective of power being relational, infrastructural, and located in everyday practices.

Public opinion is showing both polarized trust and growing acknowledgment of cybersecurity's decentralized authorities. As (Figure 5) shows, 39.5% of the respondents favored government agencies as the primary custodians of cybersecurity surveillance, while 26.7% accepted independent regulatory agencies. Notably, only 15.1% trusted platforms or companies to self-regulate, and 18.6% advocated for citizen-led democratic participation. These results demonstrate that while many still trust in state-based authority, a large section of the public has a clear preference for alternative mechanisms of accountability. The diffusion confirms Foucault's conception of power as dispersed yet infrastructural-based in networks wherein control must be constantly negotiated, as opposed to assumed.

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

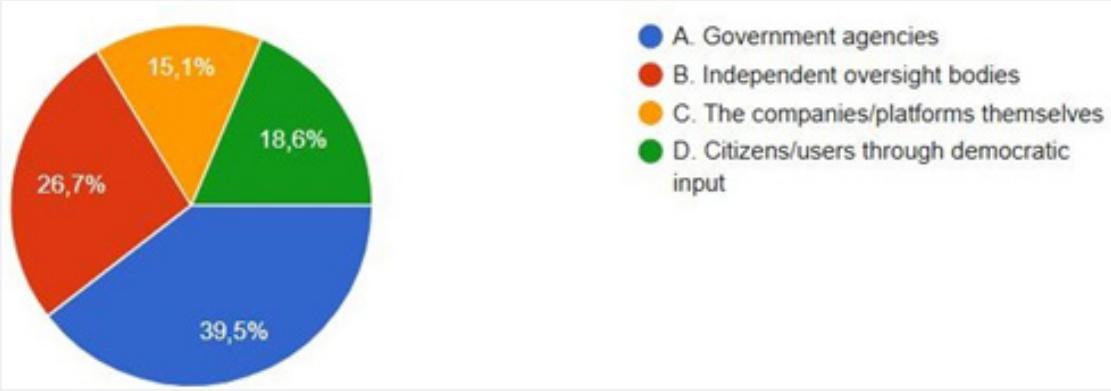

Figure 5: Respondents' preferences for surveillance governance and control.

Source: Creation of the authors.

Per our findings elucidated in (Figure 5) above, it can still be concluded that about 40% would prefer relying on government agencies for regulations, which comes to suggest that people are still inclined to put trust in higher authoritarian entities. Nonetheless, the other 60% feel easy in other corresponding entities to regulate the underlying processes, which depends on the regulations of the other correlated infrastructures.

Both theoretical and empirical considerations suggest that cyber security systems have evolved from defense-only technologies to become governance infrastructures. They structure behavior, produce classifications, and re-procreate norms through processes often hidden beneath protectionist rhetoric. The questionnaire testifies that users are not passive subjects; they are alert, suspicious, cautious, and increasingly skeptical of the systems watching and judging them.

Lastly, cybersecurity does not merely secure digital environments-it constitutes valid digital subjectivities, delineates acceptable conduct, and regulates who belongs in the digital order. In doing so, it is an effective machinery of digital governmentality, where the lines between security, surveillance, and subjectivity have become deeply and increasingly intertwined.

Clustering and Dimensional Analysis of Digital Subjectivity

To complement the theory research and provide empirical depth, we conducted a computational analysis of survey responses using unsupervised machine learning techniques. We used Principal Components Analysis (PCA) to reduce the data dimensionality for ease of visualization and analysis then we applied K-means clustering to the coded responses. This allowed us to split up participants into meaningful patterns of behavior in terms of their behavior and attitudes towards electronic surveillance, categorization, and self-regulation.

Methodology: K-Means and PCA

All ten of the survey questions were treated as categorical variables and label-encoded in numeric form. Subsequently, K-Means clustering on the encoded information by Euclidean distance was conducted to cluster respondents according to shared response patterns. To visualize and interpret the resulting clusters, we used Principal Component Analysis (PCA) to project the high-dimensional data into two dimensions, while preserving the highest variance.

As can be seen in (Figure 6), the projection readily separated two groups of users, testifying that participants varied in their experience and attitudes to digital governance and algorithmic discipline.

This very finding might come to suggest that people differ in their personality traits as well, which might underlie in their choices in digital behavior.

PCA Visualization and Cluster Identification

As we have seen, (Figure 6) shows a 2D scatterplot of the survey respondents, with one point per respondent and colors by cluster membership. The two clusters can be clearly distinguished, suggesting latent differences in how users engage with surveillance and control technologies.

Each point is a respondent; the clusters are dominant behavioral patterns.

PCA loading analysis (Table 1) revealed the dimensions most strongly predictive of the separation between the two clusters were:

Q3. Behavioral avoidance of profiling

Q2. Reaction to perceived surveillance

Q6. Adjustment to algorithms for visibility

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

Q4/Q5. Trust in digital classification systems

Q8. Views on governance and control of cybersecurity

These variables mentioned above correspond directly to the theoretical constructs of **self- regulation**, **knowledge as control**, and **normalization**, as developed in earlier sections.

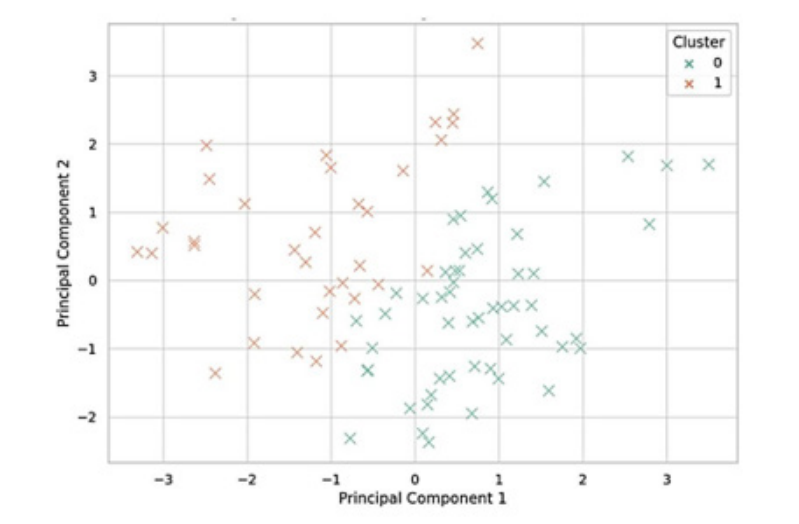

Figure 6: K-Means Clustering Results Visualized via PCA.

Source: Creation of the authors.

Table 1: Top Contributing Questions to Cluster Separation (PCA Loadings).

Question	Survey Item	Theoretical Link
Q2	How does online monitoring affect your behavior?	Surveillance/Internalization
Q3	Have you ever changed your online activity to avoid profiling?	Risk avoidance
Q4	Comfort with cybersecurity classification (low/high-risk)	Governance logic
Q5	Acceptance of trust score systems	Knowledge as control
Q6	How often do you adjust your content for algorithms?	Subject formation
Q8	Who should control surveillance tools?	Power decentralization

Source: Creation of the authors.

In this way, we have attempted to find out indivdual choices in **self-regulation**, **knowledge as control**, and **normalization** that we are mainly concerned of.

Cluster Profiles and Subject Typologies

Using the top PCA-contributing features, we analyzed the most common response patterns within each cluster. This enabled the construction of two interpretive user profiles that align with Foucault's theory of subject formation:

Cluster 0 – "Cautious Conformers"

- Frequently adjust behavior to avoid triggering surveillance.
- Modify content for better algorithmic visibility.
- Express discomfort with automated classification.
- Tend to accept government-led control over surveillance tools.

This group embodies Foucault's [10] concept of the "docile body"-subjects who have internalized the gaze of power and self-regulate within digital systems to avoid penalties and maintain legitimacy.

Cluster 1 – "Resistant Independents"

- Report little or no behavioral change due to surveillance.
- Rarely adjust content to match platform expectations.
- Largely reject trust scores and behavior-based classification.
- Nevertheless, some still express trust in institutional authority.

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

This group reflects a more resistant or indifferent stance toward digital governance, rejecting behavioral conformity even when aware of surveillance infrastructures. Their resistance may not be overt, but it implies a potential limit to the effectiveness of algorithmic normalization.

Theoretical Implications

The cluster result verifies the main thesis of this paper: cybersecurity not only functions as a technical paradigm for military protection, but also as a governmentality technology that produces digital subjectivity through intricate systems of classification, feedback, and conduct adjustment.

Moreover, cautious Conformers show how power operates through obedience and internalised discipline.

Furthermore, resistant Independents are a form of soft refusal or counter-conduct that resists normalization.

Together, these typologies provide a working theory for interpreting how subjects are differently positioned within regimes of digital power-some in alignment, some in resistance, all in movement through frameworks that circumscribe risk, trust, safety, and visibility in the digital sphere.

Social Implications

Our studies have shown that people often modify their behaviour in the presence of surveillance (both in the digital space and in real time), either out of fear of judgment or a desire to conform to the accepted social expectations, principles, procedures, and regulations. We believe that this shift has broader implications for the society at large, especially as emerging surveillance technologies become more and more integrated into our lives. Thus, in case users become much more aware of the used platforms' surveillance and exhibit a much self-aware and socially aware demeanour, they will resultantly become much more responsible citizens of this planet Earth. Moreover, the user-platform interactions will eventually become more controlled, efficient, and productive. Furthermore, human-machine interactions will become more trustworthy and reliable by means of distinct regulations.

Conclusion

In summary, this study has explored the evolution of cybersecurity from a technical shield against digital threats into a powerful apparatus of governance, capable of shaping behavior, protecting human psychology, producing norms, and constructing digital subjectivity. Through the lens of Foucauldian theory-particularly his concepts of disciplinary power, surveillance, governmentality, and power/knowledge-we have demonstrated that cybersecurity systems do not merely secure environments; they classify, normalize, and subtly govern those who inhabit them.

Case studies including Pegasus spyware, social credit systems, and algorithmic governance in Big Tech reveal how cybersecurity technologies produce subjects who are monitored, evaluated, and responsibilized. These systems enforce conformity not through coercion, but through visibility, scoring, and behavioral feedback-embedding expectations into the digital infrastructures of our everyday life.

To validate these theoretical claims, we have conducted a behavioral and attitudinal survey, supported by PCA-based dimensionality reduction and K-Means clustering.

Thus, the empirical results revealed two distinct user typologies:

- Cautious Conformers-individuals who modify their behavior in response to surveillance and algorithmic pressure, adapting to remain visible and trusted within digital systems.
- Resistant Independents-users who report minimal behavioral change, resist platform expectations, and remain skeptical of classification and scoring systems.

These profiles reflect not only different relationships to cybersecurity governance, but also different forms of digital subjectivity. They confirm Foucault's assertion that modern power operates most effectively when it becomes internalized, working through norms, classifications, and invisible boundaries of acceptability.

At the same time, this study shows that users are not uniformly passive. Many express discomfort, skepticism, or opposition to these systems, particularly when transparency is lacking or when classification mechanisms are perceived as unfair. Thus, the desire for democratic oversight and independent control over cybersecurity infrastructures reflects a public awareness of the diffuse, decentralized nature of digital power, and a demand for ethical accountability.

Given these findings, this paper concludes with several key imperatives:

- Cybersecurity policies must be re-evaluated to include transparency, auditability, and mechanisms for contesting classifications and scores. Ethical governance must accompany technical advancement.
- Designers and developers must recognize that every decision-about what is tracked, how behavior is scored, or which actions are promoted-is a political act. These systems shape the digital self, and they must be built with critical awareness of their normative consequences.

Thereinafter, we strongly believe that future research should expand upon this interdisciplinary approach, combining philosophy, psychology, data science, and empirical user studies to trace how digital subjectivity is governed and produced. Larger-

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

scale, cross- cultural, socially aware, and longitudinal studies could offer even deeper insights into the ways power operates-and is negotiated-in digital life scopes.

In sum, cybersecurity is no longer only about preventing harm. It is about determining who belongs, who is trusted, and how one must behave to remain legitimate and visible in the digital sphere. As such, it requires not only innovation, but reflection, not only protection, but accountability, and not only code-but critique of thought, that will greatly enhance, regulate, protect, and secure proper user experiences.

Recommendations

It has been revealed through our study that many individuals can modify their behavior in accordance to their awareness of surveillance, both in the digital space and in their everyday lives (both in their private life and the business spheres). We strongly believe that raising the awareness of surveillance in the digital place too and explaining its advantages and shortcomings to the users will open up space for them to function accordingly. Thus, we believe that the present study opens up space for further research and study in the field, making user-platform interactions regulated, safe, secure, efficient, and productive.

Acknowledgement

We thank the participants in the survey.

Funding Support

There has been no external funding acquired for this research.

Ethical Statement

The anonymity of the participants in the survey has been ensured.

Conflicts of Interest

The authors of this article herewith declare no conflicts of interest.

Data Availability Statement

The results of the survey can be presented upon request.

Authors' Contribution Statement

Loubna Ali1: conceptualization, theoretical framework, methodology design, empirical survey implementation, data analysis using PCA and K-means clustering, original draft writing, and visualizations. Anna Rostomyan2: writing draft's revision, proofreading & editing, assistance in the survey, working on the psycho-emotional-social analysis of cybersecurity, correspondence with the editorial. Ali Ali[3]: data collecting and analysis, reviewing the draft.

Dr. Loubna Ali is an Associate Professor in Computer Science and Informatics, holding both a Ph.D. and a Master's degree from INSA- Lyon, France. Her areas of expertise include artificial intelligence, machine learning, information systems, and cybersecurity. She has extensive experience in teaching and supervising international graduate students and has published numerous papers in national and international journals and conferences. Dr. Ali is committed to fostering a dynamic learning environment that encourages critical thinking, scientific curiosity, and innovation.

Dr. Anna Rostomyan is an Assistant Professor, international author, researcher, editor, reviewer, speaker, translator, and certified EI coach. As a world-renowned author and scholar of 7 books and about 100 publications worldwide, she reaches a readership of around 100 nationalities. She received her PhD degree with the highest grade in 2013 in cooperation between Yerevan State University (Armenia - her alma mater) and the University of Fribourg (Switzerland) within the framework of a scientific PhD research grant funding of excellence.

Her main work focuses on the linguo-cognitive analysis of emotions and their impact on our everyday life, as well as in the business sectors.

Eng. Ali Ali serves as the Assistant Secretary-General of ARISPA and Chairs its Cybersecurity Committee. He holds an Executive Master's degree in Information Society Management and a Bachelor's degree in Electronics Engineering. Mr. Ali is the Founder and General Manager of Quanty for Smart Applications and brings over eight years of experience as an information security instructor at private universities.

His expertise encompasses cybersecurity policy development, strategic information governance, and the application of smart technologies. He is committed to advancing robust cyber frameworks, fostering innovation ecosystems, and promoting secure digital transformation through both industry practice and academic development.

References

1. Zuboff S (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs.
2. Lyon D (2001) Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press.
3. Poster M (1990) The Mode of Information: Poststructuralism and Social Context. Chicago: University of Chicago Press.
4. Haggerty KD, Ericson RV (2000) The Surveillant Assemblage. Br J Sociol 51(4): 605-622.
5. Boyle J (1997) Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors. University of Cincinnati Law Review 66: 177-205.
6. Askari MU, Sheikh N (2021) Foucauldian Panopticon: A Model for U.S. Cyber Surveillance. Journal of Political Studies 28(1): 193-211.

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698

7. Lysova T (2022) Video Surveillance and Public Space: Surveillance Society Vs. Security State. In Security and Safety in the Era of Global Risks pp. 245-260.

8. Joranger L (2025) Foucault's Social, Community, and Cultural Psychology. Integr Psychol Behav Sci 59(1):17.

9. Foucault M (1954) Maladie Mentale et Personnalité. Paris: Presses Universitaires de France.

10. Foucault M (1977) Discipline and Punish: The Birth of the Prison. New York: Pantheon Books.

11. Foucault M (1980) Power/Knowledge: Selected Interviews and Other Writings, 1972-1977 (C Gordon Ed) New York: Pantheon Books.

12. Foucault M (1991) Governmentality. In Burchell G, Gordon C, Miller P (Eds.), The Foucault Effect: Studies in Governmentality Chicago: University of Chicago Press pp. 87-104.

13. Amnesty International & Forbidden Stories (2021) The Pegasus Project.

14. Creemers R (2018) China's Social Credit System: An Evolving Practice of Control. SSRN Electronic Journal.

15. Dai X (2018) Toward a Reputation State: The Social Credit System Project of China. SSRN Electronic Journal.

DOI: 10.19080/RAEJ.2025.06.555698

How to cite this article: Loubna Ali, Anna Rostomyan, Ali A. Cybersecurity through the Lens of Foucault's Theory of Power and Knowledge. Robot Autom Eng J. 2025; 6(5): 555698. DOI: 10.19080/RAEJ.2025.06.555698