University of Saida Dr. Moulay Tahar

Faculty of Law and Political Sciences

Department of Public Law

The Society of Control between National Security Imperatives and Individual Freedoms violations: A Case Study of China

Thesis submitted in partial Fulfillment of the Requirements For the Master

Degree in Political Sciences

Specialization: International Relations

Presented by   **Supervised by**

Fatima Zohra Mekkaoui   Dr Ali Elottri

Board of Examiners

Pr. A Chikhaoui	University of Saida Dr. Moulay Tahar	President
Dr. A Elottri	University of Saida Dr. Moulay Tahar	Supervisor
Dr. K Hadj Djelloul	University of Saida Dr. Moulay Tahar	Examiner

Academic Year: 2024/2025

University of Saida Dr. Moulay Tahar

Faculty of Law and Political Sciences

Department of Public Law

The Society of Control between National Security Imperatives and Individual Freedoms violations:
A Case Study of China

Thesis submitted in partial Fulfillment of the Requirements For the Master

Degree in Political Sciences

Specialization: International Relations

Presented by   **Supervised by**

Fatima Zohra Mekkaoui   Dr Ali Elottri

Board of Examiners

Pr. A Chikhaoui	University of Saida Dr. Moulay Tahar	President
Dr. A Elottri	University of Saida Dr. Moulay Tahar	Supervisor
Dr. K Hadj Djelloul	University of Saida Dr. Moulay Tahar	Examiner

Academic Year: 2024/2025

dedication

To my late father **Abdelkrim**, whose love, values, and silent strength continue to guide me every day, without him, I would not be who I am.

To my beloved mother **Samira**, whose unwavering support and boundless love are the foundation of my being.

To my second parents **Ali** and **Habiba**, whose presence in my life has been a beautiful gift of care, warmth, and wisdom.

To my cherished brothers **Fethi**, **Fouad** and **Sofiane** your loyalty and strength are my unseen shield.

To my dear sisters **Manar**, **Randa** and **Sabrina** your love is my safe haven.

To my precious nephew **Abdelkrim** who brings joy and hope with his smile.

To my beautiful nieces, **Assinette**, **Manissa** and **Aline** your light brightens our lives.

And to my brother's wife, **Nadira** thank you for being an integral part of our family, both in heart and in soul.

And to my fellow classmates, with whom I shared knowledge, laughter, challenges, and memories, thank you for walking this path with me.

With all my love,
This work is for you.

Acknowledgements

List of Abbreviations

AI   Artificial Intelligence

CCTV   Closed-Circuit Television

FBI   Federal Bureau of Investigation

IJOP   Integrated Joint Operations Platform

iOS   iPhone Operating System

NSA   National Security Agency

PRISM Planning Tool for Resource Integration, Synchronization, and Management

UK   United Kingdom

UN   United Nations

USA   United States of America

Introduction

Introduction

In recent decades, the world has witnessed unprecedented technological developments that have changed the features of daily life and reshaped the relationship between the individual and the nation state. Whereas political systems were previously limited to traditional tools to ensure security, such as security agencies and official institutions that seek to achieve discipline in society, a new phase known as 'societies of control' has emerged as one of the most prominent phenomena that characterize the digital age, as the technological boom has enhanced state's abilities to track and monitor individual's daily movements and activities, using advanced tools such as smart cameras, artificial intelligence, and big data analytics. Governments are able to collect vast amounts of personal information that is often used to enhance security and combat all kinds of threats.

These shifts are part of a historical process that began with disciplinary societies that relied on spatial and institutionalized control such as prisons and schools and moved to a more complex and comprehensive model, where digital control systems permeate all aspects of life, from public spaces to cyberspace. It has become an integral part of the security architecture of states. While these tools have greatly improved the effectiveness of security efforts, they have also raised serious concerns about their impact on individual freedoms.

In this context, China is one of the world's most prominent examples of mass control policies. It emerges as an interesting model, relying extensively on technology to ensure security and political and society of control. The Chinese government applies a vast control network that includes hundreds of millions of

cameras equipped with facial recognition technologies, as well as internet and social media monitoring to track individuals and analyze their behavior. This is to promote internal stability and ensure compliance with the government. However, despite all these developments that provide guarantees for security, they also raise many concerns about violation of privacy and restriction of personal freedoms.

Importance of the study The importance of this topic is to provide a comprehensive vision on how to balance the requirements of security and respect for individual freedoms in light of the development of control technologies, especially with the escalating use of artificial intelligence in the world and its impact on daily life. This study also sheds light on the Chinese model, which is considered one of the most advanced and widely used models of control technologies.

It is also a qualitative study that adds to the debates on control, security and individual freedoms.

Objectives of the study The main objective of this study is to understand and analyze the dialectical relationship between security requirements and the violation of individual freedoms in the context of societies of control with a focus on the Chinese experience as a model:

- Exploring how technology affects society.

- Providing conclusions and recommendations for balancing security requirements and respecting individual freedoms.

Reasons for choosing the topic

Subjective reasons: There are several reasons for choosing this topic, which were dictated by the nature of the specialisation in the first place, which generated the desire to discuss this topic, allowing the reseacher to link between contemporary issues and their applications in international politics, as well as her passion for technology, that pushes the researcher to explore how it can be

exploited in achieving public security.

Objective Reasons: In addition to the subjective reasons, there are objective ones for choosing this topic, such as the novelty of the topic and the increasing use of control technology in the world, raising questions about it and its implications on individual freedoms. China was chosen as a model because it is a prominent example of comprehensive control applications.

Limitation of the study

- Timeframe: Undetermined, but around the time China experienced a surge in control technologies.

- Spatial framework: The study focuses on China as a model of a control society.

- Thematic Framework: This study focuses on highlighting the relationship between achieving security and violating individual freedoms in the context of a society of control.

Exploratory studies:

1. Foucault's Theoretical Perspective: Michel Foucault: "Discipline and Punish: The Birth of the Prison" (1975). Focus: Introduces the concept of Panopticism as a metaphor for modern control, analyzing how power operates through observation and control. Relevance: Provides the theoretical foundation for understanding surveillance as a form of social discipline in a case study on China.

2. The Concept of Control Societies: Gilles Deleuze: "Postscript on the Societies of Control" (1992). Focus: Examines the transition from disciplinary societies to control societies, where control is pervasive and digital technologies play a central role. Relevance: Links the evolution of control technologies to modern practices in China.

3. Surveillance Capitalism: Shoshana Zuboff: "The Age of Surveillance Capitalism" (2019). Focus: Explores how digital platforms use personal

data for profit and control, often at the expense of privacy. Relevance: Highlights the intersection of technology, economy, and control practices.

4. Surveillance Systems in China:Qiang, Xiao: "The Road to Digital Unfreedom: President Xi's Surveillance State" (2019). Focus: Analyzes how China uses artificial intelligence, facial recognition, and big data to monitor its citizens. Relevance: Directly addresses case study, providing empirical data on China's control system.

5. Ethical Implications of AI in Surveillance: Xu, Qiang and Lin, Li: "The Role of AI in China's Surveillance System" (2020). Focus: Explores how artificial intelligence enhances China's ability to monitor and control its population. Relevance: Investigates the ethical dilemmas surrounding AI-driven control

6. Human Rights and Surveillance: David Lyon: "Surveillance Studies: An Overview" (2007). Focus: A comprehensive introduction to control control studies, discussing its implications for human rights Relevance: Establishes the broader context for the impact of control on individual freedoms.

7. Panopticism Revisited: Jeremy Bentham: "The Panopticon Writings" (1787). Focus: The original idea of a control mechanism designed to enforce discipline. Relevance: Serves as the historical foundation for theoretical framework.

Research Question In relation to our topic, and in light of the rapid technological developments that the world is witnessing, control societies have become one of the most prominent features that reflect the use of surveillance technologies to achieve security. Surveillance societies have become one of the most prominent features that reflect the use of surveillance technologies to achieve security by relying on tools such as artificial intelligence, surveillance cameras, facial recognition systems, etc. However, these practices have led

to widespread controversy related to individual freedoms, with the Chinese model being the most advanced and controversial. This leads us to discuss the following question:

How effective is the society of control in ensuring national security amid concerns over violations of individual freedoms?

In order to answer this question, we have to deconstruct it into a set of related questions:

1. What is the concept of a society of control and how has it evolved in line with technological development?

2. What are the justifications for the use of the society of control to achieve security?

3. What is the effect of the society of control on the individual freedoms?

4. To what extent can the Chinese model be evaluated in its use of the society of control to achieve security on the one hand and its impact on individual freedoms on the other one?

5. How can security be balanced with respect for individual freedoms in a society of control?

Hypotheses: To achieve the goals of the study, a set of hypotheses can be suggested:

1. The society of control presents an inevitable dilemma: while it is essential for achieving national security, it often leads to the restriction and violation of individual freedoms.

2. Governments tend to justify the use of surveillance and control technologies as necessary tools to ensure national security and combat threats such as terrorism and crime.

3. Balancing security and respect for individual freedoms in a society of con- trol remains a complex challenge that requires a transparent legal system, unbiased surveillance technologies, and ethical principles that respect human rights.

4. In the case of China, the state employs advanced technologies particularly artificial intelligence and facial recognition systemsŮto reinforce control mechanisms, which significantly impact and undermine individual freedoms.

Methodological framework: This study relied on a number of research approaches

- Historical method: studies the evolution of the concept of society of control, especially in light of technological advances from the past to the present.

- The case study method: used to study the Chinese model of control by knowing how to apply advanced surveillance technologies such as artificial intelligence and facial recognition, for example, and their effects.

- The descriptive-analytical method: used to describe the control system in China and provide accurate analyses of the phenomenon of the surveillance society by collecting information related to the Chinese model and analysing its dimensions and effects.

The theoretical framework of the study: This study draws on three main theories that provide a comprehensive understanding of the complex relationship between security, individual freedoms, and surveillance: Realist theory, liberal theory, and postmodernism (particularly Michel Foucault's analysis). It also draws on the Paris School of Security Studies, which interprets security as a political discourse used for authoritarian purposes.

- **Realism** is one of the strongest theories of international relations. It starts with the state as a key actor in the global system and tries to achieve

national security as a matter of survival, even at the cost of restricting freedom or applying coercive tools in an attempt to achieve internal and external stability. For classical realist theorists such as Hans Morgenthau[1], security power in the sense of survival is a central goal of the state and the citizen is seen as a component of a larger system subject to strategic considerations. The theory is then used here to illustrate the ways in which the state legitimizes a high level of surveillance policies in the interest of maintaining stability and state sovereignty.[2]

Since realism focuses on the state and its national security, the latter is often considered an end that justifies all sorts of means used to achieve it, even if these means violate essential human rights.

- **Liberalism** this theory based on the individual and his inalienable rights such as freedom of speech, privacy, and freedom of movement. It argues that security is not complete unless freedom is assured, and freedom is an inviolable value, which makes extreme censorship perilous for democracy. Liberal theorists, such as John Stuart Mill, believe that the freedom of the individual begins only when the freedom of other individuals begins, reflecting the liberal concept of "human security" which transcends the military dimension to human dignity safeguard. Liberalism is employed here as a conceptual device to trace the negative effect of surveillance on human liberty, and the pressure to exchange freedom for security in totalitarian regimes[3].

Since liberalism focuses on individual freedoms and the rule of law, it considers the protection of these liberties a fundamental priority that must not be compromised, even in the face of security threats. This approach is well expressed by the American thinker Benjamin Franklin,

---

[1] Morgenthau, Hans J. Politics Among Nations: The Struggle for Power and Peace. New York: Knopf, 1948.

[2] Buzan, Barry. People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. ECPR Press, 2008.

[3] Rawls, John. Political Liberalism. Columbia University Press, 1993

who stated: "Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety." From this perspective, liberalism rejects the idea of sacrificing basic rights in exchange for temporary security, viewing such trade-offs as both morally and politically unacceptable.

- **The Paris School** is a critical perspective on how discourses on security are framed. Scholars like Didier Bigot build their work around the concept of policing and the idea of "control" and how everyday surveillance, especially against vulnerable individuals and migrants, are not just methods used to keep the individual safe, but practices that constitute a chronic state of insecurity. This focus serves the research well in that it explains how Chinese surveillance technology is transformed into tools of political and social control, rather than security. [1]

- **Postmodernism** is about power and knowledge and how the state uses control devices to produce obedience and discipline through gentle ways like classification, examination, and judgment that reform people according to the standards of the regime. Foucault does not view power as merely a force of repression, but rather as an ensembly of relations which simultaneously produces and distributes knowledge and control. The Panopticon and the Surveillance Society are also central to the analysis within this study because they illustrate that the individual is under surveillance even in ignorance, leading to self-control. In China, they are put into practice through social credit systems which monitor behavior and reward or deny privileges based on 'political and social conformity'.[2]

   Conceptual framework of the study:

- **National Security** is the ability of a state to protect its core interests, borders, and citizens from both internal and external threats, and is a central

---

[1] Bigo, Didier. "Security and Immigration." Alternatives: Global, Local, Political, 2002.
[2] Foucault, Michel. Discipline and Punish: The Birth of the Prison. Vintage Books, 1977

concept in the realist literature.[1]

- **Disciplinary Society** is a term used by Foucault to describe societies that control behavior by employing institutions such as schools, hospitals, and prisons to enforce authority in the form of organized systems of punishment and surveillance. The term is used to describe the traditional mode of surveillance before the age of technology (the prison-school model).[2]

- **Society of Control** is a society in which individuals are constantly monitored using digital tools such as cameras, cell phones, and artificial intelligence. This concept is the backbone of the Chinese model, where technology has become a tool for the ubiquitous surveillance of political and social behavior.[3]

- **Panopticon** A term developed by Jeremy Bentham and elaborated by Foucault, it is an architectural design of a prison that allows all prisoners to be monitored from one location without the possibility of any of them knowing if and when they are being monitored. This concept describes the way in which the Chinese state allows for constant self-control of the citizen.[4]

- **Individual freedoms** are the rights granted to every human being as a free agent, including freedom of thought, movement, expression, and privacy, which are protected by international law. These freedoms are the analytical focus of the study, which assesses the extent to which they are violated under Chinese control.[5]

- **Artificial intelligence** is the ability of machines to mimic human thinking through learning, processing, and decision-making. It is currently part of

---

[1]Buzan, Barry. People, States and Fear. op. cit., p. 19
[2]Foucault, Michel. Surveiller et punir: Naissance de la prison. Gallimard, 1975.
[3]Deleuze, Gilles. "Postscript on the Societies of Control." October, 1992.
[4]Bentham, Jeremy. The Panopticon Writings. Verso, 1995.
[5]Mill, John Stuart. On Liberty. Penguin Books, 1859.

surveillance technology, and is already being used in China for security reasons by processing data, recognizing faces and predicting behavior. This has led to a system like social credit, which rates citizens based on their political and behavioral standing.[1]

- **Surveillance versus Control**

Surveillance is the process of watching individuals and tracking their movements and actions using various devices expressly aimed at ensuring social order, deterring crime, and safeguarding national security. The practice follows a centralized and hierarchical pattern where authoritative entities gather personal information using cameras, electronic devices, and computer systems to keep individuals under constant watch.

In contrast, the mechanism of control goes beyond this traditional dimension; it is not limited to monitoring actions, but aims to shape and direct behavior in advance. This concept was developed by philosopher Gilles Deleuze in his discussion of societies of control, where power uses hidden tools such as algorithms, artificial intelligence, and big data to reproduce behavior ac- cording to preconceived digital models, as is evident in the Chinese model through the social credit system and the Great Firewall.

Difficulties of the study: The main difficulties faced by this study are

- New initiatives often encounter setbacks at the very beginning of the experience.

- As a new experience in the Algeria Universities, especially in the field of political science, the student faced several difficulties and obstacles, including language barriers, methodological challenges, and a relative lack of available literature.

- The difficulty of accessing accurate data and information about control

---

[1]Zuboff, Shoshana. The Age of Surveillance Capitalism. PublicAffairs, 2019.

con- trol systems in China due to government restrictions surrounding the topic.

- The technological complexity that may cause a challenge in analysing the technological dimensions in depth.

Introducing the study: In addition to the introduction, which clarifies the study question and the conclusion, which contains the main findings, this study is divided into three chapters as follows:

Chapter One: This chapter deals with the theoretical foundations of the study. In the first section, it introduces the concept of security and its various traditional and modern theories. In addition to national security, in the second section, the surveillance society and the policing society, as well as the concept of the term panopticon, and in the third section, it addresses individual freedoms.

Chapter two: The second chapter explores the core dilemma between the imperative of achieving national security and the preservation of individual freedoms in the age of expanding surveillance systems. It aims to dissect this complex tension through a structured analytical approach, divided into three interrelated sections.

The first section is devoted to examining the positive aspects of the surveillance society in achieving security, analyzing how modern monitoring technologies have enabled states to respond to threats more efficiently, enhance public order, and prevent crime through proactive mechanisms.

The second section highlights the fears and challenges associated with the surveillance societyŠs impact on individual freedoms. It addresses the erosion of fundamental rights, the politicization and misuse of surveillance tools, as well as the psychological and social repercussions of constant monitoring. These issues are further analyzed through the lens of Nash Equilibrium Theory,

which offers insight into disciplinary behavior under uncertainty.

The third section investigates the potential for balancing national security and individual freedoms, presenting ethical principles, legal frameworks, and international models that seek to preserve democratic values and human dignity while addressing security needs.

Chapter three: The third chapter is devoted to analyzing and studying the Chinese model, in three sections: the first presents the Chinese perspective on security and the historical background of the surveillance society, the second deals with the tools of control and mechanisms of social control. The third the implications of the Chinese control system on security and individual freedoms.

Finally, the conclusion to verify the hypotheses and answer the problematic.

Chapter 1: Theoretical and Conceptual Framework

Partial Introduction

The theoretical framework is one of the key elements in any academic study, as it contributes to defining the basic concepts and analysing them according to different intellectual approaches, which helps in building an integrated understanding of the research topic. In the context of this study, which deals with the relationship between the surveillance society and national security and its impact on individual freedoms, it becomes necessary to analyze the basic concepts underlying this topic, starting from the concept of security and the evolution of its approaches, to the major transformations that modern society has witnessed from a society of discipline to a society of surveillance, and the impact of these transformations on rights and freedoms.

This chapter deals with three main discussions: The first is the concept of security, where we present some different definitions of the term and the evolution of its approaches, with a focus on different theoretical contributions, including realist, liberal, critical, and Paris School approaches to security. On the other hand, we talk about the concept of a society of discipline, which has evolved with the rise of modern technology and advanced security systems into a society of surveillance. Finally, the chapter discusses individual freedoms.

1.1 The Concept of Security and Security Approaches

The concept of security has been a major concern for thinkers and decision-makers alike, as ensuring survival, security and continuity is a priority for domestic and foreign policy, as it constitutes the cornerstone of the stability of states and societies. Despite its traditional association with protecting the state from external threats by focusing on military security issues and the

centrality of state security as the main reference point in security and national security analysis.

However, the evolution of political and security thinking and the emergence of new security threats have expanded its scope to include multiple dimensions, such as human security, environmental security, and cyber security. This section focuses on establishing the concept of security, by presenting its various definitions to arrive at a procedural definition adopted in this study. It then examines the security approaches presented by researchers, which reflect the evolution of security thought over time. Finally, the Paris School of Security will be highlighted, which contributed to providing a critical view of the traditional concept of security and linking it to the concepts of society of control and surveillance.

1.1.1 The Concept of Security

The concept of security is one of the most complex concepts in international relations, as its definitions vary depending on the angle from which it is viewed. The following are some of the definitions provided by scholars:

- Walter Lippmann defined security "A nation has security when it does not have to sacrifice its legitimate interests to avoid war and is able, if challenged, to maintain them by war."[1], Lippmann offers a traditional realist definition of security, linking it to military power and the ability to defend national interests. This definition reflects traditional realism, as it links security to military power and the ability of the state to defend its core values without making concessions. It also emphasizes that security is not only the absence of war but also not sacrificing core values. This definition converges with the theory of deterrence, as security is only achieved when

---

[1] Walter Lippmann, U.S. Foreign Policy: Shield of the Republic, (Boston: Little, Brown and Co., 1943), p. 51.

the state is able to win any war that may be imposed on it, and this proposal is in line with the ideas of George Kennan and Hans Morgenthau about the necessity of assertiveness in foreign policy to avoid existential threats.

- Arnold Wolfers defined security

"Security, in an objective sense, measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values will be attacked."[1], Wolfers introduced the concept of dual security, distinguishing between the objective and subjective dimensions. Security is not only the absence of threats but also the subjective sense of security. This definition is in line with the constructivist approach to the study of security.

- John Herz defined security "Security dilemma arises when the efforts of one state to increase its security reduce the security of others."[2] Herzl focuses on the 'security dilemma' (mutual militarization between states). It is in line with constructivist realist theories that see the concept of security as linked to the balance of power.

- Robert McNamara defined security "Security is not military hardware, though it includes it. Security is not military force, though it encompasses it. Security is development, and without development, there can be no security."[3] McNamara presents a liberal-humanist vision of security, where security is not centered on military power alone but requires economic and social development to ensure stability. This definition is linked to the idea of human security that later emerged at the United Nations, where poverty, education, health, and basic rights are emphasized as elements of security. education, health, and basic rights as elements of security.

- Hedley Bull defined security "Security is the preservation of values and the

---

[1] Arnold Wolfers, "National Security as an Ambiguous Symbol", Political Science Quarterly, Vol. 67, No. 4 (1952), pp. 481-502.
[2] John H. Herz, International Politics in the Atomic Age, (New York: Columbia University Press, 1959), p. 230
[3] Robert McNamara, The Essence of Security,(New York: Harper and Row, 1968), p. 149.

protection of individuals, states, and the international system from external threats."[1]

- Henry Kissinger defined security "Security is any action taken by a state or society to ensure its right to survive."[2] One of the pioneers of the English School, Hedley Paul argues that security is not only about states, but also about individuals and the international system. This definition offers a broader conceptualisation of security than the traditional realist perspective.

- Richard Ullman defined security "Security is the ability of a state to maintain its territorial integrity and sovereignty."[3] Ullman defines security from the perspective of the nation-state, linking it to the integrity of borders and sovereignty, a definition that is in line with the realist school, which considers sovereignty and non-interference as the pillars of national security.

- Abdulwahab Kayyali defines security as follows "Security is securing the safety of a state from internal and external dangers that may lead it to fall under foreign control as a result of external pressures or internal collapse."[4] Kayyali defines security from a traditional realist perspective, focusing on protecting the state from internal and external threats. This definition is an extension of traditional security thinking that sees security as a matter of state sovereignty and stability.

- David Baldwin defined security "Security is protecting values from military, economic, or political threats."[5] Baldwin links security to the

---

[1] Hedley Bull, The Anarchical Society: A Study of Order in World Politics, (New York: Columbia University Press, 1977).

[2] Henry Kissinger, Diplomacy, (New York: Simon and Schuster, 1994), p. 832

[3] Richard H. Ullman, "Redefining Security", International Security, Vol. 8, No. 1 (1983), pp. 129-153.

[4] Kayyali, Abdul-Wahab. Zionism and Imperialism: The Historical Origins. Journal of Palestine Studies, Vol. 6, No. 3 (Spring 1977), pp. 98-112.

[5] David Baldwin, The Concept of Security, Review of International Studies, Vol. 23, No.1(1997), p. 5-26.

protection of national values against multiple threats (military, economic, and political). This definition reflects a multidimensional approach in line with liberal thought and modern theories of security.

- Barry Buzan defined security "Security is the pursuit of freedom from threats... It is the ability of states and societies to maintain their independent identity and their functional integrity against forces of change which they see as hostile."[1] Barry Buzan introduces the concept of expanded security, which goes beyond military security to political, economic, environmental, and societal dimensions. This definition is in line with the Copenhagen School, which argues that security is not limited to states, but also includes societies.

- Charles Kupchan defined security "Security does not simply mean the absence of war; it requires the stability of international relations."[2] Kupchan adds a new dimension to the concept of security, arguing that security does not only mean the absence of wars, but also requires stable international relations. This is in line with the liberal argument that international co-operation can reduce security threats.

- Ken Booth defined security "Security is the emancipation from threat; it is not just about state protection but the well-being of individuals."[3] Booth extends the concept of security to include individuals, reflecting a human security vision that focuses on protecting human beings and not just states. This definition is in line with critical theories of security that seek to redefine the concept of security away from the traditional focus on the state.

- Lene Hansen defined security "Security is about the construction of identity and the understanding of threats in a complex global environment."[4]

---

[1]Buzan, Barry. People, States and Fear. op. cit., p. 19.
[2]Charles Kupchan, The Vulnerability of Empire, (Ithaca: Cornell University Press, 1994).
[3]Ken Booth, Theory of World Security, (Cambridge: Cambridge University Press, 2007)
[4] Lene Hansen, Security as Practice: Discourse Analysis and the Bosnian War, (New York: Routledge, 2000).

Hansen adopts a constructivist approach, arguing that security is not just a military or political issue, but is also about how we construct identity and understand threats. This definition is an extension of constructivist theory that emphasises the role of discourse and identity in shaping security policies.

The previous definitions show that the concept of security evolves from a military perspective (Kissinger, Lippmann, and Kayyali) to a societal one (Buzan) and then to an economic perspective (McNamara). This evolution reflects the influence of historical contexts and theoretical backgrounds. Realism focuses on state-centered military security, while liberalism emphasizes human and economic security. In contrast, Barry Buzan introduces the concept of expanded security, which includes both societal and state security.

Security is a state and feeling that combines the objective and subjective dimensions, as it refers objectively to the absence of actual threats that may affect the basic values of the state and society such as survival, independence, territorial integrity, economic well-being, and fundamental rights and freedoms, and subjectively to the absence of fear and anxiety about the possibility of these threats occurring. Security includes the protection of individuals, communities, and states from internal and external threats, and goes beyond the military aspect to include political, economic, social, and psychological dimensions, ensuring stability and continuity in an environment that protects the entity and supports development and public safety.

1.1.2 National Security

National security is one of the main pillars on which the stability and continuity of states are based, as it represents the framework that protects its sovereignty, preserves the integrity of its territory, and secures the well-being

of its citizens. With the complexity of the international landscape and the emergence of new threats that include economic, social, environmental, and cyber dimensions, national security is no longer limited to military aspects but includes more comprehensive concepts that overlap with human security and sustainable development.

Many researchers have sought to provide accurate and comprehensive definitions of national security. These definitions have varied according to the perspective addressed, whether in terms of protecting the state from external threats or from a perspective that includes human security as an integral part of national stability. In this context, we will present a set of definitions provided by researchers on the concept of national security, which reflect its evolution and multidimensionality in light of modern challenges. Peterside defines national security as "the freedom from actual and potential threats to national life that may arise as a result of human actions or inactions, or from disaster such as flood, earthquake, famine, drought, disease and other natural calamitous events resulting in death, human suffering and material damage". Similarly, Onuoha, views national security as "the capacity of a state to promote the pursuit and realization of the fundamental needs and vital interest of man and society, and to protect them from threats which may be economic, social, environmental, political, military or epidemiological in nature". According to Okodolor, national security is "both qualitative and dynamic in nature.[1] In its qualitative sense, it encapsulates the unending drive of the state for improvement in the well-being of citizens as well as the protection of lives, property and resources belonging to the state. It is dynamic in the sense that, its broad contours change with the emergence of new threats or the transformation of old threats arising from within or outside its territory". Thus, as the economic,social, military, political, epidemiological and environmental causes of threats change so does the national security posture of a nation changes.[2]

---

[1]Ugo C. Okolie, "Distinction between Traditional Security and Modern Security: A Conceptual Discourse," Journal of Administrative Science 19, no. 2 (2022), p.252.

[2]Ugo C. Okolie, "Distinction between Traditional Security and Modern Security: A Conceptual

The emphasis on national security according to Orhero, stems from three fundamental convictions. That is, "the sanctity and inviolability of human life, the universality and dignity of human life and the existential imperative of the value of individual safety in a world full of multifarious threats". Therefore, national security is rooted in three basic instincts of self-preservation, self-extension and self-fulfillment. Also, given the qualitative and dynamic nature of national security, a country is secure to the extent that the ruling class is able to anticipate, recognize and respond effectively to the multifarious threats, leveraging the available national resources to ensure the safety of life and property of the citizenry and guarantee the integrity of its strategic assets and values, both within and outside its territory.[1]

National security can be defined as the state's ability to protect its sovereignty, territorial integrity, institutional stability, and the well-being of its citizens from internal and external threats, whether military, political, economic, social, cyber, or environmental. National security is achieved through comprehensive policies and strategies that include military defense, political stability, economic development, legal protection, intelligence security, and international cooperation.

National security is measured by various indicators such as political stability, military deterrence capability, economic and social security levels, the state's ability to adapt to crises, and the effectiveness of its institutions in addressing different threats. Achieving national security depends on balancing the protection of national interests with respect for individual rights and freedoms, ensuring sustainable security and long-term stability.

The concept of national security emerged with the development of the modern state, tracing back to the Peace of Westphalia (1648), which established the principles of state sovereignty. Over time, it has undergone significant changes based on prevailing political and military conditions."[2]

Discourse," Journal of Administrative Science 19, no. 2 (2022), p.252.

[1] Ibid, p.252

[2] Holsti, International Politics: A Framework for Analysis, 7th ed., p. 78, Prentice Hall

A The Classical Era (Pre-20th Century)

During this period, philosophers emphasised the role of the state in maintaining security and stability:

- Thomas Hobbes (1651): In Leviathan, he argued that a strong state is necessary to prevent the chaos that arises in the absence of authority.

- Immanuel Kant (1795): In Perpetual Peace, he advocated for an international order based on co-operation to prevent wars and promote collective security.

B The World Wars and Classical Security Era (1900-1945)

- During the two world wars, military power and strategic alliances were considered the primary means of achieving national security.

- The establishment of the United Nations in 1945 was a response to the need for collective security mechanisms to prevent future wars.

C The Cold War Era (1945-1991)

This period formed the framework and climate in which terms such as nuclear deterrence, containment, and peaceful coexistence emerged. These concepts played a pivotal role in defining the parameters of national security, especially between the United States and the Soviet Union.

D Post-Cold War and the Era of New Threats (1991 - Present)

- After the collapse of the Soviet Union, the nature of security threats evolved, with growing concerns over terrorism, cyber security, organized crime, and environmental security.

- The September 11, 2001 attacks marked a turning point, as non-traditional threats such as terrorism and asymmetric warfare became central to national security strategies.

- The concept of "human security" emerged, emphasizing the protection of individuals rather than just states, with a focus on direct threats such as poverty, famines, and armed conflicts.

1.1.3   Traditional Security Approaches

- Realism

Realism, in its classical form, is reflected in Thucydides' War of the Peloponnese (27 centuries ago), and in modern times, it has been followed by figures such as Klaus Weitz, Leopold Renk, and Frederick Mainck, with American scholars like Hans Morgenthau, Henry Kissinger, and George Kennan presenting and discussing realist theories. Realism has traditionally dominated international relations theory, viewing governments as the primary actors in international and regional systems, with national interests defined in terms of power. Governments are rational actors who seek to advance their national interests, respond to external threats, and exploit opportunities in international systems. The pursuit of power, including military strength and the defense of national interests, often leads to instability, particularly when one nation's security is achieved at the expense of others. Realists argue that foreign policy operates in an environment without a central authority, unlike domestic politics, which takes place in a more orderly system with central authority. From the beginning of the 20th century, realism emerged as the dominant paradigm, influencing theorizing efforts and explaining major events such as World War I and World War II through factors like the arms race, colonial competition, and the defense of national interests."[1]

Realism and Security

Realists emphasize that if a government cannot maintain its security, nothing else will be able to do so. In this regard, an efficient military force is essential to support diplomacy, foreign policy, and security. Compared to military capability, economic power plays a lesser role in national security. Proponents argue that historical experience shows that humans are inherently

---

[1]Ghavam, S. A. (2016).   "International Relations: Theories and Approaches".   Tehran: Organization for the Study and Compilation of Science Books Humanities Universities (Position), as cited in Ardam, Seyed Mohammad, Dehnavi, Ellias Aghili, Barzyan, Mohammad Ghanbari, and Parvaresh, Amir. (2021). "Security from the perspectives of realism, Copenhagen, liberalism with a little taste of technology". PJAEE, 18(6).

selfish and inefficient. Realists view the world community as chaotic and unchangeable, with gaining more power being the main motive for state actions to ensure national security. Their approach is based on the use of force and military power. Scholars such as Morgenthau, Kaplan, Kissinger, and Huntington define national security in these terms. According to realists, state security is central, and most threats are external and military in nature, targeting territorial integrity and national sovereignty. Recommendations for achieving national security include building military installations, striving for military superiority, and ultimately achieving military balance. During the Cold War, these strategies were deterrent for global superpowers. However, with the sudden end of the Cold War, realists faced an intellectual crisis, as their approach failed to predict the collapse of the Soviet Union. The dilemma of realist theory is its emphasis on military power balance and acceptance of the status quo, which did not foresee the rapid disintegration of international politics."[1]

Realists argue that absolute security is unattainable due to the anarchic nature of the international system. States are seen as rational actors, responsible for protecting their citizens by maximizing power in a dangerous world. Internally, security is ensured through legal systems and domestic authority. However, since no higher authority exists internationally, realists believe security can only be analyzed at the international level. Thus, national security is merely a component of international security.

The realist view of security is based on ontological foundations such as a negative perception of human nature and the central role of the state as the main level of analysis, and an anarchic international system influenced by national competition. Realists, with a pessimistic view of human behavior, raise the dilemma of security at both domestic and international levels. They consider domestic security essential in forming a unified national government.

At the international level, due to the anarchic nature of the global system

---

[1]Ibid

and the absence of a central authority, realists see the balance of power, military build-up, and the weakening of rivals as key strategies to achieve security.[1] Realists believe that insecurity is a natural characteristic of the international system, with insecurity dominating over security. They acknowledge that competition for security and the struggle for power are always present. They link insecurity to the accumulation of power within governments, making them capable of harming others in pursuit of limited interests. For realists, security is synonymous with survival, and governments are the primary source of security. They emphasize that government survival is the ultimate goal, and rely on the principle of "self-help," meaning that states cannot rely on guarantees from other governments for their survival.[2]

- **Liberalism**

Liberal Internationalism and Security Liberalism is the antithesis to realism with a focus on cooperation, rather than power competition to resolve conflict. Liberalists also draw upon a plethora of scholars, mostly from the Enlightenment, including Immanuel Kant, Baron de Montesquieu, Hugo Grotius, and John Locke. As a theory, there are quite a few variants and interpretations, including neoliberal institutionalism, economic liberalism (which focuses on market behavior), and democratic peace theory. Despite this variety, liberalism as a worldview has certain characteristics. For example, proponents of liberalism also view security as a key issue in global affairs. Though unlike realists, liberalists incorporate economic concerns, issues of development, and internal domestic situations. For liberalists, non-state actors are just as important as the states themselves. All actors are responsible for security, and it should not just be up to each individual state. Liberalists have

---

[1] Sotoudeh, A. S., and Sheikhoon, E. (2014). "A Comparative Study of the Security Approach of Islam with the Security Approach of Realism and Liberalism". Journal of Political Sociology of the Islamic World, 2(1), 5, as cited in Ardam, S. M., Aghili Dehnavi, E., Ghanbari Barzyan, M., and Parvaresh, A. (2021). "Security from the Perspectives of Realism, Copenhagen, Liberalism with a Little Taste of Technology". PalArchŠs Journal of Archaeology of Egypt / Egyptology, 18(6), 123-145.

[2] Ghavam, op. cit., p.81, as cited in Ardam, 2021, p.499

an optimistic view of human nature. They believe that war is not inevitable, but the product of a failure to compromise and cooperate.[1]

For liberalists, the promotion of global norms and values is important. States' interests are not limited to survival and security is not zero-sum. Security can be ensured through positive means and can be accomplished through transparency, communication, cooperation, and burden sharing. This reduces the need for armed conflict and instead can lead to expanded trade, which in turn can raise the costs of conflict, making it even less attractive. Cooperation is thus at the heart of liberalism. Liberalists do not suggest that competition will disappear, but that the relative gains from states cooperating are greater than the alternative. Ultimately, if such cooperation could become global, this could then lead to a system that ensures global peace. This is often referred to as collective security, an arrangement where an act of aggression against any individual state is regarded as aggression against all other states. In response, these states collaborate to collectively thwart and repel the aggressor.[2]

Given this, institution building becomes paramount. Referred to as neoliberal institutionalism, this branch of liberalism stresses the importance of international institutions and international law in shaping behavior as a better way to ensure the survival of the state. For liberalists the international system is still anarchical, but international organizations could help create a global framework of cooperation. Newer theorists, such as Robert O. Keohane and Joseph S. Nye define this cooperation in their idea of complex interdependence. This concept involves increasing interconnection among transnational actors and highlights the intricate dynamics wherein they develop mutual dependencies, become susceptible to each other's actions, and attuned to each other's needs.[3]

---

[1] Bozonelos, D., Lee, C., Thelen, A., Blanchard, L., Cauchon, S., Omae, M., Walker, E., and Ritt, T. (n.d.). 7.3 : Theories and approaches to global security. In Introduction to Global Studies. ASCCC Open Educational Resources Initiative. Retrieved April 6, 2025, from $https://socialsci.libretexts.org/Bookshelves/Geography_(Human)/Introduction_to_Global_studies_(OERI)/07$

[2] Ibid., 06 April 2025

[3] Ibid., 06 April 2025

International institutions play a key role in international politics and efforts. Examples include UN actions such as peacekeeping, peacebuilding and peace enforcement. It also involves the adoption of important international treaties and conventions that guide global behavior such as the United Nations Convention on the Law of the Sea, and the incorporation of the Laws of War. Other efforts include the development of international regimes, defined by Keohane (1984) as "sets of implicit or explicit principles, norms, rules and decisionŰmaking procedures around which actorsŠ expectations converge in a given area of international relations.Ť International regimes on arms proliferation and arms control have become an integral part of the global discourse.[1]

- **Marxism**

In Marxism, named after the scientist Karl Marx, conflict arises from the economy, especially the development of capitalism. Marxists argue that the industrialisation of society leads to the formation of two main economic classes: The bourgeoisie, a group of people who own the means of production, and the proletariat who provide the labour. This labour is exploited by the bourgeoisie and over time structures are built to maintain this exploitation. For Marx, these structures mask the intrinsic contradictions within capitalism, and increasing levels of inequality between the two classes will inevitably lead to conflict.

While this source of conflict arises internally, it can have global dimensions. For Vladimir Lenin, imperialism is a direct consequence of capitalism. Marx's theory of the excessive value of labour argues that workers do not really get what their labour is worth. With production costs fixed, over time, production owners suppress wages to increase profits as this is the only variable cost. This leads to less consumption at home and a surplus of products. Thus, countries look for new outlets for products through colonisation, where colonisers are required to buy them. Other

---

[1]Ibid., 06 April 2025

theories focus on the consequences of imperialism and colonisation after independence. Formerly colonised countries find themselves still dependent on their imperialist rulers, who dominate economic relations between the two parties, even decades after independence. This is called 'dependency theory', which is used to explain why some states, especially post-colonial states, remain in a state of underdevelopment and insecurity.[1]

1.1.4 Critical Security Approaches

Since the 1970s, scholars have worked on developing alternative IR explanation. These alternatives are not quite theories, but more broad perspectives. Given this, scholars have organized such approaches into two overarching categories: social constructivism and critical or radical perspectives. Constructivists focus significant attention on the role of identities in IR. Identities shape a state's interests and can influence the country's foreign policy goals, tactics, and strategies. Constructivists emphasize the relational aspects of identities, which are understood as the way one state views another state. This is shaped in important ways by the interactions that they have had and can create perceptions of similarities and differences between states. Thus, threats are socially constructed. For example, nationalism has led to the creation of conflicting identities and the right to self-determination has led to war. Constructivists challenge nearly all realist assumptions, particularly in that states must shape the international system. And so, constructivists would contend that anarchy is not the default understanding of international affairs and that there is no zero-sum world. Security then is how a state defines the system they live in. Thus, securitization is less about actual threats, but in naming someone or something, such as communism or terrorism, as a threat. How a state defines that threat is ultimately what could lead to conflict. Constructivists argue that the focus should be on tangible threats, such as those posed by

---

[1] Ibid., 06 April 2025

poverty and disenfranchisement.[1]

- **Postmodernism**

Postmodernism is one of the critical trends that emerged in the context of the end of the Cold War within the so-called post-positivist theories, which focused on the main goal of undermining the assumptions of the rational positivist trend. The pillars of postmodern thought have been summarized in 9 main points that can be summarized as follows:

- Undermining: By undermining the foundations of Western thought.

- Skepticism: By questioning the possibility of accessing certain knowledge.

- Nihilism: By being nihilistic and anarchic and not offering scientific and realistic alternatives.

- Disintegration and incoherence: The opposite of the logic of modernity; postmodernism calls for disagreement, disorganization, and the dismantling of what is organized.

- Deconstruction of the great centralized propositions: Especially those binaries on which Western thought is based, such as the signifier and the signified, presence and absence...

- Openness: Unlike modernist thought, postmodernism emphasizes openness as a means of interaction, understanding, and coexistence.

- The power of liberation: By liberating the individual from the oppression of social and political authority as well as the philosophy of the center.

- The transcendence of truth: By denying the idea that there is an absolute truth.

- The elimination of norms and rules: Michel Foucault emphasizes that a text or discourse has multiple meanings and readings, and therefore cannot

---
[1]Bozonelos et al., 2025

always rely on specific methodologies.[1]

Postmodernism redefines the concept of security as a critical discourse that moves beyond the realist conception of security as an objective, quantifiable condition. Postmodernism is based on the belief that security is not an objective reality "out there" but constructed through discourse. From this perspective, security measures are not just responses to external threats, but discursive measures which belong to the process of state identity construction in response to the "other" as a threat.[2]

In this context, postmodernism does not ask the question of "how do we achieve security? " but "how is security produced? " Who benefit from this production, and at whose expense it marginalizes or excludes?[3]

It is a process that draws out the discursive forces that produce fear and legitimize exceptional measures in the name of security. The state, far from having an unchanging and fundamental identity, constitutes itself through stories of danger, which create the figure of "us" and "the enemy.". Postmodernism argues that security discourses are not descriptive devices for defining reality, but instead meaning production mechanisms and instruments of constructing political reality itself.[4]

When the state defines something as a "threat," it does not so much represent it as it is, but constitutes it as a threat in a linguistic act with identity and political content. That is, security is a discursive and social construct employed to define who is the "self" and who is the "other," and the other is usually charged with a negative image justifying exclusion or violence against it.[5]

---

[1] mawsoua Post-modern theory in IR

[2] Edkins, J. and Vaughan-Williams, N. (2009). Critical Theorists and International Relations, in Baylis, J., Smith, S. and Owens, P. (Eds.), The Globalization of World Politics: An Introduction to International Relations, 4th ed., Oxford University Press, p. 131

[3] ibid, p.131

[4] ibid, p.134

[5] Ibid, p.132

This is possibly the greatest postmodernist contribution to the study of security, since it moves away from studying the "things" which are threatening security and studies instead the "discourses" through which these things become threats. Questions like: Who are articulating security? On behalf of whom? Whom are they excluding from this discourse? These questions identify that "security" is commonly evoked as a pretext to support extraordinary powers, especially during crises, emergencies, or international threats.This postmodern perspective heavily coincides with the power critique and knowledge, as it holds the opinion that security knowledge is not an objective notion but is dominated by hegemonic interests and power relations. Instead of being a protective device, security policies become a device for instilling fear, control, and remapping the political space according to the discourse power.[1]

- **The Copenhagen School**

The Copenhagen School of Security Studies is one of the prominent research programs at the Copenhagen Peace Research Institute in Denmark, founded in 1985. Two key scholars associated with this school are Barry Buzan and Ole Wæver, who developed a theoretical framework addressing the changes brought about by globalization in global security, particularly in the context of identity, cultural, and social security threats. The school builds on Buzan's hypotheses in his book People, States, and Fear, along with W?ver's ideas about the identity duality (Us/Them) and sovereignty. This framework responds to the conflicts caused by globalization and cultural intermingling between communities. The school also explores several new security concepts, such as "expanded security," "securitization," "societal security dilemma," and "regional security complex.[2]

Expanded Security: One of the concepts introduced by the Copenhagen School is "expanded security," which transcends the narrow traditional

---

[1]Ibid, p.134

[2]Buzan, B., and Wæver, O. (2003). Regions and Powers: The Structure of International Security. Cambridge University Press.

notion of security confined to military defense and force. According to the Copenhagen School, this concept includes various dimensions of security affecting individuals, communities, states, and the world as a whole, including military security, political security, economic security, societal security, and environmental security. This expansion of the security concept is a response to global challenges that go beyond direct military threats.[1]

Securitization Theory: Ole Wæver contributed to the development of the concept of "securitization," which refers to the process of transforming an issue or phenomenon from an ordinary matter into a security threat. This occurs through political or media discourse that redefines the phenomenon to become a security issue. Such phenomena can include political or social matters that were previously outside the realm of security concerns. Wæver shows how political elites can use discourse to label specific issues as security concerns in order to achieve political objectives, such as influencing public opinion or justifying extraordinary measures like declaring war or imposing a state of emergency.[2]

Societal Security: Societal security is one of the prominent topics in the Copenhagen School. This school focuses on security threats faced by communities without the state itself being threatened. In the post-Cold War era, it became evident that threats to cultural identity could impact the security of communities just as much as other threats affect the security of states. Wæver defines societal security as "the ability of a society to maintain its essential characteristics in the face of changes and potential threats". Societal security can be threatened either by the state itself or by other groups within the same state.[3]

Societal Security Dilemma: In the context of global chaos and the anarchic international system, the societal security dilemma is one of the key

---

[1] Buzan, B., Wæver, O., and de Wilde, J. (1998). Security: A New Framework for Analysis. Lynne Rienner Publishers.

[2] Wæver, O. (1995). "Securitization and Desecuritization." In On Security, edited by R. D. Lipschutz. Columbia University Press.

[3] Buzan, B. (2003). Regions and Powers: The Structure of International Security. Cambridge University Press.

concepts highlighted by the Copenhagen School. This dilemma refers to a situation of competition between groups within a state, where groups take it upon themselves to defend their identity in the absence of a central authority, leading to internal conflicts that may escalate into violence or even genocide, as seen in the former Yugoslavia. This competition shows that communities face not only threats from states but also from other groups within the same sovereign borders.[1]

Regional Security Complex: Barry Buzan and Ole Wæver focused on the concept of "regional security complex," which describes the interactions between states within a given region where all share common security concerns. This concept emphasizes that security cannot be confined to the borders of a single state; rather, it is heavily dependent on relationships with other states in the same region. This analysis involves four levels: the internal security of each state, the relationships between states within the region, relations between adjacent regions, and finally, the role of global powers in the region. This concept can be applied to various regions, such as the Middle East or the Maghreb. [2]

- **Paris School of Security**

The increasing security threats such as terrorism, organized crime, and illegal immigration have prompted deep reflection and efforts by politicians, academics, and security experts to find effective solutions to these security challenges, particularly in European countries. The works of the Paris School in the field of security studies represent an academic attempt to integrate various disciplines such as international relations, sociology, criminology, and law to address the security phenomenon in a comprehensive manner. The school relied on a constructivist approach to analyze security phenomena, focusing on security as a practice and technology exercised by security professionals, such

---

[1] Buzan, B. (2003). Regions and Powers. op. cit.

[2] Buzan, B., and Wæver, O. (2003). Regions and Powers: The Structure of International Security. Cambridge University Press.

as police and the military, rather than merely being a governmental strategy adopted by political authorities. Didier Bigo is considered one of the prominent researchers of this school. [1]

The Concept of Securitization in the Paris School: The Paris School approached the concept of securitization differently from the Copenhagen School. While the latter focused on securitization as a linguistic political discourse practiced by elites to turn various issues into security threats, the Paris School treated it as a routine and security practice, detached from political discourse. According to Didier Bigo, securitizing agents are not necessarily limited to political elites, but also include security professionals such as police officers and border guards, who interact daily with various issues that, through their practices, become securitized. [2]

The Concept of Policing: The Paris School specifically focused on the lower levels of security, or "security professionals," such as police officers and other security agencies, who are crucial to achieving and maintaining security, independent of governmental strategies. This importance is attributed to the fact that these agencies are directly exposed to security threats, which makes them more efficient and responsive in dealing with risks practically and quickly. [3]

The Concept of the Security Field: The security field refers to a transnational space formed through the integration and coordination of domestic and international security actors. The globalization and transnational threats have made it difficult to separate the internal environment of states from the external one, thus necessitating coordination between security professionals across countries. This coordination includes the exchange of intelligence and cooperation between security agencies at the international level, such

---

[1]Bigo, Didier. "Security and Immigration: Toward a Critique of the Governmentality of Unease." Alternatives: Global, Local, Political, 27(1), 63-92, 2002.

[2]Bigo, Didier. "Globalized (In)Security: The Field of the 'Professionals' of the Security-Security Nexus." International Political Sociology, 1(1), 1-13, 2008.

[3]Bigo, Didier. "When Two Become One: Internal and External Securitizations in Europe." In International Relations Theory and European Security, edited by M. P. G. Menon and J. R. M. Moïsi, 155-172, 2000.

as INTERPOL and Europol. According to Didier Bigo, the security field does not rely only on the use of force and coercion but also on the ability of security actors to gather and exchange information that shapes national security strategies. [1]

The Panopticon Model and Surveillance Societies: The French philosopher Michel Foucault adopted the idea of surveillance societies promoted by the state, based on the Panopticon model designed by the English philosopher Jeremy Bentham. The Panopticon is a geometric model for a prison that allows guards to monitor prisoners without the prisoners knowing whether they are being observed, creating an assumption of constant surveillance that induces continuous discipline. Foucault developed this idea into what he called "surveillance studies," aimed at achieving security and reducing the costs of continuous monitoring. Building on Bentham's Panopticon concept, sociologist David Lyon proposed the idea of the "electronic eye," where states use technology and install surveillance cameras in public spaces to achieve security and monitor behaviors. This allows the state to be present everywhere without physically being there, creating a constant sense of surveillance among individuals. [2]

- **The Aberystwyth School of Critical Security Studies**

The Aberystwyth School of Critical Security Studies is a research group within the Department of International Politics at Aberystwyth University in Wales (UK). It was founded by key scholars such as Ken Booth and Richard Wyn Jones. The school draws on the ideas of Robert Cox's critical theory in international relations, along with influences from the Frankfurt School and Antonio Gramsci's theory of hegemony.[3]

---

[1] Bigo, Didier. Security and Immigration. op. cit

[2] Lyon, David. Surveillance Society: Monitoring Everyday Life, Open University Press, 2001, pp. 78-80.

[3] Sezal, M. (2019). Origins of Differentiation in Critical Security Schools: A philosophic-genealogical search for emancipatory roots. [Thesis fully internal (DIV), University of Groningen]. University of Groningen, p. 76.

The school challenges the traditional, state-centric notion of security by arguing that security threats are not objective. Instead, they are the result of specific understandings that involve both the state and society. In criticizing the state-centered security perspective, the school posits that the state is not only the protector of individual security but, in many cases, the greatest threat to security. The school provides an analysis suggesting that the number of people killed by their own states during the 20th century exceeds those killed by foreign armies. [1]

Moreover, the school argues that the state is not capable of securing its citizens on its own. Daniel Bell proposed that after the Cold War, the state became "too small to deal with major problems (such as environmental disasters and pandemics), and too large to address minor issues (such as individual needs) effectively." [2]

The Aberystwyth School calls for a fundamental rethinking of security from the ground up. According to Ken Booth, the focus of security studies should be on individuals rather than states. He defines security as the condition of survival and considers it a "personal or collective struggle for survival." However, survival, in this context, is not just about physical existence but about living in a way that allows individuals to pursue their political, social, and economic ambitions. [3]

This perspective introduces the concept of "emancipation" as a necessary condition for achieving security. Emancipation, according to Booth, is the liberation from domination and oppression that prevents individuals from making free choices. It involves a rejection of conventional thought that reinforces negative views about human nature, such as selfishness, the logic of power, and state-centric thinking. [4]

---

[1] Ibid,p 77.
[2] Ibid,p 78.
[3] Booth, Ken. Theory of World Security, op. cit., p. 110.
[4] Booth,op.cit.,p. 150.

In addition, William Lovett defines emancipation as "the pursuit of human needs such as bread, freedom from poverty, liberation from ignorance, superstition, and lies, and the quest for justice, freedom from political despotism, and economic exploitation." This definition closely aligns with Maslow's hierarchy of human needs, which starts with basic physiological needs and progresses to self-esteem and the fulfillment of personal ambitions.[1]

Consequently, the Aberystwyth School maintains that individuals are the core subject of security. Unlike realism, which focuses on state security, or the Copenhagen School, which emphasizes the security of communities, Aberystwyth views individual emancipation as the ultimate goal of security. The state and community are seen as mere means to achieve this goal. [2]

1.2 The Disciplinary Society and the Society of Control

1.2.1 The Disciplinary Society

Beginning in the 18th century, Western societies witnessed a radical transformation in the concept and mechanisms of punishment. Punishment, once embodied in violent, public displays-such as executions in public squares, floggings, or the disfigurement of the body-served not only to penalize but to intimidate the masses and reaffirm the sovereign's absolute power. Over time, however, these practices gave way to more "subtle" yet far more effective methods of control, based not on physical torment but on surveillance and discipline. Modern power no longer needs to demonstrate its strength through the spectacle of mutilated bodies; instead, it seeks to reform individuals and manage their behavior through continuous and unseen mechanisms of observation. The prison exemplifies this shift: it is no longer merely a space of bodily confinement, but rather a highly calculated system designed to regulate time, train movement, and transform the condemned into self-regulating

---

[1]Lovett, William. 1834. "Political and Social Philosophy,p 10."

[2]Booth, Ken, and Wyn Jones, Richard. 2005. "Security and the Politics of Fear." University of Wales Press,p 200.

subjects. By organizing every detail of daily life-from sleep and wakefulness to eating and labor-power is exercised in an invisible yet totalizing manner, producing individuals who obey rules without the need for overt coercion. This historical shift, as analyzed by Michel Foucault, marks the emergence of a new form of power-one that conceals control behind the humanitarian façade of "rehabilitation"-and positions the prison as the model institution of a society governed by temporal efficiency and internal discipline. It is within this transformation that what Foucault would later call the "disciplinary society" begins to take shape."[1]

The concept of the disciplinary society, as developed by Michel Foucault, refers to a historical phase marked by the emergence of a new form of power that does not rely on direct repression or physical coercion, but rather on precise regulatory techniques aimed at shaping individuals within closed and organized institutions such as schools, prisons, hospitals, barracks, and factories. This organization is achieved through the division of time, control of space, surveillance of movement, and analysis of performance, all with the purpose of producing obedient, useful, and self-disciplined subjects. These institutions do not merely punish; they actively reconstruct the individual according to the norms of authority, making them governable, visible, and accountable. This shift represents a break from traditional societies rooted in sovereign authority, giving rise to a new mode of power exercised through subtle, continuous, and structured networks of surveillance and discipline.[2]

The fundamental concept of the disciplinary society is a system based on techniques of power aimed at organizing individuals. In such a system, individuals are shaped within closed spaces governed by strict regulatory laws and continuous mechanisms of surveillance. Foucault describes this system as a major shift from traditional societies, which relied on sovereignty and individual authority, toward societies that focus on organizing and controlling

---

[1] Foucault, Michel. Discipline and Punish, op. cit., pp. 3Ű20.

[2]Ibid., pp 3-20

individuals through specific institutions such as prisons, schools, and factories. This system seeks to make individuals more productive and disciplined by monitoring them and distributing them across these spaces, where their actions are subject to precise control.

The prison represents one of the most prominent manifestations of disciplinary power in modern societies. It is viewed not merely as a tool of punishment, but as an institution that produces compliance through careful surveillance and strict organization of individuals' lives. In this context, the prisoner becomes a constant subject of observation, with their movements measured and actions regulated within a confined space governed by precise time and spatial divisions. This system aims not just to punish the body but to reshape behavior and mold the individual to be more obedient and disciplined. Through imposed routines and daily repetition of activities, the prisoner learns obedience and self-regulation, making the prison a microcosm of how power functions in other institutions. Thus, the prison is not the end of the penal process, but rather the beginning of a process of "producing" a compliant and socially useful individual. This function is not confined to the prison itself, but extends to permeate the logic of authority throughout society.[1]

In modern society, control has become an essential part of daily life, aiming to regulate individuals and shape their behavior within organized spaces such as schools, hospitals, and factories.

- In schools, students are subjected to detailed monitoring intended to control their behavior and guide them according to specific standards. The school system sets study times, curricula, and even behavioral norms within the institution.

- In hospitals, patients are monitored to determine what is considered normal versus pathological based on strict medical systems, thus guiding and controlling their behavior indirectly.

---

[1]Ibid., pp. 3-20

- In factories, workers undergo precise surveillance through time management and productivity evaluation, aiming to increase output by monitoring and controlling their behavior to meet institutional goals.

In these institutions, power is not exercised through violence, but through the organization of time, the analysis of movements, and constant performance assessment, resulting in individuals practicing self-discipline. The prison is a miniature model of a larger society governed by the same mechanisms of control, where modern society becomes an extensive control system, exercised through interlocking networks of monitoring, often supported by technology, making every individual a potential target for observation and regulation without the need for direct supervision. Despite this widespread authority, Foucault argues that resistance remains possible against these systems of control.[1]

1.2.2 The Panopticon as a Model of Disciplinary Society

The idea of the Panopticon first appeared at the end of the 18th century with the English philosopher Jeremy Bentham, who introduced an architectural model for a prison based on the principle of permanent surveillance. The structure was designed as a circular building with cells arranged around a central watchtower, where an inspector could observe the inmates without being seen. This configuration prevented prisoners from knowing whether they were being watched at any given moment, thus generating a constant sense of being under control and leading them to regulate their own behavior without any direct intervention from the authorities.[2]

Bentham stressed that the invisibility of the observer created a condition of uncertainty that led to automatic discipline, as prisoners began to monitor themselves out of fear of unseen observation. David Lyon described this condition as the result of an "asymmetrical gaze" that produces "voluntary

---

[1] Ibid, p. 195-228.
[2] Bentham, Jeremy. The Panopticon Writings, op. cit., pp. 35Ű36.

submission"[1], a core element of what Michel Foucault later defined as the "automatic functioning of power".[2]

PANOPTICON PRISON

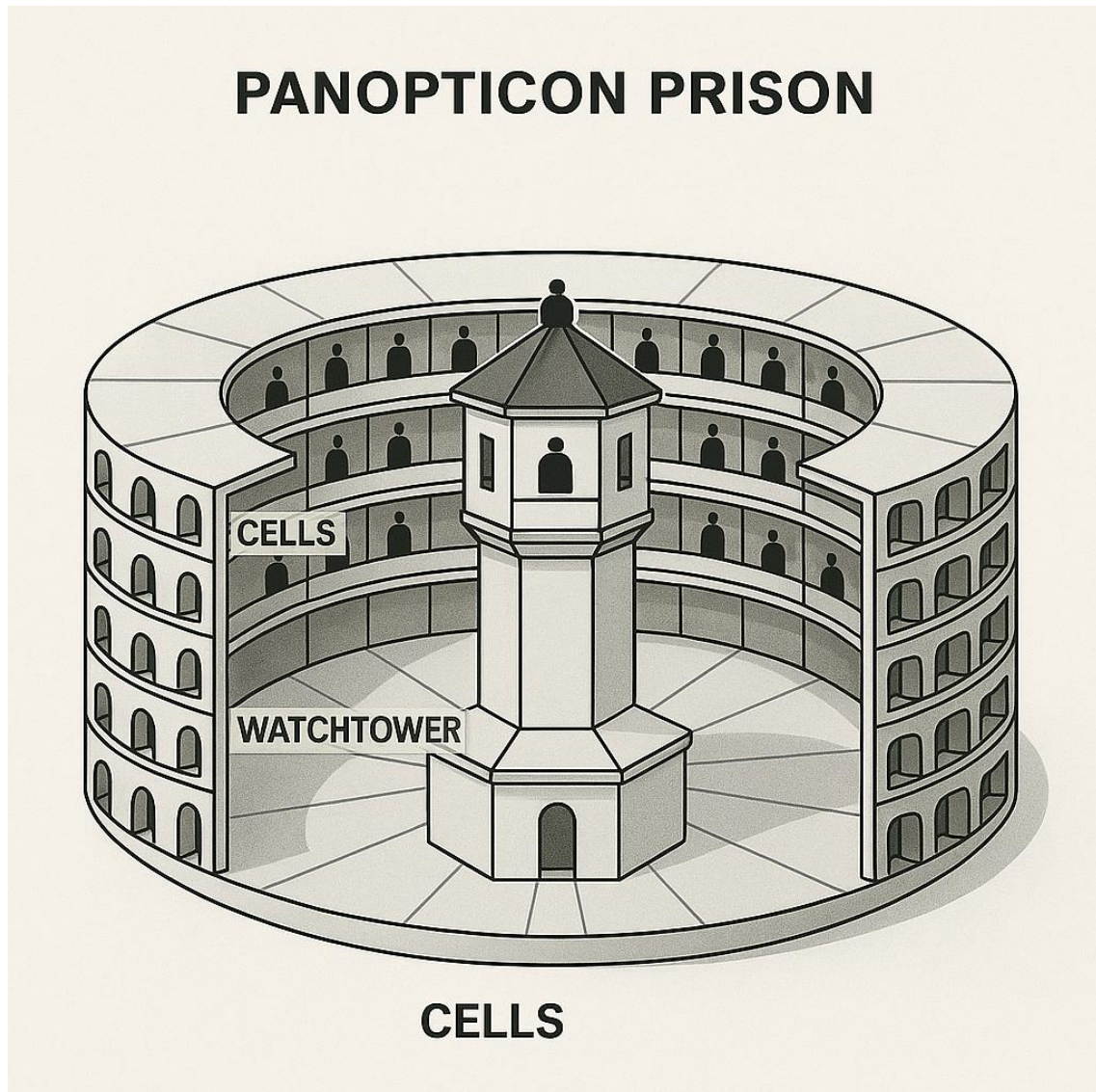CELLS

WATCHTOWER

CELLS

Figure 1.1: Panopticon: A visual embodiment of invisible power and self-censorship.

This image was created using ChatGPT at my request, presents an accurate visualization of the Panopticon Prison concept, created by the ChatGPT AI model based on detailed instructions I gave it regarding its structure and symbolism. The image features a central watchtower surrounded by concentric rows of prison cells, with each prisoner placed under the gaze of strategically placed potential observers. This architectural design embodies Jeremy

---

[1] Lyon, David. The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press, 1994, p. 65

[2] Foucault, Michel. Discipline and Punish, op. cit., p. 254.

Bentham's original vision of mass control, which was later reinterpreted by Michel Foucault as a metaphor for modern systems of power and social control. Although the prisoners cannot see the observer in the tower, the possibility of constant control forces them to regulate their behavior, a mechanism of internal discipline. The image goes beyond its physical design to represent a deeper political and psychological logic, where control becomes an internalized state. This visualization is even more relevant in today's digital age, where similar structures are reproduced through smart control technologies, biometric monitoring, and algorithmic tracking, placing individuals in a form of invisible panopticon where behavior is constantly monitored and shaped under the pretext of security or efficiency.

Bentham did not limit the Panopticon to prison design; rather, he proposed it as a universal model applicable to other institutions such as schools, hospitals, factories, and military barracks-places where organizing and monitoring people is essential. He believed this architectural concept could contribute to moral reform, public health improvement, productivity enhancement, and a reduction in social costs.[1]

Although the project had a utopian character, the Panopticon remained a theoretical design and was never implemented during Bentham's lifetime. The idea faded into obscurity until French philosopher Michel Foucault revived it in the 1970s, particularly in his seminal work Discipline and Punish, where he transformed the Panopticon from a physical model into an analytical framework for understanding modern power relations.[2]

Foucault argued that the Panopticon was not merely a building but a "political technology" that used visibility as a mechanism of control. It depersonalized authority and replaced sovereign power with spatial organization that compelled individuals to comply without the need for force.[3]

---

[1]Bentham, Jeremy. The Panopticon Writings, op. cit., p. 31.
[2]Foucault, Michel. Discipline and Punish, op. cit., p. 238
[3]Ibid., pp. 235Ű236

The strength of this model lies in its ability to subjugate individuals silently and preventively, making power more efficient and less costly.[1]

According to Foucault, the primary function of the Panopticon is to create a "new political anatomy" within society, in which control becomes internalized. Individuals, knowing they are being watched, behave in a disciplined manner even in the absence of direct coercion. Thus, power becomes less visible but more effective, producing obedient bodies through soft, nonviolent means.[2]

With the emergence of contemporary control studies, Foucauldian panopticism has been increasingly criticized, especially with the rise of digital technologies. Scholars pointed out that Foucault failed to account for the impact of computers, databases, and digital cameras, making his model inadequate for understanding control in the 21st century.[3]He was also critiqued for focusing too heavily on traditional institutions and overlooking the fact that modern control is exercised not only by the state but also by non-state actors.[4]

Consequently, many researchers have suggested that the Panopticon no longer reflects the nature of contemporary digital control, which is now decentralized and far more complex than the simple "gaze from above". A new post-Panoptic paradigm is needed to analyze the changing technological and social landscape.[5]

1.2.3 The Society of Control

Following Michel Foucault's identification of control as the central mechanism through which modern societies govern and regulate individual behavior, Gilles Deleuze introduces a new conceptual framework that moves

---

[1]Ibid., p. 240

[2]Ibid., p.243

[3] Haggerty, "Tear Down the Walls: On Demolishing the Panopticon", Theoretical Criminology, 2006, p. 32.

[4] Yesil, Bilge. "Modern Surveillance and the Panopticon". New Media and Society 11, no. 1Ű2 (2009), p 11

[5]Haggerty, Kevin D., op. cit., p. 24.

beyond disciplinary paradigms: the society of control. In this framework, Deleuze expands upon Foucault's insights by examining how contemporary technologies do not simply support disciplinary systems but transform control into a pervasive, structural element of daily life. Control, in this sense, ceases to be a localized or occasional practice and instead becomes continuous and integrated within digital and informational environments. Traditional disciplinary institutions such as the family, school, factory, prison, and hospital are undergoing a profound crisis, increasingly perceived as obsolete. Governmental reforms targeting these institutions often function merely as strategies to prolong their relevance or delay their dissolution, pending the full institutionalization of a new regime of power. According to Deleuze, contemporary society is witnessing the emergence of a novel form of authority wherein control is no longer exercised within closed, segmented environments but through open, flexible, and accelerated mechanisms. "Control" thus becomes the defining logic of the emerging social configuration.[1]

David Lyon, one of the leading scholars of control studies, defines the society of control as: "A society in which control is no longer the exception but the rule; it is embedded in everyday life through routine data collection and monitoring practices".[2]

Shoshana Zuboff extends the definition to include economic and behavioral dimensions: "Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data These data are used to predict and modify behavior to produce revenue and market control".[3]

For the purposes of this research, the society of control is defined as: "A sociopolitical environment structured around technological systems that continuously collect, analyze, and utilize personal data to monitor, predict,

---

[1] Deleuze, Gilles. "Postscript on the Societies of Control", op. cit., pp. 4-7
[2] Lyon, David. Surveillance Society, op. cit., p. 3.
[3] Zuboff, Shoshana. The Age of Surveillance Capitalism, op. cit., pp. 8-19.

and influence human behavior-often beyond the awareness of those being observed."

Gilles Deleuze argued that modern societies have moved from enclosed institutions toward "open systems" of control, where control operates through codes, access cards, and digital monitoring. As he puts it: "There is no need for enclosure anymore-control is exercised through tracking and modulation in open environments".[1]. According to Clive Norris and Gary Armstrong, control is no longer limited to state practices but is embedded in private and commercial sectors, making individuals visible and predictable in ways that were previously unimaginable: "Technologies of control now collect data on where we go, what we buy, who we communicate with, and what we say".[2]

According to Clive Northcote Parkinson, modern control does not merely record behavior but works to anticipate and influence it, using technologies such as artificial intelligence and predictive analytics. This renders individuals as "transparent bodies" before power, constantly exposed to observation and manipulation. "Surveillance is no longer content with seeing what is done; it seeks to know what will be done, and to shape it in advance".[3]

Key Characteristics of the control Society

- Permanence: control today is not episodic but continuous. It time, with no breaks, allowing authorities or corporations to monitor individuals at all times. This constant observation ensures that behaviors are captured and recorded as they unfold, making it nearly impossible for individuals to "escape" the gaze of control. The idea of being always watched has thus become ingrained in daily life.

  Example: The use of security cameras in public spaces or the constant tracking of online behavior.

---

[1] Deleuze, Gilles. "Postscript on the Societies of Control", op. cit., p. 4.
[2] Norris, Clive and Armstrong, Gary. The Maximum Surveillance Society: The Rise of CCTV, Oxford: Berg, 1999, p. 5.
[3] Parkinson, C. Northcote. The Law and the Profits. London: John Murray, 1957, p. 42

- Pervasiveness: control reaches all areas of life, not just limited to government oversight. It extends into private spaces, including homes, workplaces, and online environments. Corporations, for example, track consumer behaviors, while governments track citizens' movements, communications, and transactions.

  Example: Social media platforms collect data on user activity, and companies use that data for targeted ads or product recommendations.

- Predictive Analytics: Modern control does not only observe actions-it predicts future behaviors. Using algorithms, artificial intelligence, and machine learning, control tools can analyze patterns in data and anticipate actions before they happen. This gives authorities or corporations the ability to influence and even control behavior based on predictions.[1]

  Example: Predictive policing uses crime data to forecast where crimes might occur, allowing law enforcement to deploy resources preemptively.

- Normalization: As control becomes more pervasive, individuals begin to accept it as a natural and inevitable part of life. People no longer resist it but instead integrate it into their daily routines. This normalization makes it harder to critique or question the systems in place, as control becomes embedded in almost every aspect of daily life.[2]

  Example: People routinely share personal details online through social media, not seeing the potential risks of privacy invasion.

- Self-control: With the proliferation of smartphones and social media, individuals actively participate in their own control. They upload photos, share personal updates, and engage in self-reporting, often without thinking about the implications of these actions. This results in people continuously monitoring and sharing their own data, voluntarily making

---

[1] Sarah Brayne, Predict and Surveil: Data, Discretion, and the Future of Policing, Oxford University Press, 2020.

[2] David Lyon, Surveillance After Snowden, Polity Press, 2015

themselves more visible to both the state and corporations.[1]

Example: Posting personal experiences on platforms like Instagram or Facebook provides data that can be analyzed by companies for targeted marketing or even by governments for society of control.
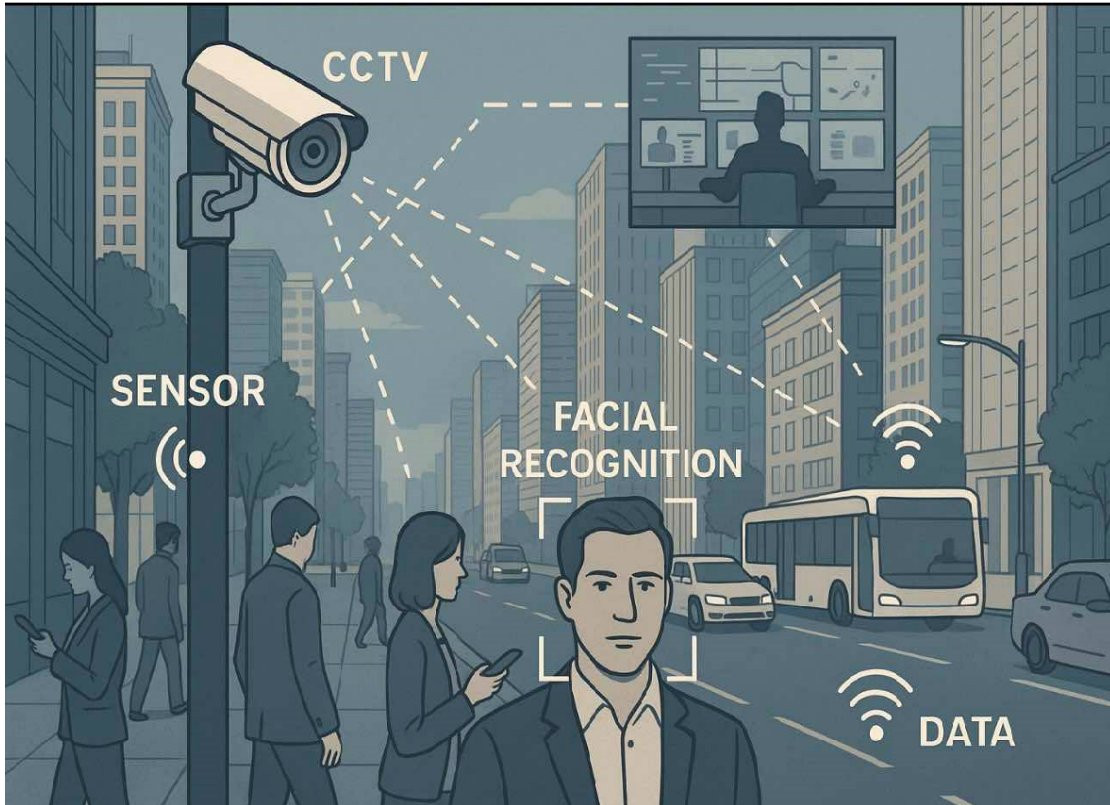

Figure 1.2: The panopticon as a Model for Modern Society of Control: Schematic Representation of Its Implementation in the Urban Space.

This image was created using ChatGPT at my request, based on a detailed explanation and set of instructions I provided. The image illustrates the application of the Panopticon model in the context of a modern society of control. It embodies the basic concepts of centralized control, multi-layered control, and behavioral control in urban space. The model integrates different control technologies such as smart cameras, facial recognition systems, and data analytics, and shows how these tools work together to create an invisible but effective mechanism for social control, in line with the theoretical underpinnings of the Panopticon model and the principles of contemporary

---

[1]Zuboff, op. cit., p. 350

control societies.

1.3 Individual Freedoms between theory and practice

1.3.1 The Concept of Individual Freedoms

History records many occasions when humans have tried hard to obtain freedom, or to preserve what they already have. Everyone wants to be free, although not everyone agrees on what constitutes freedom. Individual freedoms - commonly referred to as civil liberties - are fundamental rights that protect individuals from excessive government control. These freedoms include the right to privacy, freedom of speech, religious belief, and protection by due process of law. They are not privileges granted by the state, but rights inherent to every person. They form the moral and legal foundation of democratic societies and anchor the principles of autonomy and dignity in the legal system.[1]

1.3.2 Philosophical Foundations of Individual Freedoms

The philosophical roots of individual freedoms can be traced back to the Age of Enlightenment, particularly in the works of John Locke and John Stuart Mill. Locke is often regarded as the first philosopher of individual initiative. He believed that individuals in the state of nature possessed natural rights and that they "were moved by instincts to preserve themselves." He argued that the social contract was established to ensure life, liberty, and property, and he asserted that governments are legitimate only when they protect these rights. Any authority that deviates from this objective loses its legitimacy, and individuals have the right to resist and replace it with one that respects their rights.[2]

From his perspective, John Stuart Mill also argued that freedom needs

---

[1] OpenStax. (2022). Introduction to Political Science. Houston, TX: Rice University. p. 145.
[2] Introduction to Political Science: A Basic Framework (PDF). p. 136.

no justification; rather, the burden of proof lies on those who seek to limit or restrict it. For Mill, liberty is essential not only for personal development but also for social progress. The rise of liberalism contributed to the safeguarding of civil liberties and the promotion of democratic principles as core elements of individual freedom. These liberal thinkers emphasized negative liberty, the idea that freedom is defined by the absence of coercion from the state or others.[1]

Modern liberalism, by contrast, embraces positive liberty-the ability to act freely based on equal opportunity and supportive conditions. As John Stuart Mill argued, freedom is not meaningful without the material and social conditions that enable individuals to exercise it. This perspective demands not only state restraint but also proactive state involvement in securing civil rights and addressing structural inequality.[2]

1.3.3 Legal Guarantees and Contemporary Challenges to Individual Freedoms

In democratic systems, individual freedoms are protected by constitutions and legal frameworks. These documents-such as the U.S. Bill of Rights or the Universal Declaration of Human Rights-do not simply state ideals; they serve as practical tools that allow people to challenge the government when their rights are violated. They are meant to limit state power and give citizens the legal foundation to demand justice. Without these protections, rights could easily be ignored or abused by those in authority.[3]

A key legal safeguard is the principle of due process, which means that governments must follow fair procedures when dealing with individuals. This includes both fair trials and the right to be heard, but it also requires that laws themselves must be just and not discriminatory. However, these legal protections only work in practice when courts are truly independent and when there is real political will to respect human rights. If institutions are weak or

---

[1] ibid.p. 136

[2] OpenStax, op. cit., p. 137.

[3] Ibid., p. 147.

biased, then laws may be used to protect power rather than people.[1]

Unfortunately, even with strong legal texts, many governments still limit freedoms in practice. Today, digital control has become one of the biggest threats to privacy. Under the name of national security or fighting crime, governments collect large amounts of personal data without citizensŠ knowledge or consent. This kind of mass monitoring makes people afraid to speak freely or protest-two essential parts of democratic life.[2]

Some political systems go even further. In what are called "illiberal democracies," governments hold elections and have parliaments, but they still restrict civil liberties. They pass vague laws that can be used to silence opposition, block access to information, and control the media. In such countries, individual freedoms become selective-they are only respected if the person agrees with the ruling power. This creates an environment where freedom is not a right, but a privilege given by the state.[3]

Partial Conclusion

Theoretical transformations in the concept of security reflect a significant expansion from its traditional dimensions-centered on the protection of the state against external military threats-towards more comprehensive perspectives that encompass human, political, environmental, and societal security, as emphasized by liberal, critical, and Copenhagen and Paris School approaches. This conceptual evolution has been accompanied by a shift in the exercise of power from overt, repressive forms in traditional societies to more subtle and organized mechanisms in modern ones. This includes the transition from the disciplinary society, which regulates individuals within enclosed institutions such as schools, prisons, and factories, to the society of control, characterized by pervasive, continuous control across all spaces, often enabled by digital

---

[1] Introduction to Political Science: A Basic Framework, op. cit., p. 189

[2] Ibid., p. 201.

[3] OpenStax, op. cit., p. 150.

technologies.

Power is no longer exercised primarily through coercion, but rather through normalization and self-discipline, induced by a constant sense of observation. Michel Foucault's theory of disciplinary control, and Gilles Deleuze's expansion into societies of control, illustrate how control has become embedded in daily life through algorithmic monitoring, smart devices, and predictive data analysis. Technology is now a central tool in the extension of control over individuals, blurring the boundaries between public and private spheres and transforming modern societies into digitally surveilled environments.

As control tools expand, individual freedoms face increasingly complex challenges. The demand for security often comes at the expense of personal privacy and fundamental rights. This chapter has demonstrated the theoretical tension between security imperatives and the preservation of liberties, and how digital control mechanisms threaten to disrupt that fragile balance. It lays the necessary theoretical groundwork for the following chapters, which will explore the practical implications of control on freedoms, particularly through the case study of China. Security The theory of security in the modern period have undergone several intellectual shifts, and these represent the results of a fundamental transformation of the concept of security from its traditional roots (the state's defense against external military threats) to the notion of human, political, environmental, and social security, as highlighted by liberal, critical, and Copenhagen and Paris School theories. This intellectual transformation has been accompanied by a social transformation of power itself; in the past power had been exercised in an overtly repressive manner in the form of the state, whilst the new social structures of power have been the product of some obscurantistic action. A distinguising term for this social change has been the society of control, in which all physical spaces have been constantly monitored and, as a result, are inherently visible. Often this technology has been exploited

to enhance privacy.

Power now has no longer beget coercion, but is also a normative and self-disciplined process that takes place due to the daily experience of observation. Related readings include Michel Foucault's theory of disciplinary control, Gilles Deleuze's expansion of control to societies of control, and today's technology as a tool for control, as an algorithmic monitoring system, smart appliances and predictive data analysis, make control one of the key elements in the extension of control over individuals, blurring lines between the public and private spheres and transforming modern societies into digitally monitored environments.

As control tools become more sophisticated and powerful, the challenge faced by individual freedoms becomes more complex in its nature. The need for security is frequently at odds with the pursuit of individual privacy and fundamental human rights. This chapter has stressed the theoretical link between preoccupations with security and the protection of freedoms, and how digital control mechanisms could undermine that fragile balance. It also laid out the theoretical basis, in the case of China, for the next chapters, which will deal with the practical implications of control on freedoms.

Chapter 2: The Necessity of Society of Control to National Security and its Implications on Freedoms and Privacy

Partial Introduction

With the spread of control systems across various aspects of our daily lives, questions are increasing about the limits of authority held by monitoring entities and whether this conflicts with individual freedoms. It has become clear that continuous control is not just a tool for fighting crime or improving services, but can turn into a means of controlling individuals and imposing specific behaviors on them. In this context, many questions arise about the impact of these practices on human freedom and privacy. When discussing individual freedoms in a world saturated with control, the issue of privacy emerges as one of the core elements that must be defended. Individual freedoms form the cornerstone of any democratic society, and preserving them is a fundamental part of respecting human dignity. While control allows authorities to collect and analyze individuals' data, it can also lead to the erosion of individual freedoms, raising questions about one's place in a world where they are transformed into a "transparent body." In this context, the need to find a balance between security and the protection of individuals' rights arises, through laws and regulations that ensure the respect of privacy and basic freedoms.

2.1 The security advantages of the society of control

2.1.1 Technical and Security Architecture for the society of control

Modern societies have witnessed the quantum leap of technical control methods, which are now a component of society of control devices. The methods are grounded in stringent scientific laws and characterized by the ability to penetrate daily life structure due to the fact that they are intended to reform the environment and action using proactive and preventive means. control is not merely a reaction to a breach anymore but is based on examining

and reorganizing the setting to reduce potentialities for breaching or make them impossible without reliance on the will or free decision of the individual.[1]

Michel Foucault's theory of disciplinary societies, which emphasized enclosed institutions like prisons and schools as sites of control, has evolved in contemporary contexts into more fluid control networks that penetrate public and private spheres alike. This transition reflects a fundamental shift in the modalities of power, where control is embedded within everyday technologies and social interactions, extending control beyond physical boundaries.[2]

Moreover, this technological infrastructure does not operate in isolation but is deeply intertwined with political and economic power structures. The data harvested through control is not merely for security purposes but also serves as a mechanism for social regulation, shaping behaviors and reinforcing hegemonic relations between the state and its citizens.[3]

Among the most popular instruments adopted in this context is genetic analysis, a technique that entails the examination of the DNA of a person in an effort to identify or link him to a specific crime. It has become a central tool within forensic science, enabling DNA to be identified with phenomenal accuracy even in complex circumstances, enhancing the chances of suspect identification or the clearing of innocents.[4]

Smart chips, implantable microchips into cards, commodities or even the human body, are also used to track movement and store location and time data. They are used to monitor the movement of individuals in security agencies and airports, and monitor people entering or interacting with specific environments.[5]

Face recognition systems access image analysis algorithms to identify a person from their facial features. They can be installed in public areas, airports,

---

[1] Gary T. Marx, Technology and Social Control, International Encyclopedia of the Social and Behavioral Sciences, 2nd ed., 2015, p. 117.

[2] Foucault, Michel. Discipline and Punish, op. cit.

[3] Lyon, D. (2007). Surveillance Studies: An Overview.

[4] Marx, Gary T., op. cit., pp. 119-120.

[5] Ibid.,pp. 117-118.

schools, and even intelligent control cameras, so it would be difficult to evade visual detection or disguise, as these systems are highly precise in matching faces to huge digital databases.[1]

Biometric identification systems rely on unique physical characteristics such as fingerprints, iris, handshape, or voice. These tools enable access control to places or devices, prevent illegal use of property or systems, and in some cases are even used to prevent the operation of vehicles or weapons by unauthorized persons.[2]

Drones have also emerged as an effective means of control, especially in border areas or large gatherings. Drones are capable of capturing high-quality images and videos, and allow security agencies to monitor locations remotely and detect suspicious activities without direct human intervention.[3]

Another more advanced tool is algorithmic assessment and risk prediction systems, where individuals are categorized based on their data and digital behavior in huge databases and assigned a risk score or likelihood of engaging in deviant behavior. These systems are used to guide proactive control and security prioritization, such as in cases of crime prevention or monitoring potential terrorist threats.[4]

These tools have come to constitute what is known as "security engineering": designing the environment and social behavior in a way that makes violation less likely, more costly, or less beneficial. This is done through subtle technical strategies, including removing the potential target (e.g., demonetization), reducing its value (e.g., tainted money), enclosing it with isolation and protection (e.g., bulletproof glass), incapacitating the potential actor (e.g., non-lethal tools for temporary paralysis), electronically excluding it (e.g., surveillance bracelets), or through real-time identification of violators

---

[1]Ibid., p. 117.
[2]Ibid., pp. 118-119.
[3]Ibid., p. 117.
[4]Ibid., p. 119.

(e.g., smart cameras, sound and heat systems).[1]

The technological boom has contributed to a radical shift in the concepts of control and control, so that these tools are no longer just means of surveillance, but have become a structural component of state's security policies. Hence, understanding the evolution of these tools requires understanding how they have become a mainstay in national security strategies, especially in light of contemporary cross-border threats. This requires moving on to analyzing the role of these tools in building a new security model that goes beyond traditional methods of protection and response.

2.1.2 Control tools as a means of achieving national security

Achieving national security in the digital age has come to depend largely on a state's ability to own and employ technological control tools. The rise of complex threats, especially in the aftermath of the September 11 attacks, has accelerated the integration of technology into national security policies. No longer content with post-event deterrence or punishment, the state has focused on proactively collecting and analyzing information through multi-level predictive and digital systems.[2]

In this context, new institutional structures were developed, research and development budgets were increased, and cooperation between local and international agencies, both public and private, was intensified. This networked structure has enabled real-time data sharing, allowing cross-border threats to be detected and suspicious movements to be tracked with high accuracy. The combination of biometric control and algorithmic profiling has enabled the construction of smart security maps, identifying hotspots and assessing the riskiness of individuals even before they commit any actual criminal act.[3]

These technologies have been translated into practical measures, such as

---

[1]Ibid., pp. 118-120
[2]Ibid., p. 117
[3]Ibid., pp. 117-118.

adopting behavioral pattern analysis-based programs to identify individuals "at risk" of delinquency, or placing people on watchlists based on their digital behavior or social profile. Technical tools are able to track people, vehicles, and communications, and correlate data from control cameras, sensors, and criminal databases, enhancing constant vigilance and reducing response time to any threat.[1]

In this model, security is seen as a dynamic, proactive system, and society is sought to be "designed" in a way that closes off access to crime, or makes it cost-effective and unviable. Strategies such as removing attractive targets of offense, devaluing them, surrounding them with enhanced physical and digital protection, and disabling potential perpetrators through non-lethal tools or electronic tracking systems are adopted in this context.[2]

For example, biometric systems such as fingerprint and iris scanners facilitate secure identity verification processes, while AI algorithms scan social media content to detect extremist rhetoric or plans for violent acts. Cross-border intelligence-sharing alliances, exemplified by the Five Eyes network, further augment state's control capabilities by enabling the exchange of sensitive data and coordinated responses to transnational threats.[3]

While these tools are effective, over-reliance on them can lead to unintended consequences. Focusing on the technical treatment of risk may overlook the deeper social and political aspects that contribute to the production of the threat. Removing humans from the "decision-making circle" in favor of the machine may result in models of injustice or misclassification, as algorithms fail to recognize the nuances of individual cases.[4]

On the other hand, this security model may lead to overloading the security system, due to the huge amount of information flowing in, opening the door for patterns of bias, corruption, or illicit exploitation of data to emerge. Social

---

[1] Ibid., pp. 119-120.
[2] Ibid., pp. 118-120.
[3] 9. Five Eyes Alliance. (2022). Intelligence Sharing Report
[4] Marx, Gary T., op. cit., p.121.

complacency may even arise when individuals believe that the machine is capable of complete protection, weakening the immunity of society and making it hostage to technical engineering rather than ethical contracting and collective consciousness.[1]

2.1.3 The effectiveness of control tools and the state's justification for their use

As technological policing tools have evolved and proliferated in various aspects of contemporary life, there have been real indications of their real potential to enhance security within societies. These tools, when employed within a clear legal and institutionalized environment, can reduce threats and enhance the sense of security, especially in sensitive environments that require a quick and proactive response.

The best example of such achievement is the use of facial recognition technology in airports and public establishments, leading to instant arrest of targeted people or identification of suspicious identity, without any need for manual checks or overt intervention. Similarly, chips enabled traceability of commodities and people in vulnerable locations such as ports and manufacturing areas, eliminating smuggling and theft of resources.[2]

Algorithmic risk prediction systems and profiling algorithms are used to monitor individual's behavioral patterns and categorize them according to how dangerous they can be, so that security operations can be directed towards the most likely individuals to stray. For example, such systems have been used to monitor the activities of some individuals with criminal records or who are threats to society using tracking devices linked to intelligent alarm systems.[3]

Intelligent camera technology and thermal and acoustic sensors have also proved to be effective in safeguarding banking facilities and strategic facilities, facilitating early detection of intrusion or attempt at theft and facilitating timely

---

[1] Ibid., pp. 121-122.
[2] Ibid.,p. 119
[3] Ibid., p. 119.

intervention before the damage is inflicted.[1] Some schools and health facilities rely on biometric access systems to ensure the protection of vulnerable groups such as children or patients and prevent unauthorized access, reducing security incidents related to intrusion or violence.[2]

Despite some ethical and social reservations about the extensive use of these technologies, their effectiveness in preventing danger and facilitating security response are among the strengths that justify, in the eyes of the state, the increased investment in them. The state sees these tools as a means of protecting society, especially in light of increasing and complex risks, such as cross-border terrorism, organized crime, and illicit flows.[3]

Effectiveness and State Justifications Governments justify the deployment of extensive control measures by emphasizing their role in protecting public safety and ensuring national stability amid evolving security challenges. Empirical evidence from various jurisdictions indicates that the presence of control cameras correlates with reductions in crime rates ranging from 30% to 40%, particularly in urban environments.[4] Furthermore, big data analytics have enabled security agencies to disrupt planned terrorist operations by identifying suspicious patterns and networks before attacks occur. United Nations reports attribute the prevention of over 60% of foiled terrorist plots in the past decade to the effective use of control technologies and intelligence analysis.[5] Nonetheless, these justifications are subject to critical scrutiny, as concerns persist regarding the opacity of data collection methods, potential abuses of power, and the absence of robust oversight mechanisms. Critics argue that without transparent governance and accountability, control risks becoming a tool of unchecked state control rather than a means of legitimate security enhancement.[6]

---

[1]Ibid., pp. 119-120.
[2]Ibid., p. 118.
[3]Ibid., p. 117.
[4]Home Office UK, Crime Reduction and CCTV, 2020
[5] UN Security Council, Terrorism Prevention Report, 2021
[6]E-International Relations, Justifying Surveillance,2015

In moments of crisis, such as pandemics or disasters, control technology may be the determining factor in the response of local governments. For example, in the COVID-19 pandemic, governments utilized control and tracking individuals technology to restrict the transmission of the disease. Through contact tracing apps, it was able to identify high-risk areas and warn the public immediately about areas to avoid. As per this, control is demonstrating how efficacious it can be in public health conservation in times of emergency.[1]

However, this practical success does not negate the need to consider potential side effects, especially the tension between security protection and individual freedoms. While these tools are capable of achieving security, they may, in some contexts, lead to the restriction of private life.

2.2 The Risks and Fears Associated with the Society of control's Impact on Individual Freedoms

As security threats escalate and the reliance on technology to manage public affairs increases, security has become a top priority for governments, which has often led to an over-prioritization of security at the expense of individual freedoms. In the pursuit of stabilization and risk management, control and data collection powers have been widely expanded, raising many legal and ethical concerns about the extent to which individual freedoms are respected.

2.2.1 Core Human Rights Implications

- **Right to Privacy:**

---

[1]Ferguson, N. M., Laydon, D., Nedjati-Gilani, G., et al. "Impact of non-pharmaceutical interventions (NPIs) to reduce COVID-19 mortality and healthcare demand." Nature Medicine, vol. 26, no. 5, 2020, pp. 679Ű685.

Privacy is one of the most prominent rights affected by this security trend. The right to privacy is a prerequisite for most other rights, including the right to freedom of expression; freedom of association with others; the right to express political opinion; the right to seek medical care; the right to education; and the right to found a family. However, the right to privacy, as enshrined in numerous international instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, and at the regional level through instruments such as the African Charter on Human and Peoples' Rights, the African Charter on the Rights and Welfare of the Child, and the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), is under siege due to the widespread use of control technologies. Large-scale information gathering, widespread control, and the practice of covert control by vigilant observers significantly undermine the autonomy of individuals and subvert reasonable expectations of privacy in the private and public spheres, whether through control cameras, facial recognition technologies, or digital tracking, transforming privacy from a recognized right to a restricted privilege. This shift undermines the core principles that underpin democratic societies, where privacy is the foundation of individual freedom and self-determination. Moreover, the absence of precise legal frameworks and effective oversight mechanisms paves the way for serious abuses and provides authorities with oversight tools that operate outside the framework of public accountability.[1]

- **Freedom of expression:**

Freedom of expression: control technologies have the potential to undermine the protection of the human right to freedom of expression envisioned by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Depending on the extent and manner in

---

[1] Marie Patricia Natakwa, "Balancing Security and Freedom: Human Rights Amid Technological Surveillance", LinkedIn, 23 May 2024, accessed 10 May 2025, available at: https://www.linkedin.com/pulse/balancing-security-freedom-human-rights-b5o1e

which they are used, these technologies can violate individuals' right to express their views by creating a chilling effect that forces individuals to practice self-censorship and not engage in dissent. For example, there are at least 22 nations whose legal frameworks require or urge digital platforms and social media companies to remove undesired political, social, and religious speech using machine learning.

- **Right to Assembly and Association:**

Contrary to the Universal Declaration on Human Rights and International Covenant on Civil and Political Rights, the monitoring of social media platforms and companies, telecommunications, and public spaces can impede the exercise of the right to peaceful assembly and association. Control might discourage people from attending protests, organizing rallies, or joining advocacy groups, lest they suffer retaliation or consequences associated with control.[1]

- **Right to a fair trial:**

This right as encapsulated in Article 11 and Article 14 of the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights has also felt the claws of technological control. The monitoring of social media platforms and companies, telecommunications, and public spaces can impede the exercise of the right to peaceful assembly and association. Control might discourage people from attending protests, organizing rallies, or joining advocacy groups, lest they suffer retaliation or consequences associated with control. Surveillance technologies raise innumerable questions of profound ethics regarding the development, deployment, and impact on individuals and society. The use of control evidence in courts seriously jeopardizes the right to fair trial and due process. Concerns regarding the validity, admissibility of

---

[1]Mohamed Hamza, Balancing Security, Freedom, and Human Rights, LinkedIn Article, published April 17, 2023. Available at: https://www.linkedin.com/pulse/balancing-security-freedom-human-rights-b5o1e (accessed May 25, 2025).

data are raised. The techniques of gathering and monitoring may make legal procedures unfair and unbalanced, putting the rights to a fair trial at risk.[1]

Continuous monitoring engenders an environment of fear and self-censorship, whereby individuals restrain their speech and behavior due to perceived or actual control. This chilling effect undermines democratic participation and stifles dissent, impeding the open exchange of ideas essential to pluralistic societies.[2] European Court reports explain that "control undermines freedom of opinion, especially on sensitive political or religious topics." In China, it has been documented that lawyers and human rights activists have been tracked and imprisoned under the pretext of threatening national security.[3]

Moreover, the indiscriminate collection and retention of personal data-often without informed consent-exacerbate vulnerabilities to misuse, discrimination, and political persecution. Such practices erode trust in public institutions and weaken the social contract between citizens and the state.[4]

2.2.2 The Politicization and Abuse of control

In authoritarian and hybrid regimes, control technology tends to be employed not in the interests of public safety, but as a political repression tool. Initiatives that begin life as a national security mechanism soon turn into a means to utilize against opposition, investigative journalism, and civil society at large. As rights organization Amnesty International pointed out in its 2022 report, governments are using control technology more and more to repress expression, assembly, and freedom of dissenting opinion instead of

---

[1] Mohamed Hamza, Balancing Security, Freedom, and Human Rights, LinkedIn Article, published April 17, 2023. Available at: https://www.linkedin.com/pulse/balancing-security-freedom-human-rights-b5o1e (accessed May 25, 2025).

[2] Muedano, A. (2025). "Will You Monitor Us, Harvard?" The Harvard Crimson, February 3, 2025.

[3] Marie Patricia Natakwa, "Balancing Security and Freedom: Human Rights Amid Technological Surveillance", LinkedIn, 23 May 2024, accessed 10 May 2025, available at: https://www.linkedin.com/pulse/balancing-security-freedom-human-rights-b5o1e

[4] Privacy International. (2017). Human Rights Committee Briefing on the Data Protection Bill. November 21, 2017.

protecting the public. The report describes that, "control is becoming a key pillar in the architecture of repression," especially in those states with no proper independent judiciary oversight.[1]

A striking illustration is the digital governance approach of the Chinese government, specifically how it has treated the Uyghur Muslim minority in Xinjiang. Through extensive deployment of facial recognition, biometric data collection, artificial intelligence-powered profiling systems, and pervasiveness of real-time control, Chinese government has built what Human Rights Watch calls a "virtual prison". People's smartphones are continuously scanned for forbidden content, movement is hampered through checkpoints, and behavior is scored on the basis of algorithmic assessments, often without clear criteria. The cyber infrastructure, as used in the context of counterterrorism, amounts to a tool of cultural assimilation and blanket control against an entire ethnic community.[2]

The issue extends beyond Chinese boundaries. Worldwide, several governments have employed control as a tactic, allegedly to fight extremism. Russia, Egypt, Saudi Arabia, and Turkey are nations that have enacted laws allowing data interception and online activity monitoring, in many cases without the requirement for judicial supervision. In most instances, the language employed by these legislations is ambiguous, and this provides security agencies with plenty of discretion in deciding what will constitute a "threat". According to the 2023 Digital Authoritarianism report published by Freedom House, a minimum of 29 nations-some of which are so-called democracies-are using cutting-edge control technology to surveil and harass political competitors, journalists, and civil society members.[3]

---

[1]Amnesty International. Surveillance and Political Repression. London: Amnesty International Publications, 2022, p. 5. Available at: https://www.amnesty.org/en/documents/pol30/4321/2022/en/

[2] Human Rights Watch. China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App. New York: HRW, 2021, pp. 3Ű10. Available at: https://www.hrw.org/report/2021/05/01/chinas-surveillance-uyghurs

[3]Freedom House. Freedom on the Net 2023: The Repressive Power of Artificial Intelligence. Washington DC: Freedom House, 2023, pp. 8Ű11. Available at: https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence

The politicized use of control technology undermines the pillars of democratic governance. This state results in lost confidence in institution frameworks, fosters widespread self-censorship, and strengthens the power of executive elites. And in the lack of openness and free regulatory institutions, the distinction between allowed control and prohibited spying becomes increasingly blurred. Actions undertaken in the name of being in the national interest typically translate to cyber-oppression. Within such a framework, control is transformed from protection of the public to instruments of suppression of dissent.

Unchecked control is one of the most significant threats to modern democracies. Without an independent judicial check on control mechanisms, it is highly likely that the mechanisms will be employed by the state to limit political and social freedoms. Excessive dependence on control in society can lead to the political system being transformed into tyranny or even authoritarianism, where control is utilized to consolidate power and not protect the people. Centralization of sensitive data and information in private or government hands is a powerful threat to the rule of law and the rights of the individual.[1]

2.2.3 The Psychological and Social Effects of the Society of control under Nash Equilibrium Theory: A Study of Disciplinary Behavior under Conditions of Uncertainty

Normalization of control is most likely the darkest indirect consequence that can result from the proliferation of control technology. The individuals slowly adapt to increasing levels of control, as they are no longer so keen on expressing their views freely out of fear of retribution. If control is made the new normal in daily life, then the citizens can start policing themselves and eradicating their various or dissenting conduct, taking away from them their freedom as individuals. As French philosopher Michel Foucault argues, we can

---

[1] Jürgen Habermas, The Structural Transformation of the Public Sphere, MIT Press, 1991, p. 73.

see how control has risen from a primitive and forceful device to an invisible force which affects individuals through self-control.[1] This pervasive control has a profound psychological and social effect on individuals, reaching beyond concerns of privacy to affect mental health and social behavior.

Being in a state of constant control is a highly costly psychological state. Individuals become more stressed, anxious, and continuously threatened, leading to social withdrawal and isolation[2]. Studies indicate that control provokes "anticipatory remorse" as people avoid political action or participation out of fear of retaliation[3]. All this control diminishes social trust, breaks down communities, and weakens democratic resilience[4].

In addition, algorithmic profiling and online content bias strengthen social divides by sustaining echo chambers and excluding opposing voices to the margins[5], hence compromising social cohesion and democratic debate. Under constant scrutiny, the psychological burden is tremendously high. Individuals are more nervous, tense, and always exposed, and this can lead to social withdrawal and isolation[6]. Research finds that control evokes "anticipatory remorse," causing individuals to desist from political participation or activism to avoid anticipated consequences[7]. Such control erodes social trust, breaks

---

[1]Michel Foucault, Discipline and Punish, op. cit., p 196.

[2]Cambridge University, "Monitoring Mental Health: Legal and Ethical Considerations of Deploying AI in Psychiatric Units", Cambridge University Press, 2023, available at: https://www.cambridge.org/core/product/C873AF5A4123E3C5224C8AB3E045F942, accessed on May 19, 2025, at 01:04.

[3]RIWI & Data4Change, "Self-Censorship on Social Media: Understanding the Safety Crisis", Research Report, 2025, available at: https://riwi.com/research/self-censorship-online-how-toxicity-and-disinformation-are-silencing-voices, accessed on May 19, 2025, at 01:04.

[4]The Journal of Social Psychology, "The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'", 2022, available at: https://www.researchgate.net/publication/251705541, accessed on May 19, 2025, at 01:04.

[5] D. Murray et al., The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe, Journal of Human Rights Practice, Vol. 16, No. 1, 2023, p. 398, available at: https://academic.oup.com/jhrp/article/16/1/397/7234270 (accessed 19 May 2025).

[6]Cambridge University, "Monitoring Mental Health: Legal and Ethical Considerations of Deploying AI in Psychiatric Units", Cambridge University Press, 2023, available at: https://www.cambridge.org/core/product/C873AF5A4123E3C5224C8AB3E045F942, accessed on May 19, 2025, at 01:10.

[7]Data4Change, "Researching Self-Censorship Among Human Rights Activists", Field Study, 2025, available at: https://www.data4chan.ge/blog/self-censorship-research, accessed on May 19,

down communities, and emboldens democratic vulnerability[1]. In addition, algorithmic profiling and biased content curation on internet platforms reinforce the social cleavages by empowering echo chambers and suppressing contrary opinions[2], further undermining social cohesion and democratic debate.

Nash equilibrium is a game theory concept meaning that a state of strategic interdependence among competing agents in their interactions whereby no agent can do better for itself by unilaterally changing its strategy, provided the other agents keep their strategies unchanged. To that end, it is the point at which each individual decision is optimal under the expectations of other's behavior; therefore, an equilibrium system does not have anyone as a lever to rebel or change. The Nash equilibrium is also widely used in modeling human and social behavior, explaining how decisions are made in competitive or cooperative multi-party environments, and showing that individually rational strategies can lead to stable outcomes on a collective level.[3]

One of the most famous applications of Nash equilibrium is the Prisoner's Dilemma model, which illustrates how individual rational decisions under uncertainty can lead to less-than-optimal outcomes at the collective level. In this famous game, two separate prisoners are held separately and presented with the options of cooperation (silence and not confessing) or betrayal (confessing the crime to the partner's frame). In this model, neither party knows the other's decision, so if both remain silent, they are lightly punished. If one confesses, they are released and the other is severely punished. If both confess, they are punished moderately. Each prisoner's rational choice (according to the Nash equilibrium) is to betray, because it achieves the best individual

2025, at 01:15.

[1] The Journal of Social Psychology, "The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'", 2022, available at: https://www.researchgate.net/publication/251705541, accessed on May 19, 2025, at 01:17.

[2] D. Murray et al., The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe, Journal of Human Rights Practice, Vol. 16, No. 1, 2023, p. 398, available at: https://academic.oup.com/jhrp/article/16/1/397/7234270 (accessed 19 May 2025).

[3] Osborne, M. J., & Rubinstein, A. (1994). A Course in Game Theory. MIT Press, p. 15.

outcome regardless of the other's choice. Although mutual silence would have achieved a better outcome, the collective outcome here is worse than if they had cooperated. This illustrates how individual rational decisions can lead to disastrous collective outcomes.[1]

Applying Nash Equilibrium on the dilemma of the Society of Control Strategic Players:

- The state (security agencies)

  Objective: Maximize national security.

- Individuals

  Objective: Exercise freedom and protect privacy.

The Game:

	Individual	
	Obey	Resist
High Surveillance	0/ 0 (1)	0/-1 (2)
Low Surveillance	+1/0 (3)	-1/+1 (4)

State

Figure 2.1: Nash Equilibrium in the Surveillance Society: A Strategic Interaction Matrix.

Matrix analysis:

- Case 1:

  – The state incurs the costs of control, yet it gains security.

  – The individual loses public freedom, but gains security and avoids punishment.

- Case 2:

---

[1]Ibid., p. 16

  – The state gains security.

  – The individual gets punished.

- Case 3:

  – The state saves control costs, while maintaining security.

  – The individual loses freedoms, but he still avoids punishment.

- Case 4:

  – The state loses security.

  – The individual gains freedom and avoids punishment.

Strategies evaluation:

For the state, the most advantageous outcome is case 3. As it ensures both security and cost efficiency.

For the individual, the best outcome is case 4. As it ensures both freedom and protection from punishment.

However, in the absence of mutual trust, both players tend to assume the worst case scenario. This leads each of them to adopt a rational choice, that guarantees their respective interests regardless of the opponent's behavior.

Accordingly:

- The state's optimal strategy is High Surveillance (case 1)

- The individual's optimal strategy is to abide (case 1).

- Thus, the Nash Equilibrium is (CASE 1), where neither player can improve its outcome unilaterally.

Applying the Nash equilibrium to the society of control shows a strategic dilemma resulting from the mutual distrust between the two parties. The state, fearing individual disobedience and rebellion if it minimizes control, chooses to impose strict control to maintain security. On the other hand, the individual

chooses to obey rather than demand freedom for fear of being punished under control, preferring safety to exercising his or her freedoms. As a result, each party adopts a strategy that protects them from the worst possible scenarios, rather than seeking a joint optimal outcome. The first case represents a Nash equilibrium, where neither the state nor the individual can unilaterally improve their situation by changing their strategy. Although there are better scenarios for both parties (such as the third or fourth case), the lack of trust keeps them in a stable but suboptimal situation, characterized by higher costs for the state and less freedom for the individual.

Within the framework of a control state, this can be utilized to describe the multifaceted dynamic between the state and the people wherein the people are presented with a situation similar to the prisoner's dilemma with doubt regarding their control status. But with greater complexity, the individual makes a decision between obeying the rules and behaving well (cooperation) or disobeying them (betrayal), without knowing whether there is actual control that imposes sanctions. According to Nash equilibrium, the rational choice for individuals is to abide, because the possibility of control exists, and the potential penalties (such as fines or imprisonment) outweigh the gains of disobedience. This leads to self-discipline that stabilizes the social order and reduces the need for constant and effective monitoring of every action.

This balance creates a state of social discipline that relies on individual's expectations of each other's behavior and uncertainty about the presence of control, which reinforces order and reduces offending behaviors without the need for constant monitoring. This is the effectiveness of the modern society of control, which relies not only on technological monitoring mechanisms, but also on the transformation of the individual into a "watcher of himself" due to the constant threat of an invisible eye.[1]

Although this balance achieves superficial security stability, it has profound psychological and ethical ramifications. The constant state of

---

[1]Foucault, Michel. Discipline and Punish, op. cit., p. 201

uncertainty produces a constant existential anxiety that limits the spontaneity of human behavior and undermines freedom of expression and individual initiative. The observed individual does not act as himself, but rather codifies his actions based on what may be assumed to be "visible", generating collective psychological tension[1].It also builds up interpersonal relations characterized by suspicion and fear, resulting in a decline in social trust, which is one of the fundamental dimensions of democratic existence. There is, therefore, a requirement to review security policies for striking a good balance between safety and freedoms, through transparent processes and well-defined demarcations of the boundaries of control.[2]

Incorporating the concept of Nash equilibrium into the study of the society of control provides an in-depth understanding of how individuals interact with an uncertain control environment, and explains how uncertainty leads to self-disciplined behavior, but at the same time highlights the negative psychological and social effects that may result from this discipline. Achieving a delicate balance between security and freedom requires balanced policies that take into account these dimensions and ensure the protection of individual freedoms without compromising social stability.

2.3   Balancing National Security and Individual Freedoms

Balancing security and individual freedoms is a complex dilemma faced by societies, especially with the emergence of digital technologies and increasing global security concerns. This balance consists of trying to reconcile the necessity of achieving national security on the one hand, and preserving individual freedoms on the other. The main challenge is to determine the extent to which governments can intervene in security without excessively infringing on individual freedoms.

---

[1]Zuboff, Shoshana. The Age of Surveillance Capitalism, op. cit., p. 243.

[2] Solove, D. J. (2004). The Digital Person: Technology and Privacy in the Information Age. New York University Press, pp. 42Ű45.

2.3.1 Ethical Norms for Protecting Individual Freedoms in the Society of Control

Beyond legal regulation, protecting individual freedoms in the age of digital control also requires adherence to strong ethical norms. These norms emphasize that the use of control technologies should always be legitimate, proportionate, and respectful of human dignity. Ethical guidelines call for minimizing intrusiveness, maintaining transparency, and ensuring accountability in how control data is collected and used. As noted by Mosa et al., the ethical dimension is essential for creating a balanced approach to control that does not sacrifice fundamental liberties in the name of temporary security needs.[1] In this sense, ethics serve as a protective shield against arbitrary state behavior, reinforcing the principle that not everything legally permissible is morally acceptable.

- **Public Interest vs Individual Rights** The ethical debate around control often hinges on the tension between public interest and individual rights. On one hand, control can serve the public interest by promoting security and preventing crime. On the other hand, excessive control can undermine individual rights to privacy, autonomy, and freedom of expression. Striking an ethical balance requires a careful assessment of when it is appropriate to prioritize public safety over individual freedoms. Ethical guidelines should provide clear criteria for determining when control is justified and when it crosses the line into unjustifiable privacy violations.[2]

- **Ethical Guidelines for society of control** To address the challenges of balancing security and privacy, ethical guidelines for control are essential. These guidelines should be grounded in principles such as

    – **Legitimate**: Practiced in accordance with the law and aimed at achieving specific ends, such as combating terrorism or organized

---

[1]Msbah J. Mosa et al., "AI and Ethics in Surveillance: Balancing Security and Privacy in a Digital World," PhilArchive, 2023, p. 10.

[2]Ibid., p. 10.

crime.[1]

– **Necessary:** Used only when less intrusive means are not available to achieve the same objectives.[2]

– **Proportionate:** Balances the public interest with individual rights, so that control measures are not excessive or unjustified.[3]

Governments, policymakers, and organizations deploying control systems must ensure that ethical considerations are embedded in the design, implementation, and governance of these technologies. This includes conducting impact assessments, providing avenues for redress, and ensuring that control measures do not disproportionately target vulnerable or marginalized communities. Balancing security and privacy is a complex ethical challenge, particularly in the context of AI-driven control. While security is a legitimate concern, it should not come at the expense of individual freedoms. Ethical frameworks for control must prioritize transparency, accountability, and proportionality to ensure that privacy rights are protected while meeting security objectives. By carefully navigating the trade-offs between security and privacy, control systems can be deployed in a manner that respects both public safety and civil liberties.[4]

2.3.2 Legal Mechanisms for Protecting Individual Freedoms in the Society of Control

In light of the rapid development of control technologies, such as smart cameras, facial recognition systems, and artificial intelligence applications, legal mechanisms for protecting individual freedoms are becoming increasingly vital. These technologies enable the collection and real-time analysis of massive amounts of personal data, allowing state authorities to permanently

---

[1]Ibid., p. 10.
[2]Ibid., p. 10.
[3]Ibid., p. 10.
[4]Ibid., p. 11.

monitor individuals and construct a comprehensive control environment. This situation poses a serious threat to individual privacy and fundamental rights. Thus, robust legal frameworks must be enacted to regulate data collection, limit the discretionary power of security institutions, and ensure that control practices remain under strict judicial oversight. These mechanisms serve as safeguards against abuse and help maintain the delicate balance between national security and civil liberties.

- **The Security-Privacy Trade-off** AI control systems are often justified on the grounds of improving public safety and national security. Governments and law enforcement agencies argue that the ability to monitor public spaces, track individuals, and predict criminal activity can prevent crime and enhance social order. However, this security comes at a price. The collection and analysis of vast amounts of personal data raise significant privacy concerns, particularly when individuals have little control over how their data is used or shared. The ethical question revolves around whether the benefits of security outweigh the costs of privacy infringement.[1]

- **Proportionality in control** An important ethical principle in the security-privacy debate is proportionality. Surveillance measures should be proportionate to the threat they are designed to address. Excessive control, particularly mass control that targets entire populations, is often viewed as a disproportionate response to security threats. Ethical frameworks for AI control must ensure that data collection and monitoring are limited to specific, justified cases where there is a clear need for security intervention. The principle of proportionality is essential in maintaining a fair balance between security needs and privacy rights.[2]

- **Minimizing Intrusiveness** Ethical control systems should aim to minimize intrusiveness, collecting only the data necessary to achieve

---

[1]Ibid., p. 10.
[2]Ibid., p. 10.

security objectives. Overreaching control practices, such as indiscriminate data collection and prolonged monitoring of individuals, can lead to unnecessary invasions of privacy. control systems should be designed with privacy-preserving mechanisms, such as data anonymization and encryption, to limit the impact on individual freedoms. The ethical challenge lies in ensuring that control technologies are used sparingly and with adequate safeguards to protect personal data.

- **Transparency and Accountability** A key ethical consideration in balancing security and privacy is transparency. Individuals should be informed about how AI control systems are being used, what data is being collected, and how it is stored or shared. Transparency promotes trust and allows the public to hold organizations accountable for any misuse of control technologies. Moreover, there should be clear mechanisms for individuals to challenge or opt out of control when they believe their privacy rights are being violated. Ethical control requires both transparency in system operations and accountability for any harms caused by control activities.[1]

2.3.3 International Models for Balancing Security and Individual Freedoms in the Society of Control: The United States Experience

In the modern world, there is a constant struggle between the privacy and personal freedom of individuals on the one hand and the security of the nation on the other. It is an indisputable fact that the modern world has been characterized by advanced technology, such as the Internet, which not only promises a higher level of freedom, but also requires a higher level of security. Based on the achievements of technology, and in order to ensure national security, more and more governments are adopting various control tools to reduce crises, such as terrorism, and to maintain social stability. However,

---

[1]Ibid., p. 10.

the essence of national security has been intensified and replaced by political repression.

- **The United States of America (USA)**

The world witnessed a dramatic shift after the September 11, 2001 attacks, as concerns over national security intensified and individual freedoms came under threat. The United States launched wars in Iraq and Afghanistan under the justification of national security. However, both its domestic and foreign policies have triggered major debates about the balance between protecting citizens and preserving civil liberties.

This enduring tension resurfaced prominently in 2016 during the legal dispute between Apple and the FBI. After the San Bernardino terrorist attack in December 2015, where Syed Farook and Tashfeen Malik killed 14 people, the Federal Bureau of Investigation (FBI) recovered Farook's iPhone and sought Apple's help to unlock the device. The FBI argued that access to encrypted data was crucial for national security and public safety. However, Apple refused to comply, claiming that creating a tool to bypass encryption would violate user privacy and set a dangerous precedent. [1]

The Apple and the Federal Bureau of Investigation case highlighted a core dilemma of the digital age: the same encryption technologies that protect the privacy of everyday users also shield terrorists from lawful control. The case ignited a national debate, especially as politicians from both major parties began pushing for greater cooperation between tech companies and government agencies to address the misuse of encrypted platforms by terrorists. This conflict reflects a larger issue that continues to shape modern governance: how to strike a fair and effective balance between individual freedoms and the imperatives of national security. [2]

---

[1] AiThor, Individual Freedoms and National Security Essay, available at: https://aithor.com/essay-examples/individual-freedoms-and-national-security-essay, accessed on May 26, 2025.

[2] Ibid, may 26, 2025

The intricacies of contemporary society, which have been characterized by globalization, terrorism, and the advancement of communications technology, have caused the interaction between national security and individual freedom to become ever more complicated and significant. The United States is not the only nation to have to cope with the issues; numerous other nations worldwide are also being forced to consider these matters. The challenge of achieving an appropriate equilibrium between safeguarding individual liberties and ensuring national security is not new. Previously, particularly in the 20th century, the equilibrium leaned more towards national security. Nevertheless, following the September 11, 2001, terrorist attacks, the federal government, led by President George W. Bush, enacted several legislative pieces that significantly enhanced national security powers. In particular, the USA PATRIOT Act, a hastily enacted law only six weeks following 9/11, broadened the authority of law enforcement and intelligence agencies to seek and conduct searches and control, and loosened restrictions on foreign intelligence gathering within the United States. The statute also broadened the definition of domestic terrorism to cover acts that "involve acts dangerous to human life that violate the criminal laws of the United States or of any State" and "that appear to be intended to influence governmental policy through intimidation or coercion."[1]

This modification transformed the law from merely giving assistance to a particular terrorist enemy to covering a wider array of acts. There has been a considerable shift in mood in recent years. The bipartisan indignation regarding the extent of control conducted by the National Security Agency, along with allegations of spying on allied nations such as Germany and Brazil, has triggered extensive discussion on the adequate balance between national security and the protection of civil liberties. This is also corroborated by disclosures provided by whistleblowers like Edward Snowden, who has revealed the staggering extent to which intelligence agencies can monitor and retain information. As such, increasing numbers of individuals agree with

---

[1] Ibid, may 26,2025

the views presented by such specialists as Nuala O'Connor, President and CEO of the Centre for Democracy & Technology, who stated, "Freedom and liberty and democracy are all critical and not just to individual citizens in the US and Europe but to the world and international affairs." Freedom and liberty are values that transcend the American and European philosophies; most individuals and nations view them as universal rights.[1]

One of the most important examples is the passage of the Alien and Sedition Acts in 1798, which greatly restricted freedom of the press along with freedom of speech. These acts were imposed by the Federalist Party, who firmly believed that stringent measures were required to avert a revolution spurred on by French philosophies. Under the Sedition Act, those who hindered government policies or slandered its officials could be fined up to $2,000$ Dollar and jailed for up to two years. A total of 25 people, mostly journalists, were arrested and charged under this act, with 10 being convicted. Those convicted were all Republican newspaper editors who had criticized President John Adams publicly. The Sedition Act effectively silenced the Republican Party, but it also served as a mobilizing force for the party. The broad public outcry against the Alien and Sedition Acts played a large role in the election of 1800, resulting in the triumph of Thomas Jefferson's Democratic-Republican Party. Jefferson, upon assuming office, issued pardons and ordered released all those who were jailed under the Sedition Act, and Congress eventually repealed the act. This case powerfully demonstrates the risk of misuse of national security policy and forces to the surface the contentious and divisive quality inherent in the trade-off between national security and individual liberties during periods of crisis.[2]

The executive and legislative branches have taken different measures to balance freedom and security. The Congress struck the attention between freedom and national security, particularly after the US was attacked by

---

[1] Ibid, may 26,2025
[2] Ibid, may 26,2025

terrorists on September 11, 2001. The former United States Attorney General John Ashcroft stated that the president had the "inherent authority to surveil and intercept" in the United States. The USA Patriot Act, in its provision, sanctioned the president to utilize wiretap in an attempt to obtain non-content wire and electronic communications and allowed a non-US citizen suspect to be targeted by a roving control authority. The Act also removed the restrictions on intelligence sharing and against foreign intelligence and law enforcement. Although these provisions can enhance the equilibrium between security and freedom, a section of American citizens is strongly against the bill. They believe that the Act provides the government with excessive authority to monitor all citizens and lawful permanent residents, without sufficiently guarding the people's privacy rights. Reacting to the public, President Obama enacted into law the reauthorization of the USA Patriot Act in May 2011, which was regarded as the closing act of a legislative process aimed at renewing it.[1]

The incident can raise question regarding the ideal balance between freedom and security. However, gaining an absolutely freedom is not the best for people and realizing the maximum security either; therefore, compromises to the two political demands are in need. Public understandings and vigilance for freedom from both congress and general people are also quite important to limit the possibility of government to exploit the national anxiety for relinquishing liberty. On the whole, the strategy is quite effective because that all around the word, achieving freedom has the similar principle that is it may be necessary to take any moves slowly and to involve a mass amount of the people in the decision making process. Also, the judgment on taking away freedom must have an objective ground and it should not just appears by the name of national security. It is believed that when more people are involved, everyone learns from each other. A community is possible if the members are respecting each other's freedom and people would not give up their freedom which cannot be taken by others. If government works well and

---

[1] Ibid, may 26,2025

truly in respecting the freedom, each act will be justifiable.[1]

Mechanisms for balancing national security and individual freedom extend beyond external and political realms. A very useful method for striking a balance between these competing interests is to educate the public better regarding the types of threats to national security, in addition to why particular methods of protection are being employed. An educated population is far less likely to manifest adverse reactions to laws and programs aimed at national security enhancement. Yet, the course of events in the early 21st century years has demonstrated that it is typically only after a large-scale attack has taken place that discussion on the interpretation and balance of national security and individual freedoms becomes very lively. Attempts at enhancing public awareness must be more than just disseminating information regarding threats to national security. To encourage people to take an active part in assisting efforts of enhancing national security, the public must be informed not only about the scope of their potential contributions but also about the beneficial effects of individual actions being undertaken to respond to threats to national security. Noted specialist Robert Heibel emphasizes the necessity to create and institutionalize an "integrated enterprise approach" to national security enhancement. He also recommends that "all of us in the United States, citizens and foreign nationals, public or private sector organizations must understand that any weakness can be exploited by an adversary to harm us."

Partial Conclusion

Today's society of control relies on an advanced technical and security architecture that helps the state monitor individuals and analyze their behavior with high accuracy, through tools ranging from smart cameras, facial recognition technologies, artificial intelligence systems, communication and geo-location tracking networks to more complex types such as genetic testing

---

[1] Ibid, may 26,2025

and biometric analysis that, in aggregate, transform it into a new form of panopticism. These control technologies are divided into those that we can see and recognize and thus know that we are under control and others that work in secret by analyzing the data collected by the various technologies that we use in our daily lives. Here, we are forced to comply with an authority that we cannot see but believe exists.

This structure has contributed to a radical shift in the concepts of control and control, so that these tools are no longer just means of control, but have become a structural component of the state's security policies. They are capable of early detection of security threats and enable proactive and effective intervention to confront crimes and extremism, thus enhancing the state's ability to protect national security. The executive authority justifies these strategies on the basis of vital security imperatives aimed at maintaining public order and preventing threats of a complex and cross-border nature.

However, in exchange for these security benefits, there are serious implications for individual freedoms, as the widespread proliferation of control technologies undermines the right to privacy, freedom of expression, and freedom of movement. An individual's daily life becomes a field of constant control, generating a kind of self-disciplinary behavior that is in line with the Nash equilibrium model. According to this model, individuals adapt their decisions and behavior based on their knowledge or suspicion that they are under control, causing them to act according to the expectations of authority, even in the absence of direct intervention. This results in an ostensibly stable but fear based behavioral equilibrium in which individuals are willing to sacrifice part of their freedom to avoid punishment or suspicion, creating a state of systematic collective compliance. This is where the Nash equilibrium comes into play as a strategic dilemma arises due to the mutual distrust between the two parties. As a result, each party adopts a strategy that protects it from the worst possible scenarios, rather than striving for a joint optimal outcome.

This effect is compounded when control tools are used for political purposes, whether to monitor opponents or restrict the public sphere, leading to a shrinking democratic space and an erosion of trust in the state. The situation is even more dangerous when there is a lack of transparency about how data is used, or when security agencies overreach without effective institutional oversight. Therefore, it becomes necessary to establish strict legal and ethical frameworks that regulate control, protect individual freedoms from systematic violation, and ensure that security does not become a pretext to undermine the foundations of democracy.

The American experience represents a complex model of this balance between security and freedoms. After the events of September 11, expansive laws such as the Patriot Act were enacted, granting security agencies unprecedented powers of domestic wiretapping and spying.However, this expansion later faced resistance from civil society and from within the judiciary itself, which led to some amendments aimed at minimizing abuses and providing some degree of transparency.Despite the ongoing controversy, the American system has tried, within its limits, to maintain a kind of Nash equilibrium between state power and individual freedom, where citizens act under the pressure of knowing that they are being monitored, while at the same time benefiting from legal guarantees that limit this pressure and protect them from arbitrariness.

Chapter 3: Case of Study China

Partial Introduction

The People's Republic of China is one of the most prominent contemporary examples of the transformation from a punitive state to a society of control, as described by Foucault and Deleuze, as the Chinese authorities were able to build an integrated security system based on advanced technology and comprehensive control of the population. Today, the Chinese experience is presented as a pioneering model in achieving national security, but at the same time it raises a wide debate about the infringement of individual freedoms, especially with regard to the right to privacy and freedom of expression.

China has set up an all-inclusive model of control as part of its national strategy to strengthen national security and ensure social stability. This model, which combines sophisticated technological means and instruments of state control, has been touted as the solution to various social and political problems of the nation. China, in particular, has established mass control as its foundation in monitoring its populace and enforcing public order, presenting a compelling case study regarding balance between security and society. and individual liberties.

3.1 The Chinese Perspective on Security and the Historical Background of the Control Society

3.1.1 Security in Chinese Political Thought

Since the imperial era, the Chinese view of security has been associated with the concept of "safeguarding order" and "social harmony." This view continued to take root during the Communist Party period, especially after Mao Zedong came to power. Security policies witnessed a shift from a focus on external threats to a focus on internal security as a top priority, which justified the expansion of tools of control and control over society. In this

context, security is not merely comprehended as a defense against external threats, but also includes internal policing and control of society for the aim of national unity. Maintaining the integrity of the state and concentration of power is a constant concern for the regime, especially in in light of the enormous ethnic and cultural diversity of China. Policies of repression and control are justified as necessary to protect "social harmony," a vague concept used as a pretext to justify various forms of restriction of freedoms in the name of national security.[1] This trend has been reinforced in recent decades by an escalating political discourse linking China's ethnic and linguistic diversity to the potential disintegration of the state, which explains the heavy presence of security agencies in areas such as Xinjiang and Tibet, under the pretext of combating "separatist tendencies" and "religious extremism".[2]

From a deeper perspective, this perception of security has its roots in Confucian philosophy, which elevates the group above the individual, which has contributed to a political culture that justifies restricting freedoms in the name of the "public interest." The philosophy of the modern Chinese state is based on what can be called "anticipatory control," meaning the need to monitor and analyze the behavior of individuals through smart and advanced tools, with the aim of predicting and containing potential dangers before they occur. Thus, the citizen becomes a subject of constant suspicion in a system that assumes that security prevention can only be achieved through total and comprehensive control. Some researchers believe that this control is not limited to the security dimension, but includes shaping social and cultural behavior according to the state's standards.[3]

---

[1] Creemers, Rogier. "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century", Journal of Contemporary China, Vol. 26, No. 103, 2017, Routledge, p. 8

[2] Brady, Anne-Marie. Marketing Dictatorship: Propaganda and Thought Work in Contemporary China, Rowman and Littlefield Publishers, 2008, p. 42

[3] Qiang, Xiao. "The Road to Digital Unfreedom: President Xi's Surveillance State", Journal of Democracy, Vol. 30, No. 1, 2019, Johns Hopkins University Press, p. 14

3.1.2 The Historical Background of the Control Society in China

control in China has its roots in imperial times, where centralized control and population control were essential tools for maintaining state power. From the Qin Dynasty (221-206 BC), the Chinese state developed an administrative tradition characterized by a strong bureaucracy and meticulous record-keeping systems. Surveillance was used to ensure loyalty to the emperor, maintain social order, and prevent disobedience. A network of spies and informants was used to monitor citizens and report any irregularities or rebellions against the imperial government. With the formation of the People's Republic of China in 1949 led by Mao Zedong, China entered a new period of exercising control over all spheres of political and social life because it became a part of routine life. The CCP established an ideologically and centralized control system. The "professional unit" (Danwei) system allowed the government to control the political activity of citizens, common everyday life, and human relations.[1] Mass campaigns such as the Cultural Revolution (1966-1976) created a snitch culture and shaming environment, with an atmosphere of mutual fear and control.[2]

3.1.3 The Society of Control in the Modern Age

In the post-Mao period, especially since the 1990s, China entered a new phase marked by economic reforms and technological modernization.With the rise of digital technology, the state began to integrate traditional methods of control with modern tools such as CCTV cameras, internet control, and data collection.The 2008 Beijing Olympics marked a turning point in the expansion of the national control infrastructure, under the justification of enhancing public safety and security.[3]

---

[1] Andrew G. Walder, Communist Neo-Traditionalism: Work and Authority in Chinese Industry, University of California Press, 1986, p. 87.

[2] Frank Dikötter, The Cultural Revolution: A People's History, 1962Ű1976, Bloomsbury, 2016, p. 215.

[3] Rogier Creemers, "China's Social Credit System: An Evolving Practice of Control", SSRN Electronic Journal, 2018, p. 3.

China has undergone profound political and legislative transformations, through which it has established a unique national security model based on the fusion of centralized power and modern technology, in what is known as the "digital security state." Legislative frameworks have played a pivotal role in enabling the political system to expand control tools and strengthen control over society, especially after President Xi Jinping came to power, who reformulated the concept of "comprehensive national security" to include not only protecting borders and institutions, but also protecting the "political, cultural, and ideological system" from any potential threat.[1]

3.2   Control Tools and Social Control Mechanisms

3.2.1   Technological Infrastructure of Control

In the context of promoting comprehensive security policies, China has developed a complex technologically advanced structure based on artificial intelligence and sophisticated digital control technologies, aimed at instituting holistic control over social and political processes. The control system entails smart cameras, facial recognition, big data, and internet-based control technologies, which have been integrated into an intelligent network of control over the populace.

These technologies are a vital resource for the authorities to monitor the movement of individuals and analyze their behavior, as all of their daily activities have been placed under monitoring in what can be referred to as a "smart city.". China's Ministry of Public Security released a report that said more than 170 million control cameras had been installed by 2020 and are backed up with face recognition technology to identify individuals in real-time.[2] The vast network of cameras is reported to reach not only public places such as stations and markets but also homes and private areas via apps

---

[1] Baylis, Smith and Owens. The Globalization of World Politics, Seventh Edition, , p. 649

[2] Ibid., p. 652.

linked to the national network.

The People's Republic of China has ambitious control plans, the most well-known being Sharp Eyes. In this system, China's already installed millions of security cameras are linked to one national control platform, even in streets and shops, and personal cameras. Police officers monitor citizens on computer screens as they stroll down the street through cameras and facial recognition software. China also has the "Police Cloud" scheme, a follow-up project employed to collect the data of citizens' online information and government records and link them to their facial scans and identity cards.[1]

Further, the government of China has also relied on interpreting the use of big data collected by way of these cameras and citizens' digital interactions and internet usage. For example, sophisticated software monitors individuals' movement patterns on domestic Chinese apps such as WeChat and Alipay, allowing the state to track their activity at a highly specific level even if there is no physical evidence of suspicious behavior. Such systems have been categorized as "proactive control," where authorities use information to predict illegal or potentially destabilizing behaviors.[2]

In 2015, China adopted a new national security law, giving the authorities broad powers to surveil individuals, companies, and even non-governmental organizations, under the justification of protecting the country's "intellectual and cultural sovereignty".[3] This was followed by the Cybersecurity Law in 2017, which required domestic and foreign tech companies to adhere to data storage policies within China and allow authorities to access them upon request, marking a decisive step in linking technology to political control.[4]

---

[1] Human Rights Watch, "China: Police ŚBig DataŠ Systems Violate Privacy, Target Dissent," Human Rights Watch, November 19, 2017, https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent (accessed April 30, 2025).

[2] The Globalization of World Politics, Seventh Edition, Baylis, Smith and Owens, p. 653

[3] Ibid., p. 649

[4] Ibid., p. 650

3.2.2 The Social Credit System and The Great Firewall as Exam- ples of a Society of Control

The Social Credit System

China's social credit system is the most provocative and disputed endeavor of the digital age. It's more than a bureaucratic framework for grading citizens, however; it's a profound vision of the Chinese state on how to organize and calm society with novel digital tools. The idea of this system has been simmering in the background since the 2000s, but was made public in 2014 in a planning report issued by China's State Council called "2014-2020 Social Credit System Construction Plan." Since then, the project has grown extensively, in terms of technical mechanisms employed, the nature of data collected and processed, as well as actual applications implemented in day-to-day life among citizens.[1]

China's social credit system is the physical manifestation of social control as a concept, in which companies and individuals are scored based on their compliance with the law and societal norms. It exists through bringing together huge amounts of information from a variety of sources, like government records, commercial transactions, and regular behavior, and having people scored and granted or denied privileges according to that score. This is a typical example of the convergence of technology and mechanisms of governance to social discipline, which has raised a whole lot of issues around privacy and freedom.[2]

Essentially, the system is based on a seemingly simple principle of assessing the "social credit" of citizens and institutions on the basis of their behavior, perceived trustworthiness, and compliance with the law, but this simple principle underlies a complex machinery that entwines advanced technologies such as artificial intelligence and big data analysis with a political imagination to govern public conduct through incentives and sanctions. Each

---

[1]Creemers, R. (2018). China's Social Credit System,op. cit., p. 2-19

[2]Ibid., p. 2

individual or organization is digitally registered with "points," which are downgraded or upgraded according to their behavior, such that citizens who make their social payments and comply with the law are rewarded and those who fail in their loan repayment, violate traffic laws, or even post "harmful information" on the web are penalized.[1]

But as we examine further the ends and means of such a system, we discover that it is not so much to establish trust or maximize market performance, as the authorities would have us believe, but to try to create an "electronic mechanism" in order to re-engineer the entire social behavior. As Roger Creemers puts it, the real purpose of the system is not so much to fight corruption or help improve economic relations, but to create a climate wherein citizens will be forced to adopt politically and socially correct methods by never really feeling totally out of sight, regardless of whether they realize that the agents are observing them or not.[2] This type of control does not require direct state intervention every time, but rather operates as a "cybernetic mechanism" that leads to automatic feedback, whereby desirable behavior is incentivized and undesirable behavior is automatically and indirectly punished.

What makes a social credit system different from other control systems is its comprehensiveness and its ambition to cover all dimensions of life. It not only tracks people's economic performance, but also their legal obligations, their respect for public order, their social relationships, and even their speech on social media. The system is not only run by the central government, but also includes several local experiments and private initiatives run by municipalities or tech companies, making the system a multi-actor space that shares the same goal: To produce "good" citizens according to the standards set by the Chinese state.[3]

It is also worth pointing out that the system does not operate in one and

---

[1] Ibid., p. 2
[2] Ibid., p. 3
[3] Ibid., p. 5

central way as might be envisaged but as a "network" of discrete programs differing in method but having similar principles.This allows authorities to experiment with different mechanisms locally and then select the most effective ones to be later generalized at the national level.   For example, pilot projects have been implemented in cities such as Hangzhou and Suzhou, where citizens are evaluated based on very specific rules, such as respect for neighbors, participation in charity, or even the number of volunteer hours they accomplish.[1]

However, without decentralizing the control of the system, the central government remains strongly rooted by exercising power over sweeping control rules for assessment and penalty, and guiding technological policies, symbolizing the will of the state to uphold its position as the center of society of control. It may be said that such a project constitutes the pragmatic incarnation of the "society of control" notion stretching beyond traditional penal systems, which transforms everyday life into an ongoing control environment wherein every conduct - no matter how mundane it appears -is made recordable and assessable, and therefore accountable and penal.

To this extent, lines between private and public life are blurring, as the private sphere itself falls under scrutiny and control. This makes the system a chief cause for concern for proponents of personal freedoms, especially in the absence of an independent oversight mechanism or clear-cut laws protecting personal information. The Chinese citizen today is not just being monitored by the state, but is also becoming a "data producer" that can be turned against him at will and modify his actions and imprison him in invisible boundaries.

Finally, it must be understood that such a system, as great as it may be in combating monetary fraudulence and increasing discipline amongst citizens, evokes deep ethical and political issues regarding the destiny of freedom of individuals with artificial intelligence and big data analysis hegemony.   If society of control must be exercised in the interest of supplying security, how far

---

[1]Ibid., p. 4

can the state be allowed to intrude into the details of people's private lives? Can this sort of large-scale control be defended as a means of furnishing stability or "aking good citizens"? Such questions remain very much on the table and call for a broad critical debate on the nature of power in the digital age".

The Great Firewall

One of the efforts of the Chinese state to strictly control the virtual world and manage the information flow, the government since the late 1990s has established what is known as the Great Firewall, a high-tech technical and security apparatus employed to deny access to overseas Internet material that the state considers a national security or political stability threat. This mechanism consists of numerous tools such as Content Filtering, IP address blocking, DNS Hijacking, as well as traffic examination (Deep Packet Inspection), thus making it one of the most evolved and complex cyber censorship systems in the world.

The Great Firewall not only technologically censors foreign websites and services such as Google, Facebook, Twitter, YouTube, and Wikipedia but also tightly controls native content on the Chinese Internet via algorithms that scan for prohibited words and automatically censor any violation by closing accounts, banning visitors, or even punishing them in criminal court. Homegrown digital service providers such as WeChat and Baidu are under pressure to obey governmental commands scrupulously and provide user data at will, showing virtually complete integration of political powers and technology actors in China.[1]

The Great Firewall monitoring has become one of the columns of the Chinese model of the "society of control," in which technology is used not only to ensure information security, but also to re-engineer the public space and ground the discourse of the state in the citizens' minds. Compared to the old systems which are reliant on security centers or clearly defined institutions, the

---

[1]Deleuze, Gilles. "Postscript...", op. cit., p. 4.

wall system is intangible and fluid and is turned on at every moment without physical manifestation of power. This corresponds to the notion of Gilles Deleuze's "society of control," where closed walls or doors do not exist as they would in Foucauldian disciplinarian society, but infinite and self-renewing control on the side of intelligent systems pervades every instant of digital connectivity in the life of human beings.[1]

On this note, the Chinese citizen is an endless subject of intelligent control, not only by the places they visit, but also by their web navigation, posts, interactions, and even what they do within payment apps or the transportation network. This technological integration is augmented by additional systems such as the "social credit system," rendering the citizen a "perpetually recorded and monitored being," and monitoring an intrinsic component of every normal action, implemented by the state but also between citizens, on a type of mass mass control in which politics and technology coalesce.[2]

The most profound political impact of the Great Firewall is not merely the exclusion of information, but the reconceptualization of the collective psyche of Chinese citizens to the framework of the Chinese Communist Party. Through the exclusion of alternative and oppositional accounts and overriding sources of information, the state sets up an uncontested "official truth" and a paradigm of digital compliance where citizens internalize censorship and recirculate it in their daily practices. This creates a type of self-censorship, where individuals refrain from investigating or speaking about off-limits topics, not just because they are afraid of being punished, but because they have learned and live in a very limited and interpreted knowledge space.[3]

Socially, the wall created an isolated digital space cut off from the outside world, which resulted in so-called "Internet with Chinese characteristics,"

---

[1]Deleuze, Gilles. "Postscript...", op. cit., p. 4.

[2]Samantha Hoffman, Engineering Global Consent: The Chinese Communist PartyŠs Data-Driven Power Expansion, Australian Strategic Policy Institute (ASPI), 2019, p. 19.

[3] Rebecca MacKinnon, Consent of the Networked: The Worldwide Struggle for Internet Freedom, Basic Books, New York, 2012, p. 83.

under which alternative localized communication platforms and search engines, such as Weibo and Baidu, have arisen, all of which are subject to continued censorship. This virtual isolation from the global network established an enclosed internal referential society and assisted in solidifying digital nationalism because it viewed the outside world as dangerous and the inside world as welcoming and stability. This eroded cross-cultural exchanges and reduced potential for political and intellectual openness, thus making Chinese citizens more tolerant of central power and more fearful of foreign influence.[1]

On the other hand, the wall's reliance on artificial intelligence and predictive algorithms has made it also a tool capable of anticipating dissident action before it occurs, by monitoring public trends and communication networks. The over-reliance on such technology for security makes it possible for what some scholars have termed "digital authoritarianism," whereby new communication technologies are transformed into soft tools for repression in pursuit of coercive stability, rather than for participation or transparency.[2]

The effectiveness of "The Great Firewall" does not solely stem from its technological prowess but also from the culture of self-censorship pervasive in China. Chinese companies bear responsibility for the content hosted on their websites and are held liable if they fail to report and remove content conflicting with the Chinese Communist Party's narrative. These companies are required to engage in self-regulation characterized by a commitment to patriotic observance of law, equitableness, trustworthiness and honesty.[3]

Even US corporations are opting for self-censorship to safeguard the substantial profits derived from their engagements with China. In July 2020, Apple made the decision to remove thousands of games from its Chinese App Store in response to a policy mandating that all paid games or games featuring

---

[1] Ron Deibert, Reset: Reclaiming the Internet for Civil Society, House of Anansi, Toronto, 2020, p. 139.

[2] Florian Schneider, "China's Digital Nationalism," Oxford University Press, 2018, p. 117

[3] "Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry," China Services Info, 26 December 2018, https://govt.chinadaily.com.cn/.

in-app purchases must be licensed by Chinese regulators. Apple provided no specific guidance to app developers regarding content that contravened Chinese regulations; instead, there was an abrupt and sweeping removal. Amid this purge, Apple also withdrew the popular iPhone Operating System (iOS) and Android podcast client, Pocket Casts, from the Chinese App Store.[1] The Cyberspace Administration of China determined that Pocket Casts could potentially provide access to content considered illegal within the country and thus demanded its removal. This marked the second prominent podcast app removal from China's App Store.[2]

In the international arena, the principle of sovereignty may appear incongruent with cyberspace. Traditionally, violations of sovereignty pertain to physical acts within the territory of other states. Sovereignty is a concrete, territorial concept, while cyberspace establishes connections between states that seem ethereal in nature. Yet, these two concepts coexist. States and the international community are striving to harmonize the ideals of an unimpeded flow of information in cyberspace with a state's authoritative control over cyber activities within its borders.[3] An increasing number of states, such as China, staunchly advocate for sovereignty over an open and unrestricted cyberspace. For liberal democracies, countering this trend is of paramount importance.[4]

3.2.3 Control in Minority and Autonomous Regions

The Chinese state exercises a highly restrictive control over spaces inhabited by ethnic and religious minorities, especially in Xinjiang and

---

[1]Jon Porter, "Apple Closes Chinese App Store Loophole, Causing Thousands of Games to Be Removed," The Verge, 22 June 2020, https://www.theverge.com/.

[2]Foley, Jordan J. "China's Authoritarian Grip: How China Reinforces Social Control, Cultivates a Climate of Fear, and Minimizes Dissent." Journal of Indo-Pacific Affairs, Air University, 15 November 2023.

[3]Catherine Lotrionte, "State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights," Emory International Law Review 26, no. 2 (2012): 825Ű919, https://scholarlycommons.law.emory.edu/.

[4]Foley, Jordan J. "China's Authoritarian Grip: How China Reinforces Social Control, Cultivates a Climate of Fear, and Minimizes Dissent." Journal of Indo-Pacific Affairs, Air University, 15 November 2023.

Uyghur-majority Tibet which is the ideal ground for experimentation and intensification of digital control systems, where their identity is crossed with national security issues and policies of national unity. The official discourse of the Chinese state is based on the assumption that the existence of minorities entails "potential dangers," separatism or radicalization, which in its opinion justifies the imposition of total control instruments and exact domination of the daily routine of the population. These technologies are not limited to facial recognition or phone tracking, but include monitoring activity in schools, mosques, and workplaces, taking biometric snapshots, and creating "security profiles" for each citizen, on which their degree of loyalty and integration into Chinese national values can be assessed.[1]

These are elements of a broad concept of society of control that goes beyond deterrence and seeks to reshape behavior and identities from the inside, by a combination of digital control and ideological education policy, such as political rehabilitation and mass indoctrination in "educational" detention centers. It can be seen, then, that policing in such areas moves beyond security designs to become a tool of social and cultural engineering to deconstruct collective identities into the centralized identity of the state. Here, the individual is not seen as a free subject, but as an object that must be reshaped to be compelled into the norms of obedience and devotion, which is a direct violation of individual freedoms and minority rights.[2]

China adopts a double strategy in controlling minority areas: one that utilizes technology extensively with the aim of exerting direct control over citizens, and the other that calls upon an ideological discourse that strives to redefine loyalty and belonging. Apart from creating a gargantuan infrastructure of cameras integrated with artificial intelligence technology, the state spends in spreading the "model citizen's" culture through the media and education,

---

[1]Baylis, John, Patricia Owens, and Steve Smith. The Globalization of World Politics: An Introduction to International Relations, 8th ed. Oxford: Oxford University Press, 2020, pp. 572-573.

[2]Lyon, David. The Culture of Surveillance: Watching as a Way of Life. Cambridge: Polity Press, 2018, p. 91

initiating a system of self-policing where the citizens turn themselves and others into watchdogs. This type of control not only wields control from above, but also enacts it horizontally, across society itself, in a "complicit society of control," where communities and families are prompted to report "unpatriotic" or "suspicious" behavior.[1]

This model is a paradigm shift from the idea of power, as not only are bodies surveiled by the state, but the state also attempts to penetrate minds and remake perceptions and values according to the state discourse. To this extent, Chinese methods are more akin to what Michel Foucault portrayed as "societies of control," in which the traditional boundaries of institutionalized control are transgressed in favor of fluid and ethereal mechanisms that permeate the entire social fabric. These systems reach an end in targeting minorities, not only because they are a "potential threat" but because they are the "other" that undermines the narrative of national unity in the centralized state, and it is for this reason that symbolic and material violence is so widespread against these groups, in the name of protecting security and stability.[2]

3.3   The implications of the Chinese control system on security and individual freedoms

3.3.1   The effectiveness of Chinese control in promoting internal security and stability

Despite the controversy surrounding China's control systemone cannot refute the fact that this model has produced many positive effects of enhancing national security, deterring crime, and combating terrorism. Due to advances in facial recognition technology, behavioral analysis, and artificial intelligence, Chinese authorities have managed to enhance control over public space and monitor suspicious actions and activity so that they can achieve tangible results

---

[1]Buzan, Barry, Ole Wæver, and Jaap de Wilde. Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers, 1998, p. 25.

[2] Foucault, Michel. Discipline and Punish, op. cit., pp. 209-221.

in the realm of internal security.

An example is the city of Guiyang, where the rollout of facial recognition technology has enabled the police to identify and arrest suspects within minutes[1]. This ability to respond rapidly has greatly enhanced the effectiveness of urban policing programs.

In Xinjiang, the Integrated Joint Operations Platform (IJOP) collects data from various sources, including closed-circuit television footage, biometric data, and online activities, to identify prospective security challenges[2]. This predictive policing approach allows the authorities to foresee risks, thus lowering the incidence of violent incidents.

Furthermore, the network-based social management software separates communities. into smaller units, each of which is governed by appointed officers[3]. This local control provides for the real-time reporting of suspicious behavior and improves safety rules for the community.

Together, these measures contribute to a comprehensive security system that has proven effective in reducing criminal behavior and preventing terrorist acts. However, the widespread proliferation of control has also raised concerns about privacy and civil liberties, highlighting the the need for a balanced approach that protects both security and individual freedoms.[4]

3.3.2 Effects of control on Individual Freedoms in China

China is the country with the most advanced and widespread control system, which has been built over the past two decades. The establishment of a massive control system in China has had a profound impact on personal

---

[1]Business Insider, "China's City Guiyang Using Facial Recognition to Arrest Criminals," businessinsider.com, accessed May 16, 2025, 15:30, https://www.businessinsider.com/china-guiyang-using-facial-recognition-to-arrest-criminals-2018-3.

[2]Human Rights Watch, "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," hrw.org, accessed May 16, 2025, 15:45, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

[3]The Diplomat. (2021). China's Paper Tiger Surveillance State. Retrieved May 16, 2025, 16:00, from https://thediplomat.com/2021/04/chinas-paper-tiger-surveillance-state/

[4]ibid.,May 16, 2025, 16:15

freedoms, fundamentally changing the relationship between the state and citizens. The widespread adoption of technologies such as facial recognition, data control, and biometric identification has had an enormous impact in making China a country where personal privacy is greatly diminished. While the government justifies this system as necessary to maintain security and social order, the potential long-term effects on individual freedoms are significant and troubling.

One of the biggest implications of China's control state is the loss of personal privacy. Citizens' activities, including their movements, online behavior, and even their facial expressions, are being constantly tracked using a variety of sophisticated control technologies.[1] Thus, individuals are deprived of freedom of action or movement without the fear of being under control. Such pervasive control has a chilling effect, wherein individuals are compelled to change their habits, limit their social interactions, and even their linguistic expression to escape control or punitive action. Essentially, the prospect of imminent threat in the form of control serves as an instrument of social control, wherein individuals engage in self-censorship of behavior to adhere to government-sanctioned norms. [2]

In addition, the extensive use of control by the Chinese government goes beyond mere observation, extending into the area of behavior control through such tools as the Social Credit System. It ties individual behavior with rewards and punishment, such as loans, travel grants, or job opportunities. Those who engage in behavior not approved of by the state may endure social sanctions like restricted access to state facilities or deprivation of social status. This institutes a social atmosphere where conformation to state values is encouraged and opposition or nonconformity warrants material sanctions. The fear of social exclusion or reprisal for expressing independent opinions or independent

---

[1] Lee, C.S. "Datafication, dataveillance, and the social credit system as China's new normal." Online Information Review 43, no. 6 (2019): 952Ű970.

[2] Creemers, Rogier. "China's Social Credit System, op. cit.p. 25-27

actions precludes public discussion and dissuades individuals from engaging in political or social activities that could counter existing norms.[1]

Furthermore, the overall ubiquity of control across China has made it virtually impossible for individuals to conduct personal or private activities without worrying about being observed or scrutinized. The constant control, online and offline, intrudes into fundamental rights under the freedom of expression and association. Individuals are apprehensive about expressing themselves, especially opinions of dissent against governments, due to concern about using control technology for monitoring and retaliating against their actions.

A lot of the AI involved in the Chinese control state is similarly deceptive. Chinese state media is full of stories of lost children being found through facial recognition that turn out to be exaggerated or completely made up. But in a sense, it does not matter. What matters for the Communist Party is that people "believe" the technology works. It's the same dynamic that the British social theorist Jeremy Bentham famously exploited in creating the panopticon, a circular prison based on designs that his brother conjured while working on one of Potemkin's villages. The guard in the central tower can only watch so many prisoners at any given time, but the building is designed in such a way that every prisoner has to assume he or she is being watched all the time.[2]

The deployment of control technology thus not only disables the exercise of personal liberties but also encourages an environment of fear, wherein persons are discouraged from engaging in meaningful discourse or even carrying out deeds that will be interpreted as non-conformist

---

[1] Ibid., pp. 25-27

[2] Jacob Fromer, "Surveillance State: Social Control in China," The Diplomat, October 7, 2022, available at: https://thediplomat.com/2022/10/surveillance-state-social-control-in-china/, accessed on May 10, 2025.

3.3.3   A Comprehensive Evaluation of China's Experience

The Chinese society of control model has brought about a paradoxical condition under which security is increased through methods that simultaneously erode the same freedoms that they claim to protect. Through deploying an omnipresent control apparatus-comprising facial recognition technology, online control, pre-crime algorithmic policing, and neighborhood control networks-the state has succeeded in establishing what can be termed "stability through submission." Although the strategy has managed to quell popular dissent and deal with perceived separatist threats, it has rolled back individual rights drastically, particularly in regions like Xinjiang and Tibet where populations are dealt with en masse as security threats.[1]

This system is premised on a preemptive repression rationality: individuals are not merely monitored for what they do, but also for what they can be expected to do, as predicted by profiling and data analysis. As such, cultural, religious, or political difference is used as an indicator of risk instead of as a right to be protected. The freezing effect on public life is profound-citizens internalize the state's control, with resultant self-censorship and dissolution of community trust. This situation illustrates the tension between collective security and individual freedom, and raises pressing ethical questions about the cost of technological rule in authoritarian states.[2]

Here, the control of the state over its people has reached new heights, as technological advancement is being used not just to observe conduct but also to influence it actively. The outcome is a society where individual freedoms are sacrificed in the name of national security and social order. This shift raises important questions about the balance between security policies and citizens' rights, and the legitimacy of such trade-offs in the context of China's political and social climate.

---

[1]Lyon, David. The Culture of Surveillance: Watching as a Way of Life. Cambridge: Polity Press, 2018, pp. 89-92.

[2]Baylis, John, Patricia Owens, and Steve Smith. The Globalization of World Politics, 8th ed., p. 574.

China's approach to control and control is not unique, as many countries grapple with similar challenges in the face of terrorism and cybercrime.[1] However, the scale and scope of China's control apparatus, combined with its authoritarian political system, raise particular concerns. The export of Chinese control technology to other countries, particularly in Africa, raises further questions about the global spread of digital authoritarianism.[2] The Chinese control industry has exported its products to dozens of countries on every continent except Australia and Antarctica, including the software and hardware it uses in its control system, overseas; in some cases, the Chinese government provides training to foreign police forces on how to use the systems they purchase. These tools make it easier for authoritarian leaders to stay in power. In countries where democratic institutions are weak, incumbent leaders can use them to set up de facto authoritarian regimes under the guise of fighting crime-as Yoweri Museveni did in Uganda using a control system purchased from Chinese tech giant Huawei.[3] ăă

China's success in exporting its control hardware and software has laid the foundations for a lucrative 150 billion dollars industry but with hidden, insidious consequences for free and open societies. China has taken the authoritarian model employed at home and exported it to governments that are likely to use it with increasingly nefarious intentions. As such, the Chinese Communist Party has become a significant actor in securitization programs abroad that include the full-spectrum control of citizen and society. Not only does China occupy a unique position, setting a new standard in the field of control and security, it is reshaping the global debate on security, (democratic) freedom, and openness, and rewriting the rules while championing new norms.[4]

---

[1]Tariqul Islam, Implications of Anti-Terrorism Law on Civil Liberties: A Human Rights Perspective in Bangladesh

[2]Digital Neocolonialism: The Chinese Surveillance State in Africa

[3]Fromer, Jacob. Surveillance State, op. cit. accessed on May 10, 2025

[4] Scott N. Romaniuk and Tobias Burgers, "How ChinaŠs AI Technology Exports Are Seeding Surveillance Societies Globally," The Diplomat, October 18, 2018, available at: https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/, accessed on May 10, 2025.

The challenge to advanced democracies, particularly amid the global democratic recession, is immense. China offers a clear vision for how states should make use of these technologies. Democracies, meanwhile, are struggling to put forth an alternative. The European Union has clearly decided to put privacy first and is considering an outright ban on real-time digital control. But the U.S. is mired in confusion, with individual states adopting a grab bag of approaches. Americans helped create the global market for digital control with the War on Terror. Where things go from here likely depends on their willingness to confront this latest evolution in tracking technologies.[1]

Partial Conclusion

China's comprehensive control system is a unique model that reflects the tension between security and individual freedom and illustrates the complex and often uncomfortable intersection between technological progress and authoritarian control. Through ideological legitimacy, expanded legal authority, and sophisticated control tools, while China presents this control as a tool to ensure public security and protect political stability, control practices indicate a significant curtailment of individual freedoms. The Chinese state has created a system in which the boundaries between security and repression have become increasingly blurred. Despite tangible security outcomes, such as reducing crime and controlling opposition political movements, the implications for individual freedoms that extend to privacy, expression, and civil society in all walks of life.

Instead of a balance between protection of rights and security, the Chinese model prioritizes state control over freedom. The control machine, while effective in maintaining populations in line and dissenters in check, is an inherent issue on both the ethical and legal fronts. Ordinary control as an omnipresent fact affects Chinese citizens inwardly, but establishes a precedent

---

[1]ibid

that other countries would attempt to emulate although China has faced constant criticism over human rights issues and restrictions on freedoms.

This argument, in tandem with China's exports, is conducive to a framework that could motivate other nations to follow China's governance models and security practices. Ultimately, such a framework may also lead to the growing idea in the global governance debate, among states, that ChinaŠs philosophy of power could be the leading model for future developments in control and security.

Conclusion

Conclusion

The society of control has become a hallmark of the modern digital age, as countries seek to utilize advanced technology to ensure national security and combat contemporary threats. A moment's reflection on the nature of the technological society we live in today makes us realize that Bentham's dream has finally come true. Power now sees almost everything, watches everywhere, at all times, and does so unseen, because it is invisible, hidden behind glass lenses, smart chips or credit cards. Today, we do not see large numbers of police on our streets, nor do we see the structures of prisons and barracks in the center of the city as before, but even though the authority has withdrawn from our daily field of vision, we know for sure that we are under its constant control; in the streets, shops, malls, banks, hospitals, schools, hotels, public transportation stations, stadiums, parks, apartment complexes, and even in our homes. Here Foucault's prophecy is also realized: We are forced to conform to an authority that we do not see but believe it exists.

The main feature of the contemporary society of control is its elaborate infrastructure. It consists of a large variety of technologies that, taken together, transform it into a new form of panopticism. The types of contemporary control range from the more rudimentary type of visual observation and recording of information, to the more complex types of genetic testing and biostatistical analysis. These control technologies are divided into those that we can see and recognize and thus know that we are under control and those that operate covertly through the data collected by the various technologies we use in our daily lives. The development of electronic control technologies has provided

the authorities with a way to transform society into a kind of "Big Panopticon." The authorities can now monitor all places and at all times, and increase their ability to anticipate risks and threats through the information provided by these technologies. Surveillance technologies contribute significantly to modifying social behavior and act as a form of social engineering by enacting norms of acceptable and unacceptable behavior

Despite the effectiveness of control tools in tracking suspicious activities and responding quickly to threats, this development carries with it a real threat to individual freedoms, especially the right to privacy and freedom of expression. Nash equilibrium theory has been employed to explain how, under the pressure of constant control, individuals rationally and strategically modify their behavior, not out of morality, but out of fear of consequences. Discipline is imposed, not by conviction, but by a collective terror equation that ensures compliance at the expense of authenticity.

Here we find ourselves facing an old philosophical question: Is man inherently good or evil? So that we can know whether he deserves to be monitored to restrain him or whether he deserves trust and freedom. Returning to Thomas Hobbes as a pessimistic realist, he describes man as an inherently selfish and harmful being, and that only a strong state, represented by a society of control, can curb this evil and control his behavior. On the other hand, liberal thinkers, led by John Locke, defend the optimistic image of man as inherently good and deserving of trust and freedom away from the state.

Between these two visions, the security and ethical dilemma emerges, which is represented in the dialectical relationship between achieving security and protecting individual freedoms and trying to strike a balance between them, i.e. do we adopt a society based on doubt and fear or do we risk trust and bear the consequences?

Achieving a true balance between the requirements of security and individual rights is not easy. It often favors the security authority over

the individual, especially in regimes that lack democratic oversight and independent institutions. With increasing reliance on algorithms and artificial intelligence, control becomes more expansive and less transparent, making it harder to hold those in control accountable. This is where the Nash equilibrium comes into play as a strategic dilemma arises due to the mutual distrust between the two parties. As a result, each party adopts a strategy that protects it from the worst possible scenarios, rather than seeking a common optimal outcome.

Building a society that balances security and freedoms requires a strict legal framework, independent oversight, and informed community participation. Surveillance is not an issue in and of itself, but rather the absence of boundaries and standards that ensure that security is not used as a pretext to abolish freedoms. Without this balance, the society of control becomes a tool of control rather than a means of protection.

The American and Chinese examples highlight two contrasting tendencies in the ways that states are reacting to the balance between security and freedom in a control regime. While China demonstrates an exemplar of an authoritarian state deploying ubiquitous and systematic observation as a tool of political and social control, thanks to advanced technologies such as facial recognition and social credit,. The state has succeeded, on the whole, in imposing "stability," but one of mounting restriction of individual freedom and privacy, which is a profound moral and political issue.

On the other hand, the United States of America is a liberal democracy but none the less has its shortcomings. In the wake of 9/11, home control programs such as the NSA's PRISM program expanded manifold, resulting in mass controversy over privacy violations and executive power abuse, despite the existence of oversight and judicial checks. Individual freedoms there, nonetheless, continue to be subject to public scrutiny and answerability, indicating a recurring tension between security demands and democratic ideals.

Both experiences highlight that no state is exempt from the political and

ethical challenge that comes with the society of control, and that whether censorship exists or not is not what distinguishes one regime from another, but the legal limits, openness, and accountability procedures that go with it. While regimes are moving towards "coercive security" in some, other regimes are actively pursuing "democratic security," a precarious balance that requires constant watchful eyes from society and a new legal order that accommodates technological change without upsetting the character of freedoms.

Bibliography

[1] Bentham, Jeremy. The Panopticon Writings. Verso, 1995.

[2] Booth, Ken. Theory of World Security. Cambridge University Press, 2007.

[3] Brady, Anne-Marie. Marketing Dictatorship: Propaganda and Thought Work in Contemporary China. Rowman & Littlefield, 2008.

[4] Bull, Hedley. The Anarchical Society: A Study of Order in World Politics. Columbia University Press, 1977.

[5] Barry, Buzan. People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. ECPR Press, 2008.

[6] Barry, Buzan. People, States and Fear. Harvester Wheatsheaf, 1991.

[7] Brayne,Sarah. Predict and Surveil: Data, Discretion, and the Future of Policing, Oxford University Press, 2020.

[8] Creemers, Rogier. China's Social Credit System: An Evolving Practice of Control. SSRN, 2018.

[9] Deibert, Ronald. Reset: Reclaiming the Internet for Civil Society. House of Anansi, 2020.

[10] Dikötter, Frank. The Cultural Revolution: A People's History, 1962Ű1976. Bloomsbury, 2016.

[11] Edkins, Jenny and Vaughan-Williams, Nick. In Baylis et al., The Globalization of World Politics. Oxford University Press, 2009.

[12] Foucault, Michel. Discipline and Punish: The Birth of the Prison. Vintage Books, 1977.

[13] Foucault, Michel. Surveiller et punir: Naissance de la prison. Gallimard, 1975.

[14] Habermas, Jürgen. The Structural Transformation of the Public Sphere. MIT Press, 1991.

[15] Hansen, Lene. Security as Practice: Discourse Analysis and the Bosnian War. Routledge, 2000.

[16] Herz, John H. International Politics in the Atomic Age. Columbia University Press, 1959.

[17] Holsti, Kalevi Jaakko. International Politics: A Framework for Analysis. Prentice Hall, 7th ed.

[18] Kissinger, Henry. Diplomacy. Simon & Schuster, 1994.

[19] Kupchan, Charles. The Vulnerability of Empire. Cornell University Press, 1994.

[20] Lyon,David. Surveillance After Snowden, Polity Press, 2015

[21] Lyon, David. Surveillance Society: Monitoring Everyday Life. Open University Press, 2001.

[22] Lyon, David. The Electronic Eye: The Rise of Surveillance Society. University of Minnesota Press, 1994.

[23] Lyon, David. The Culture of Surveillance: Watching as a Way of Life. Polity Press, 2018.

[24] MacKinnon, Rebecca. Consent of the Networked: The Worldwide Struggle for Internet Freedom. Basic Books, 2012.

[25] McNamara, Robert. The Essence of Security. Harper and Row, 1968.

[26] Mill, John Stuart. On Liberty. Penguin Books, 1859.

[27] Morgenthau, Hans Joachim. Politics Among Nations: The Struggle for Power and Peace. Knopf, 1948.

[28] Osborne, Martin. J. & Rubinstein, Ariel. A Course in Game Theory. MIT Press, 1994.

[29] Parkinson, Cyril. Northcote. The Law and the Profits. John Murray, 1957.

[30] Rawls, John. Political Liberalism. Columbia University Press, 1993.

[31] Schneider, Florian. China's Digital Nationalism. Oxford University Press, 2018.

[32] Solove, Daniel J. The Digital Person: Technology and Privacy in the Information Age. NYU Press, 2004.

[33] Zuboff, Shoshana. The Age of Surveillance Capitalism. PublicAffairs, 2019.

Graduation Thesis:

[34] Sezal, M. Origins of Differentiation in Critical Security Schools: A Philosophic-Genealogical Search for Emancipatory Roots. Master's Thesis, University of Groningen, 2019.

Scientific articles

[35] Abdul-Wahab, Kayyali. Zionism and Imperialism: The Historical Origins. Journal of Palestine Studies, Vol. 6, No. 3 (Spring 1977), pp. 98-112.

[36] Baldwin, David. "The Concept of Security." Review of International Studies, 1997.

[37] Bigo, Didier. "Security and Immigration." Alternatives: Global, Local, Political, 2002.

[38] Bigo, Didier. "Globalized (In)Security." International Political Sociology, 2008.

[39] Bigo, Didier. "When Two Become One..." In International Relations Theory and European Security, 2000.

[40] Deleuze, Gilles. "Postscript on the Societies of Control." October, 1992.

[41] Ferguson, N. M. et al. "Impact of Non-Pharmaceutical Interventions (NPIs)." Nature Medicine, 2020.

[42] Haggerty, Kevin. "Tear Down the Walls: On Demolishing the Panopticon." Theoretical Criminology, 2006.

[43] Okolie, Ugo C. "Distinction between Traditional and Modern Security." Journal of Administrative Science, 2022.

[44] Ullman, Richard H. "Redefining Security." International Security, 1983.

[45] Yesil, Bilge. "Modern Surveillance and the Panopticon." New Media and Society, 2009.

Online resources, reports and lectures:

[46] AiThor. Individual Freedoms and National Security Essay. [https://aithor.com]

[47] Amnesty International. Surveillance and Political Repression. 2022.

[48] Baylis, Smith & Owens. The Globalization of World Politics. 7th & 8th editions.

[49] Business Insider. "China's City Guiyang Using Facial Recognition", 2018.

[50] Cambridge University. "Monitoring Mental Health." 2023. [https://www.cambridge.org]

[51] Data4Change. Self-Censorship Research, 2025.

[52] E-International Relations. Justifying Surveillance, 2015.

[53] Freedom House. Freedom on the Net 2023.

[54] Fromer, Jacob. "Surveillance State in China.." The Diplomat, 2022.

[55] Human Rights Watch. China's Algorithms of Repression. 2017Ű2021.

[56] LinkedIn. Articles by Hamza and Natakwa. 2023Ű2024.

[57] Porter, Jon. "Apple Closes Chinese App Store Loophole." The Verge, 2020.

[58] Privacy International. Briefing on the Data Protection Bill, 2017.

[59] RIWI & Data4Change. Self-Censorship on Social Media, 2025.

[60] Romaniuk, Scott N. and Burgers, Tobias. "China's AI Technology Export." The Diplomat, 2018.

[61] UN Security Council. Terrorism Prevention Report, 2021.

[62] OpenStax. Introduction to Political Science. Rice University, 2022.

List of Figures

Contents

Abstract:
This study deals with the theme of the society of control by highlighting its important and effective role It aims to understand and analyze the dialectical relationship between security requirements and the violation of individual freedoms in the context of control societies as an emerging paradigm that redefines the relationship between them. Taking China as a case study as an advanced example in the application of control systems and how the technological development used in China that relies on artificial intelligence and facial recognition technology has contributed to enhancing social and political security in the country. Although these technologies contribute to achieving security, they raise many questions about their impact on individual freedoms and privacy. This paper highlights the difficulties and challenges faced by governments, especially in China, in striking a balance between ensuring security and protecting individual freedoms in the age of digitization, using the frameworks of Michel Foucault's Panopticon theory and Deleuze's society of control theory to understand how control has become a tool of control at the expense of individual freedoms.

Keywords: Artificial Intelligence; Individual Freedoms; Nash Equilibrium; Panopticon; Society Of Control; Surveillance Society.

Résumé
Cette étude aborde le thème de la société de contrôle en soulignant son rôle important et efficace Elle vise à comprendre et à analyser la relation dialectique entre les exigences de sécurité et la violation des libertés individuelles dans le contexte des sociétés de contrôle en tant que paradigme émergent qui redéfinit la relation entre les deux. En prenant la Chine comme étude de cas, comme exemple avancé de l'application des systèmes de contrôle et de la manière dont le développement technologique utilisé en Chine, qui repose sur l'intelligence artificielle et la technologie de reconnaissance faciale, a contribué à renforcer la sécurité sociale et politique dans le pays, bien que ces technologies contribuent à assurer la sécurité, elles soulèvent de nombreuses questions quant à leur impact sur les libertés individuelles et la protection de la vie privée. Cet mémoire met en lumière les difficultés et les défis auxquels sont confrontés les gouvernements, en particulier en Chine, pour trouver un équilibre entre la garantie de la sécurité et la protection des libertés individuelles à l'ère de la numérisation, en s'appuyant sur la théorie du panopticon de Michel Foucault et sur la théorie de la société de surveillance de Deleuze pour comprendre comment la surveillance est devenue un outil de contrôle au détriment des libertés individuelles.

ملخص:

تتناول هذه الدراسة موضوع مجتمع المراقبة من خلال تسليط الضوء على دوره الهام والفعال وتهدف إلى فهم وتحليل العلاقة الجدلية بين متطلبات الأمن وانتهاك الحريات الفردية في سياق مجتمعات المراقبة باعتبارها نموذج يعيد تعريف العلاقة بينهما. بأخذ الصين كمثال متقدم في تطبيق أنظمة المراقبة، وكيف ان الدولة الصينية تعتمد بشكل متزايد على الذكاء الاصطناعي وتقنيات التعرف على الوجه لتعزيز الأمن الاجتماعي والسياسي في البلاد. و على الرغم من أن هذه التقنيات تساهم في تحقيق الأمن، إلا أنها تثير العديد من التساؤلات حول تأثيرها على الحريات الفردية والخصوصية. تسلط هذه الدراسة الضوء على الصعوبات والتحديات التي تواجهها الحكومات، خاصة الصين في محاولة تحقيق التوازن بين ضمان الأمن و حماية الحريات الفردية في عصر الرقمنة، ، مستندة في تحليلها إلى أطر نظرية البانوبتيكون لميشيل فوكو ونظرية مجتمع المراقبة لجيل دلوز لفهم كيف أصبحت المراقبة أداة للسيطرة على حساب الحريات الفردية.

كلمات مفتاحية: البانوبتيكون؛ الحريات الفردية؛ الذكاء الاصطناعي؛ توازن ناش؛ مجتمع السيطرة؛ مجتمع المراقبة.