LUISS

Department of Political Science

Bachelor's Degree in Politics: Philosophy and Economics

Course of International Relations

Surveillance Technologies in Egypt and Saudi Arabia: From Domestic Control to Geopolitical Leverage

Raffaele Marchetti
SUPERVISOR

Martina Lucaccini
COSUPERVISOR

Gaia Mancini ID: 103462
CANDIDATE

Academic Year 2024/2025

Table of Contents

Abstract

Digital technologies have reshaped contemporary state power in authoritarian contexts where surveillance tools are critical control instruments. This thesis examines the strategic use of digital surveillance technologies by authoritarian regimes in the Middle East and North Africa, with a focused comparative analysis of Egypt and Saudi Arabia. It explores how these regimes harness advanced technologies to maintain domestic political repression and enhance their geopolitical influence through strengthened economic and technological partnerships with global powers such as the United States and China. The central research question investigates how surveillance investments function as both internal governance tools and international diplomacy assets. The thesis formulates hypotheses linking higher surveillance technology adoption to deeper bilateral cooperation in technological and economic spheres. This dual surveillance role reflects a complex recalibration of authoritarian power within the digital age. Employing a comparative quantitative approach, the study integrates data sources on political freedom and internet censorship indices, specialised digital repression measures, and international technology cooperation records. The analysis leverages datasets such as the Varieties of Democracy project, Freedom House reports, Steven Feldstein's Digital Repression Index, and AidData's investment tracking, enabling a rigorous assessment of surveillance's impact on domestic and foreign policy dynamics. Findings demonstrate a significant correlation between increased surveillance infrastructure and enhanced partnerships with prominent global actors. In Egypt, surveillance technology cooperation is a key component of its longstanding strategic partnership with the United States, enabling access to advanced tools supporting regime stability and regional security interests. Saudi Arabia has expanded its international partnerships by incorporating Chinese surveillance technologies within its Vision 2030 modernisation framework, reflecting its growing engagement with China's Belt and Road Initiative and a broader diversification of geopolitical alliances. This dual-use surveillance paradigm—as a mechanism of repression and as diplomatic capital—illustrates an authoritarian adaptation to the digital era, wherein control over data and information flows is pivotal for domestic legitimacy and international strategic positioning. The thesis further highlights the broader implications for global governance, emphasising the challenges digital authoritarianism poses to human rights, sovereignty, and international stability. Ultimately, the research contributes to a nuanced understanding of how digital surveillance technologies shape authoritarian governance and geopolitics in the MENA region. It calls for urgent international coordination to regulate surveillance technology exports, promote corporate accountability, and safeguard digital rights.

Introduction

The pervasive diffusion of digital technologies in recent decades has profoundly transformed mechanisms of power and control worldwide, challenging traditional governance paradigms. While digital tools offer the potential to enhance transparency and civic participation, they have also become central to the evolution of authoritarian control, particularly through sophisticated surveillance systems. These systems, leveraging artificial intelligence, biometrics, spyware, and big data analytics, enable states to monitor populations with unprecedented precision and scale, reshaping the landscape of political repression.

This thesis investigates the role of digital surveillance in authoritarian regimes of the Middle East and North Africa (MENA), focusing specifically on Egypt and Saudi Arabia. It explores how digital surveillance functions not only as a domestic instrument of political repression and social control but also as a strategic asset intertwined with broader geopolitical and economic relations. The research highlights the dual dimension of digital authoritarianism by analyzing how surveillance infrastructure investments align with international cooperation, especially involving global powers such as the United States and China. The study is organized into three chapters, each building a comprehensive understanding of the subject matter.

Chapter 1 provides a detailed literature review and theoretical framework. It traces the historical evolution of surveillance, from analogic and human-centered methods like informant networks and wiretapping to digital techniques based on automated data collection, AI-driven analytics, and biometric identification. This chapter examines key concepts of digital authoritarianism, detailing the "digital authoritarian toolkit" and the intelligence frameworks prevalent in authoritarian regimes. Furthermore, it engages with ongoing debates around cyber-optimism and cyber-pessimism, while situating surveillance politics within the MENA region. Special attention is devoted to the legacies of post-colonial intelligence services, the role of surveillance in governance in Arab authoritarian states, and the transformation of surveillance practices in the post-Arab Spring context, characterized by intensified geopolitical entanglements and internal control mechanisms.

Chapter 2 outlines the research design, including the formulation of hypotheses and methodological approaches. It clarifies the scope of the study and describes the data sources and analytical tools used to explore the relationship between surveillance capabilities and international cooperation.

Chapter 3 presents a comparative empirical analysis of Egypt and Saudi Arabia's surveillance systems. It evaluates political freedom and internet freedom indicators alongside data on digital

repression and bilateral cooperation, investigating correlations between surveillance investments and partnerships with the United States and China. This analysis reveals how digital surveillance operates as diplomatic capital that regimes leverage to consolidate international support and economic advantages, linking domestic authoritarian control with global strategic positioning.

The conclusion synthesizes the research findings, emphasizing the dual role of surveillance technologies as instruments of internal repression and international diplomacy. It highlights the urgent need for robust global regulatory frameworks and coordinated policies to address the human rights implications and geopolitical consequences of digital authoritarianism. By integrating theoretical insights with empirical evidence, this thesis contributes a nuanced perspective on the evolving dynamics of authoritarian governance, technology deployment, and international relations in the digital era.

Chapter 1 – Literature Review

Introduction

The rapid advancement of digital technology has not only transformed everyday life but also redefined how states exert power and control. Around the world, governments are increasingly using digital tools to monitor, manipulate, and suppress dissent—a phenomenon widely known as digital repression. This growing reliance on technologies such as big data analytics, artificial intelligence (AI), and surveillance software marks a pivotal shift in how authoritarian regimes consolidate their pillars of stability and manage civil society.

The first chapter of the thesis explores the evolution of digital surveillance, its role in authoritarian governance, and its specific manifestations within the Middle East and North Africa (MENA) region. It highlights how technological advancements, geopolitical alliances, and post-colonial legacies have entrenched digital surveillance as a core instrument of state power. The review is organized into three main sections sections.

The first section examines the historical shift from traditional analogic and traditional surveillance methods to advanced digital systems powered by AI, spyware, and biometric technologies. It investigates how these tools have rendered surveillance more pervasive and predictive, allowing states to monitor dissent, influence online discourse, and preempt social unrest.

The second section delves into digital authoritarianism, analyzing how regimes strategically deploy surveillance technologies to reinforce repression, control narratives, and suppress civil liberties. It also engages with the broader theoretical debate between cyber-optimism and cyber-pessimism, addressing the paradox of digital tools as both instruments of liberation and control. This section places the MENA region in the context of global trends in digital repression, examining how authoritarian governments utilize technological developments for both domestic surveillance and transnational suppression influence.

The third section further contextualizes these themes within the MENA region, where digital surveillance is deeply intertwined with post-colonial intelligence practices, geopolitical alliances, and regional power dynamics. This section explores how regimes like Saudi Arabia, Egypt, Syria, and the UAE have updated their intelligence systems—often receiving technological assistance from global powers such as the United States, China, and Russia—to enhance their digital capabilities and stifle dissent within their territorial borders.

This analysis draws from key scholarship and well-established literature on digital repression and authoritarian control. In The Rise of Digital Repression, Steven Feldstein (2021) offers a comprehensive account of how governments globally exploit digital tools to suppress dissent and maintain power, with case studies spanning from China to the Middle East. Anita R. Gohdes, in Repression in the Digital Age (2023), focuses on the mechanics of online surveillance and censorship, illustrating how authoritarian regimes leverage digital platforms for social control and predictive policing. Both authors underscore the dual-use nature of digital technologies, which concurrently empower activists while also enabling state repression.

In Authoritarianism in an Age of Democratization (2007), Jason Brownlee provides a broader theoretical lens on how authoritarian regimes adapt to democratization challenges through digital means, highlighting the historical continuity from Cold War-era intelligence practices to modern digital repression strategies. In addition, Edward Snowden, in Permanent Record (2019), offers a firsthand account of how digital surveillance programs, such as PRISM, have been deployed by democratic states to monitor populations under the pretext of national security.

Within the MENA region, Marc Owen Jones, in his book Digital Authoritarianism in the Middle East (2022), explores how Gulf states and other authoritarian regimes exploit digital technologies for propaganda, disinformation, and transnational repression. In Authoritarianism in an Age of Democratization (2007), Jason Brownlee provides a broader theoretical lens on how authoritarian regimes adapt to democratization challenges through digital means. At the same time, Leila Hudson, in The Political Economy of Surveillance in the Middle East (2017), situates digital surveillance within the region's economic and geopolitical context, linking technological investments to political repression. The literature review also relies on reports published by Human Rights Watch in the years 2023 and 2024 to further illustrate these dynamics with concrete evidence examples.

Together, these studies and reports form a comprehensive framework for understanding digital repression’s global and regional dimensions. They illustrate how digital technologies, heralded initially as tools for democratization and civic empowerment, have increasingly been weaponized by authoritarian regimes to extend state power and suppress civil liberties.

By integrating global and regional perspectives, this chapter highlights how the intersection of technology, state power, and civil rights defines the evolving landscape of digital repression, with particular attention to its implications in the MENA region.

1. Digital Surveillance

Surveillance has long been a central tool of state power, evolving from traditional analog methods to sophisticated digital systems that significantly expand the scope and efficiency of monitoring practices. Traditional surveillance, refers to the pre-digital strategies employed by states to observe, control, and regulate populations. It is often characterized by pre-digital practices such as physical observation, informant networks, and wiretapping. While these approaches were effective in maintaining state control, they were resource-intensive, geographically constrained, and limited in scale. Gohdes (2024) highlights that traditional surveillance heavily relied on human operatives and manual data collection, which restricted its adaptability and scope.

The rise of digital surveillance has eliminated many of these constraints. As outlined by Gohdes (2024), digital surveillance enables states to extend their reach into private spheres, monitoring online behaviours, social networks, and communications with unprecedented precision. Feldstein (2021) further notes that AI-driven systems now allow for proactive repression, utilising predictive algorithms to identify potential dissent before it materializes, fundamentally shifting the balance of power between states and citizens.

The following sections will first explore the historical evolution of surveillance, tracing its transition from analog methods to modern digital ecosystems, followed by an examination of the tools and technologies that underpin contemporary surveillance practices. Together, this structure will provide a framework for understanding how states have adapted surveillance strategies to strengthen control, manipulate information flows, and preempt dissent in the digital age.

1.1. The Historical Evolution of Surveillance

The history of surveillance reflects a continuous adaptation of technologies and strategies aimed at controlling populations and suppressing dissent. From analogic methods rooted in the 20th century to today's digital ecosystems, surveillance practices have evolved alongside technological advancements and global shifts in power dynamics.

Initially, surveillance systems relied on physical observation, informant networks, and analog technologies such as telephone wiretapping and closed-circuit television (CCTV) (Gohdes, 2024). The two World Wars and the Cold War era accelerated the development of state-controlled monitoring, as governments expanded their surveillance capabilities to manage

security threats and suppress political opposition. During the Cold War, surveillance became a geopolitical tool, with both democratic and authoritarian states adopting mass monitoring programs (Brownlee, 2007). In the United States, programs like COINTELPRO targeted civil rights movements, while in the Soviet Union, the KGB created one of the most extensive surveillance networks in history. The East German Stasi maintained European control through a vast network of informants and domestic spying. This period established surveillance as a central pillar of state security, reinforcing the link between intelligence operations and political control (Brownlee, 2007).

The digital revolution in the late 20th century marked a turning point, transforming surveillance from labor-intensive analog methods to automated digital systems (Feldstein, 2021). The rise of the internet, mobile communications, and digital databases enabled states to collect and process vast amounts of personal data. This shift was particularly evident after the September 11, 2001, attacks, which triggered a global expansion of digital surveillance under the pretext of counterterrorism (Zuboff, 2019). In the United States, the National Security Agency (NSA) developed extensive programs such as PRISM, which collected data from major technology companies, as revealed by Edward Snowden in 2013 (Snowden, 2019). Similar expansions occurred in the United Kingdom through GCHQ and within international alliances such as the Five Eyes, a global intelligence-sharing partnership.

Social media and digital platforms further expanded the scope of surveillance (Jones, 2022). Initially praised for empowering activism and civic engagement, these platforms quickly became tools for state control. Governments began to exploit social networks to monitor public opinion, track dissidents, and spread disinformation. During mass protests in Hong Kong, Iran, and Russia, authorities combined real-time social media surveillance with advanced AI tools to identify organizers and disrupt movements.

The rise of surveillance capitalism has further blurred the lines between state control and corporate data collection (Zuboff, 2019). Technology giants such as Google, Facebook, and Amazon accumulate vast amounts of user data, often accessible to governments through legal mandates or covert agreements. This private-sector involvement in data collection has created an ecosystem where digital footprints are continuously harvested, analyzed, and monetized. Companies like Palantir have developed predictive policing technologies law enforcement agencies use to profile individuals and communities, raising concerns about algorithmic bias and mass surveillance. In China, private firms such as Huawei and Hikvision provide the

technological backbone for state surveillance networks, demonstrating the convergence of commercial interests and authoritarian control (Zuboff, 2019).

The historical trajectory of surveillance technologies highlights how states continually adapt their methods to technological advancements while maintaining the same underlying objectives: control, suppression of dissent, and public perception management. From the analogic methods of the 20th century to the sophisticated digital ecosystems of today, surveillance has become more pervasive and less visible. The shift from physical to digital control has not replaced traditional methods but integrated them into a broader system (Zuboff, 2019). With advancements in surveillance technologies, their influence on state power and citizen behavior is crucial for comprehending contemporary governance and authoritarianism control.

1.2.Tools and Technologies in Digital Surveillance

Technological advancements have driven the evolution of surveillance methods, which have redefined state control in the digital era. Modern surveillance leverages advanced digital tools that enable real-time tracking, large-scale data collection, and algorithm-driven behavioral analysis, surpassing the limitations of earlier methods.

Artificial intelligence (AI) and big data analytics are central to modern digital surveillance, which empowers states to monitor, analyze, and predict social behavior with unprecedented precision. Jones (2022) describes how authoritarian regimes utilize machine-learning algorithms to analyze digital conversations, detect dissent through keyword patterns, and create behavioral profiles. These tools facilitate surveillance and support propaganda operations, amplifying state narratives on social media—a tactic Jones terms 'Journoganda' (Jones, 2022). Additionally, predictive policing models, driven by historical data, enable governments to anticipate and preempt opposition activities before they materialize, reinforcing control through preemptive measures. While AI and Big Data enable mass surveillance and predictive control, more invasive methods target individuals directly. Spyware, for example, has become a key instrument of digital repression. Feldstein (2021) highlights the role of Pegasus spyware, which infiltrates personal devices, granting access to private communications and encrypted messages. Amnesty International's Pegasus Project (2021) exposes the extensive use of this tool across the MENA region, where it has been deployed to target journalists, activists, and

political opponents, leading to harassment, arrests, and intimidation. Such technologies enable governments to surveil and suppress dissent without overt displays of force.

Social media monitoring and censorship are integral to digital repression, which refers to the use of digital technologies —such as AI-driven surveillance, content filtering, and internet shutdowns — to monitor, control, and suppress dissent. Gohdes (2024) documents Iran's suppression of the 2019 protests, where authorities combined AI-driven content filtering with targeted internet shutdowns to disrupt protest coordination and isolate activists. By mining social media data, the state identified and arrested protest leaders, preemptively dismantling networks of dissent.

Biometric surveillance further erodes anonymity by using unique physical and behavioral characteristics —such as facial features, fingerprints, iris patterns, and voice recognition—to identify and track individuals. This form of surveillance collects and stores biometric data through technologies like facial recognition cameras, fingerprint scanners, and iris scanners, enabling continuous monitoring in both public and private spaces. Feldstein (2021) reports that the UAE integrates biometric data, such as facial recognition and iris scans, into national identification systems and airport security, transforming routine interactions into opportunities for state monitoring. Jones (2022) highlights how Saudi Arabia uses biometric registration for Hajj pilgrims, presenting it as a logistical measure while enabling mass population tracking.

Digital surveillance extends beyond authoritarian regimes. Feldstein (2021) notes that democratic states such as the U.S. and E.U. members also deploy AI, big data, and biometrics for counterterrorism and public safety. However, concerns persist over the erosion of privacy, potential abuses of power, and the expansion of surveillance under the guise of security. This phenomenon is particularly pronounced in democracies led by illiberal leaders, where surveillance tools are often used to undermine dissent and consolidate power. Additionally, even stable democracies may resort to repressive measures during periods of internal unrest or regional tensions. For instance, India has frequently implemented regional internet shutdowns to curb protests and maintain public order, reflecting how democratic governments can adopt authoritarian-like tactics when managing domestic instability.

Egypt's post-Arab Spring crackdown is a prominent case illustrating digital repression. Gohdes (2024) details how the Egyptian government combined big data analytics, spyware, and social media surveillance to dismantle activist networks. Authorities mapped social connections using

predictive algorithms, which enabled preemptive arrests, effectively stifling opposition movements before they could organize. Digital surveillance technologies have equipped states with powerful tools to monitor, influence, and control populations, often under the pretext of security. However, their application frequently extends into repression and censorship.

2. Authoritarian Regimes

Authoritarianism has been a cornerstone of political science, offering a framework for understanding regimes that consolidate power by limiting political freedoms and suppressing dissent. In Authoritarian and Totalitarian Regimes (1975), Juan J. Linz provides foundational definition of authoritarianism, distinguishing it from both democratic governance and totalitarian rule. According to Linz, authoritarian regimes are characterized by limited political pluralism, where certain social and political groups may exist but are tightly controlled or coopted by the state to prevent meaningful opposition. Unlike totalitarian regimes that pursue overarching ideological goals, authoritarian systems typically operate without a guiding ideology, focusing instead on regime stability and power preservation. Linz further emphasizes that authoritarian regimes discourage mass political mobilization, fostering political apathy among citizens to reduce the risk of organized dissent. Power is often concentrated in the hands of a leader, military junta, or dominant party, with minimal institutional checks and balances, allowing for a centralization of authority that minimizes challenges to the regime.

However, the rise of digital technologies has profoundly transformed these dynamics. Oliver Schlumberger, in How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship (2023), argues that digital tools have expanded the reach and efficiency of authoritarian control, giving rise to what he terms "digital dictatorship." While the core principles of authoritarianism remain intact—power centralization and suppression of dissent—digital technologies have enhanced regimes' ability to control populations with unprecedented precision. Surveillance tools like AI-driven data analytics, social media monitoring, and predictive policing allow governments to track dissent in real-time, often preemptively neutralizing opposition before it materializes.

The following sections will explore the evolution and mechanics of digital authoritarianism. First, Digital Authoritarianism will examine how regimes use technology for social control. Next, The Digital Authoritarian Toolkit will detail the specific technologies employed, followed by Intelligence Framework in Authoritarian Regimes, which focuses on how intelligence agencies leverage these tools for repression. Finally, Cyber-Optimism and Cyber-Pessimism

will analyze the debate on whether technology fosters liberation or enhances authoritarian control, setting the stage for understanding the complex dynamics of power in the digital age.

2.1. Digital Authoritarianism

Digital authoritarianism is a form of governance in which states utilize digital tools—such as AI, big data, and surveillance technologies—to monitor, censor, and manipulate populations, often undermining civil liberties (Feldstein, 2021). Jones (2022) frames digital authoritarianism as a strategic system in which digital platforms become instruments for social control through techniques like algorithmic content moderation, predictive policing, and disinformation campaigns.

Governments worldwide have rapidly expanded their digital authoritarian strategies, creating a continuum of repression that extends beyond traditional autocracies. For instance, China has emerged as one of the most advanced digital authoritarian states, leveraging technology to monitor and regulate its population. The country's Social Credit System is a prime example of how AI and big data enforce compliance, assigning behavioral scores to citizens based on their financial transactions, social interactions, and online activity. Individuals with low scores face restrictions on travel, employment, and access to social services, effectively turning digital surveillance into an instrument of state discipline (Feldstein, 2021). In Xinjiang, the Chinese government has expanded its AI-driven surveillance networks to track and detain Uighur Muslims. Predictive policing models flag individuals for suspicious behaviour, often leading to arbitrary detentions and forced re-education. Facial recognition, biometric data collection, and real-time geolocation tracking have made it nearly impossible for targeted communities to evade government scrutiny, demonstrating how digital repression can be seamlessly integrated into everyday governance (Gohdes, 2024).

Iran and Russia have also implemented highly sophisticated models of digital repression, combining AI-driven censorship, disinformation campaigns, and internet control to suppress opposition. In Iran, the development of a domestic intranet, known as the National Information Network (NIN), allows authorities to monitor and filter online activity, isolating citizens from the global internet. This enables the state to control political discourse, block foreign media, and restrict encrypted communication services. In Russia, AI-driven surveillance and deep-packet inspection (DPI) technology allow authorities to identify and remove politically sensitive content in real time, ensuring that online discussions remain within state-approved

boundaries (Jones, 2022). The Kremlin has also been at the forefront of algorithmic disinformation, deploying troll farms, bot networks, and AI-generated propaganda to manipulate public opinion and undermine opposition movements. These tactics not only serve domestic political control but also function as a means of influencing foreign elections and destabilizing democratic institutions worldwide.

The private sector, preeminent technology companies, enables digital authoritarianism. According to Amnesty International (2022), tech giants often facilitate censorship and surveillance by selling advanced monitoring tools to authoritarian regimes. Feldstein (2021) critiques this ecosystem of surveillance capitalism, where profit motives align with state repression.

The increasing reliance on digital authoritarianism poses significant challenges to democratic norms, human rights, and the future of political participation. As more states adopt AI-driven governance, biometric surveillance, and predictive policing, the traditional boundaries between authoritarianism and democracy continue to blur. The global spread of digital repression raises urgent questions about who controls digital infrastructure, how surveillance technologies should be regulated, and what safeguards can be put in place to prevent abuse (Gohdes, 2024).

2.2. The Digital Authoritarian Toolkit

The toolkit employed by digital dictators encompasses a diverse array of technologies aimed at controlling domestic populations and engaging in strategic competition on the global stage. According to Yayboke and Brannen (2020), these tools can be broadly categorized into two primary functions: tools of repression and disruption, and tools for strategic competition among great powers.

At the core of this toolkit lies extensive surveillance. The proliferation of connected devices—smartphones, computers, and embedded sensors—provides regimes with a vast platform for data collection. The integration of artificial intelligence (AI) into surveillance systems has further expanded the reach and precision of state monitoring, enabling real-time tracking of perceived threats. China has become the world's leading exporter of surveillance technologies through its Digital Silk Road initiative, equipping authoritarian regimes in Africa, Asia, and Latin America with AI-powered facial recognition, biometric tracking, and smart city infrastructure, all aimed at tightening domestic control.

Cyberattacks and digital espionage form another critical component of the authoritarian playbook. States like Iran, North Korea, and Russia have developed sophisticated capabilities for hacking, phishing, ransomware, and malware attacks, often targeting democratic institutions and critical infrastructure. The availability of commercial spyware and the global black market for hacking tools have further democratized access to these capabilities, enabling even smaller states to engage in digital espionage and disruption.

Censorship has also evolved in the digital era, moving beyond traditional content blocking to sophisticated algorithmic filtering, social media manipulation, and data localization. Authoritarian regimes employ firewalls, keyword blacklisting, and network shutdowns to suppress dissent and control information flows. China's Great Firewall remains the most comprehensive example, but similar tactics—such as internet shutdowns and geofencing—are used globally, particularly during protests or elections. In 2019 alone, there were 213 recorded internet shutdowns across 33 countries.

Disinformation has become a potent tool for manipulating public opinion and destabilizing democratic systems. Authoritarian regimes deploy troll farms, bot networks, and AI-generated propaganda to spread false narratives, polarize societies, and erode trust in democratic institutions. Russia's interference in the 2016 U.S. presidential election showcased the disruptive power of coordinated disinformation campaigns. These tactics are not exclusive to authoritarian regimes; some democratic actors have also employed disinformation to sway public opinion or undermine opponents.

A more subtle but equally strategic component of the toolkit is the export of digital infrastructure. China, through its Belt and Road Initiative, has built 5G networks, undersea cables, and surveillance systems across Asia, Africa, and Latin America, effectively exporting its model of digital control. This infrastructure not only facilitates domestic repression in recipient countries but also extends China's geopolitical reach, providing potential backdoor access to global data flows.

Finally, authoritarian regimes advocate for alternative models of internet governance under the banner of "digital sovereignty." China and Russia, for example, promote policies that emphasize state control over internet ecosystems, challenging the open and decentralized nature of the global web. This approach encourages data localization, stricter cybersecurity laws, and new internet protocols that enhance state surveillance capabilities. Competing initiatives like China's Global Initiative on Data Security and the U.S.-led Clean Network highlight the growing fragmentation of the global internet into rival digital spheres.

In sum, the digital authoritarian toolkit represents a multifaceted strategy that blends surveillance, censorship, disinformation, cyberattacks, and strategic infrastructure development. Yayboke and Brannen (2020) warn that the accessibility of these tools has democratized repression, enabling a wide range of regimes to adopt sophisticated methods of control. Countering this growing threat requires coordinated international efforts to regulate technology exports, enforce global cybersecurity standards, and defend digital rights. Without such measures, the spread of authoritarian digital practices risks eroding democratic institutions and civil liberties worldwide.

2.3. Intelligence Framework in Authoritarian Regimes

As a core pillar of digital authoritarianism, intelligence agencies play a crucial role in sustaining political control. Unlike their democratic counterparts, these agencies are centralized and politicized, operating as direct extensions of state power with minimal accountability (Gohdes, 2024). Their activities leverage advanced digital tools, from spyware to mass surveillance, to suppress dissent and neutralize opposition both domestically and abroad.

A prime example is Pegasus spyware, developed by the Israeli NSO Group, which has become a symbol of digital repression. Amnesty International's Pegasus Project (2021) revealed how regimes in the MENA region used this tool to infiltrate smartphones, intercept encrypted communications, track real-time locations, and remotely activate microphones and cameras. Notably, Pegasus employs zero-click exploits, enabling surveillance without user interaction and bypassing even the most secure encryptions, such as those on WhatsApp and Signal. This technological sophistication fosters pervasive self-censorship, as activists, journalists, and dissidents become acutely aware that their private communications are vulnerable to interception.

The human impact of Pegasus is profound. Saudi authorities used it to surveil Omar Abdulaziz, a close associate of Jamal Khashoggi, monitoring their private conversations—a factor that contributed to the journalist's assassination. Similarly, UAE activist Ahmed Mansoor was targeted with Pegasus before being imprisoned for his online activism. In Morocco, journalist Omar Radi faced politically motivated charges, supported by evidence gathered through Pegasus surveillance. Amnesty International condemned these actions as egregious violations of privacy and press freedom, highlighting how spyware facilitates transnational repression by enabling regimes to silence dissenters beyond their borders. The scandal also spurred

international responses, including sanctions against NSO Group by the United States in 2021 and renewed calls for global regulation of spyware technologies.

Beyond targeted spyware, mass surveillance expands authoritarian control to entire populations. Using AI-driven sentiment analysis and real-time social media monitoring, regimes detect patterns of dissent and disrupt collective action before it materializes. During Iran's 2019 protests, authorities employed these tools to identify activists, track their online activities, and enforce selective internet shutdowns, crippling protest coordination (Gohdes, 2024). Similarly, during the Arab Spring, Egyptian and Bahraini intelligence agencies leveraged social media monitoring to identify and arrest protest organizers, preemptively dismantling activist networks.

This expansive reach is enabled by a centralized intelligence apparatus, where cyber units, law enforcement, and military forces collaborate seamlessly. Unlike democratic systems, which separate intelligence and policing functions, authoritarian regimes integrate them into a singular structure. China exemplifies this approach: the Ministry of State Security (MSS) coordinates with domestic police and cyber units, employing AI-powered facial recognition and internet monitoring to enforce ideological conformity and swiftly suppress dissent (Gohdes, 2024). This centralized model ensures that digital surveillance, predictive policing, and physical repression function as a unified mechanism of control. Authoritarian regimes' intelligence frameworks illustrate how digital technologies are fully embedded into state repression strategies. Tools like Pegasus and mass surveillance not only quash domestic dissent but also extend authoritarian power globally. The debate between those who view digital tools as liberating forces (i.e., cyber-optimism) and those who highlight their repressive potential (i.e., cyber-pessimism) remains central to understanding how technology shapes power in the digital age. The following section will explore this theme further.

2.4. Cyber-Optimism and Cyber-Pessimism

The rise of digital technology has introduced a fundamental paradox. While digital platforms offer unprecedented opportunities for political mobilization and free expression, they have also become powerful instruments of state surveillance, repression, and disinformation. This tension is often framed within the debate between cyber-optimism and cyber-pessimism. Cyber-optimists argue that digital tools empower civil society, facilitate activism, and provide alternative information channels, particularly in authoritarian contexts where traditional media are tightly controlled. Conversely, cyber-pessimists highlight how the same technologies that

enable activism can be weaponized by regimes to monitor, manipulate, and suppress dissent, often more effectively than ever before (Jones, 2022).

The role of social media and digital platforms in grassroots movements is one of the key arguments in favor of cyber-optimism. Platforms such as Twitter, Facebook, and Telegram have played a critical role in organizing protests, disseminating uncensored information, and exposing human rights violations. The Arab Spring provides a prominent example, where digital activism facilitated rapid mobilization, cross-border solidarity, and global visibility. Beyond social media coordination, activists have leveraged digital tools such as encrypted messaging apps and open-source intelligence (OSINT) platforms to document human rights abuses. For example, during the 2022 Iranian protests, platforms like Telegram and Signal were vital for sharing real-time updates and organizing flash protests while evading surveillance (Jones, 2022). OSINT efforts, such as geolocated videos of police brutality, provided crucial evidence for international human rights investigations, showcasing technology's power as a tool for truth and accountability.

However, this cyber-optimism is countered by a more sobering reality—authoritarian regimes have adapted quickly to the digital age, repurposing social media platforms as tools of repression rather than liberation. A striking example of this cyber-pessimistic reality is how regimes use AI-driven surveillance, predictive analytics, and social media monitoring to anticipate and crush opposition before it gains traction (Gohdes, 2024). State security agencies frequently monitor hashtags, infiltrate encrypted messaging groups, and deploy spyware to surveil activists (Amnesty International, 2021). The same digital platforms that facilitated uprisings have now become sites of state-controlled manipulation, where opposition voices are drowned out by pro-regime narratives amplified through bot networks and state-sponsored disinformation campaigns (Jones, 2022).

The weaponization of state-controlled digital armies has further reinforced the cyber-pessimist perspective. In countries such as Saudi Arabia and the UAE, social media platforms have been flooded with bot accounts programmed to spread regime propaganda, attack dissidents, and distort reality. During the diplomatic crisis between Qatar and the Saudi-led bloc in 2017, a massive disinformation campaign unfolded, where fake accounts and automated trolls flooded Twitter with anti-Qatar rhetoric, shaping public perception through algorithmic manipulation (Jones, 2022). Similarly, in Bahrain, pro-government forces have employed cyber militias to target opposition figures systematically, spreading misinformation and harassment to

delegitimize activists and journalists. These strategies illustrate how digital repression extends beyond censorship to active narrative control, shaping public discourse in ways that make genuine opposition increasingly tricky. In addition to overt disinformation campaigns, regimes exploit algorithmic tools like shadow banning and geofencing to suppress dissent. Opposition posts are algorithmically buried by manipulating content visibility, making it harder for activists to reach audiences without direct censorship (Feldstein, 2021). These tactics are particularly effective on platforms like Facebook and YouTube, where algorithmic biases—often shaped by state pressure—control what users see.

The AI-driven moderation of content on global platforms has also contributed to cyber-pessimism, as governments influence the policies of major tech companies to silence dissent. Feldstein (2021) discusses how authoritarian states pressure tech firms to remove content under the guise of combating terrorism, misinformation, or threats to public order. These regulations often disproportionately target opposition activists, independent media, and human rights organizations, rather than genuine security threats. Using geofencing and algorithmic de-prioritization enables governments to suppress unwanted political speech without direct censorship, creating a filtered digital landscape that reinforces state propaganda while erasing dissenting voices.

Despite these challenges, digital resistance remains an evolving phenomenon, demonstrating that cyber-optimism is not entirely misplaced. Activists have developed countermeasures such as encrypted messaging apps (e.g., Signal, Telegram), decentralized social networks, and digital forensics to expose government-led misinformation campaigns (Feldstein, 2021). The exile-based digital activism of Saudi dissidents, the VPN-driven counter-surveillance tactics of Iranian protesters, and the open-source intelligence efforts to track abuses in Syria highlight that technology remains a contested space rather than an inevitable tool of repression (Jones, 2022). Such technological adaptations highlight that digital spaces remain contested, where repression and resistance coexist in a continuous arms race.

The debate between cyber-optimism and cyber-pessimism ultimately underscores the dual nature of digital technologies, where the balance between liberation and control constantly shifts. As authoritarian regimes refine their digital strategies, the battleground for digital rights becomes increasingly complex. The resolution of this struggle will depend on the ability of civil society and international institutions to safeguard digital freedoms. This ongoing contest

between control and resistance will shape not only the future of online activism but also the future of civil liberties in the digital age.

This duality is particularly evident in the context of surveillance, where the same data flows that enable mass mobilization and grassroots activism also provide states with tools for unprecedented control. The vast amount of data generated through social media, messaging platforms, and online interactions facilitates faster communication, the spread of information, and the organization of protests. Yet, this very data becomes the foundation for extensive surveillance networks, predictive policing, and targeted repression. More data means more opportunities for civic engagement and activism—but it also means more opportunities for states to monitor, censor, and manipulate dissent. This paradox places digital technologies at the center of a power struggle, where the potential for empowerment is constantly undermined by the potential for control.

3. The Politics of Control: Surveillance in the MENA Region

The Middle East and North Africa (MENA) region offers a particularly relevant and complex landscape for the study of digital authoritarianism. Characterized by deeply entrenched authoritarian regimes, the region has long been a focal point for the use of surveillance and state control, evolving from colonial-era practices to sophisticated digital repression strategies. The choice to focus on MENA is driven by its unique socio-political dynamics, where authoritarian governance intersects with rapid technological adoption, making it a critical case for understanding how digital tools reshape state power and civil liberties.

The Arab Spring serves as a pivotal moment in this evolution. Initially celebrated as a digital revolution that empowered grassroots activism, it ultimately led many regimes to intensify surveillance and repression. This duality—where digital tools both empower activism and strengthen authoritarian control—makes MENA central to debates on the impact of technology in governance.

MENA's role in the global surveillance ecosystem further underscores its importance. Countries like China, Russia, and the United States have supplied advanced surveillance technologies to regional regimes, embedding MENA within broader geopolitical struggles over security, privacy, and civil rights.

The following chapters will explore these dynamics through three lenses. First, the historical use of surveillance in Arab authoritarian regimes will be examined, focusing on the evolution from traditional to digital control. Next, the legacy of post-colonial intelligence services will be

analyzed to understand how colonial surveillance frameworks shaped modern state practices. Finally, the post-Arab Spring era will be explored, highlighting how regimes have leveraged technological advancements and geopolitical alliances to strengthen internal control and extend their influence.

3.1. Arab Authoritarian Regimes and the Role of Surveillance in Governance

Surveillance has long been a fundamental pillar of governance in Arab authoritarian regimes, where the state exercises strict control over public discourse and political activity. The evolution of authoritarian surveillance in the region accelerated following the Arab Spring, as regimes sought to preempt future uprisings. In response to the mass protests 2011, states such as Saudi Arabia, the UAE, and Bahrain heavily invested in AI-driven surveillance systems, spyware, and large-scale digital monitoring infrastructures. These investments transformed the internet into a battleground for political control, shifting from reactive censorship to proactive monitoring (Feldstein, 2021). Governments now employ AI-driven sentiment analysis, keyword tracking, and network mapping to detect and dismantle opposition movements before they can escalate. For instance, Saudi Arabia and the UAE have used these tools to infiltrate online activist networks and arrest key figures preemptively (Jones, 2022). A particularly stark example of digital repression in the region is Saudi Arabia's use of bots and disinformation networks to shape public perception and silence dissent. As discussed previously in the context of transnational repression, the Jamal Khashoggi case also exemplifies how digital tools are weaponized within the MENA region, mainly through disinformation and bot campaigns aimed at narrative control. Before Khashoggi's assassination in 2018, Saudi intelligence operatives used spyware to monitor his communications and track his contacts. In the aftermath of his murder, Saudi state-backed bot networks flooded Twitter with coordinated disinformation campaigns, spreading false narratives to discredit Khashoggi and obscure the regime's culpability (Jones, 2022). These bot armies engaged in hashtag manipulation, mass reporting of critical voices, and coordinated harassment of opposition figures, creating a digital smokescreen to stifle critical discourse. Investigations revealed that a significant percentage of tweets under #JamalKhashoggi originated from automated Saudi accounts designed to amplify pro-regime propaganda and suppress genuine discussion (Jones, 2022).

In contrast to Saudi Arabia's disinformation-centered approach, the UAE has focused on large-scale acquisition and deployment of advanced surveillance technologies. Abu Dhabi has invested billions in AI-driven security systems, biometric identification programs, and

sophisticated cyber-intelligence operations, positioning the UAE as a hub for digital authoritarianism. The Emirati government collaborates with private surveillance firms and imports cutting-edge spyware from international providers, including Israeli and European companies, using these tools to monitor dissidents and journalists both domestically and abroad (Feldstein, 2021).

One of the UAE's most significant surveillance tools is its innovative city initiatives, which integrate AI-driven monitoring systems into urban infrastructure to enhance public safety. These systems, including facial recognition technology and real-time geofencing, create a comprehensive surveillance grid that tracks citizen movements, social interactions and online behaviors. Such pervasive monitoring allows the state to build behavioral profiles, anticipate dissent and neutralize perceived threats (Jones, 2022).

Both Saudi Arabia and the UAE have weaponized social media platforms to extend their influence beyond national borders. Through state-sponsored influencers, troll networks and AI-generated propaganda, they manipulate international narratives, undermine critics, and shape global perceptions. Saudi Arabia's Twitter operations, for example, have been instrumental in attacking dissidents, promoting pro-government narratives, and spreading disinformation about regional conflicts (Jones, 2022). Similarly, the UAE has used targeted online campaigns to discredit opposition figures and spread favorable narratives about its foreign policy and domestic reforms. These digital operations illustrate how the regimes exploit global platforms to wage information warfare and suppress dissent at home and abroad.

The broader implications of these Arab authoritarian surveillance regimes extend well beyond their borders. Saudi Arabia and the UAE have increasingly influenced international cybersecurity policies, acquired stakes in global tech firms, and exported surveillance software to allied states, contributing to the globalization of digital repression. Other authoritarian states increasingly emulate Their tactics and technologies, normalizing digital authoritarianism globally.

3.2. Post-Colonial Intelligence Services

The transition from colonial rule to independence not only shaped the political landscape of Arab states but also laid the foundation for modern intelligence networks. Although initially built on colonial-era models of physical surveillance and informant networks, these services

evolved, integrating digital technologies and cyber capabilities to extend state control into the digital sphere (Brownlee, 2007). Leaders such as Egypt's Nasser, Syria's Assad, and the Saudi monarchy repurposed inherited intelligence frameworks to consolidate power, enforce ideological conformity, and suppress dissent, a pattern that has continued into the digital age.

Post-independence, Arab leaders rapidly adapted colonial intelligence structures to enforce centralized control. Jason Brownlee (2007) notes that these networks became critical instruments for suppressing opposition and controlling public discourse. In Egypt, Nasser's intelligence services deeply penetrated political, academic, and cultural spheres, reinforcing his pan-Arab nationalist ideology and crushing dissent. This apparatus of surveillance, developed under the Cold War's shadow, evolved further in the digital era. During and after the 2011 uprisings, Egyptian intelligence services expanded their capabilities, blending traditional informant networks with digital surveillance tools. They employed social media monitoring, mobile phone tracking, and spyware to identify and arrest activists, using digital platforms to surveil and spread pro-regime narratives (Brownlee, 2007).

In Syria, Assad's mukhabarat became synonymous with state terror, extending surveillance into every facet of public and private life. Initially strengthened through close ties with the USSR during the Cold War, the mukhabarat modernized its operations with digital tools during the civil war. Leveraging spyware and AI-driven social media analytics, the Syrian regime intercepted encrypted communications, infiltrated digital activist networks, and deployed facial recognition software to monitor urban protests and refugee movements. Human Rights Watch (2023) documented the regime's use of AI-powered video analysis to identify dissidents, even in humanitarian corridors. This blend of traditional surveillance and digital repression created an atmosphere of constant online and offline fear (Gohdes, 2024).

The Cold War period played a crucial role in accelerating the modernization of intelligence services in the region. Egypt, under Nasser, built one of the most formidable intelligence networks in the Arab world with Soviet support. At the same time, Syria's alliance with the USSR enabled operations that extended beyond its borders, particularly into Lebanon. Saudi Arabia, aligning with the United States, developed a highly sophisticated intelligence apparatus focused on suppressing both regional rivals and internal dissenters within the Gulf Cooperation Council (GCC). This foreign support introduced advanced surveillance techniques, including telephone wiretapping, signal interception and joint intelligence-sharing operations, laying the groundwork for today's digital capabilities (Feldstein, 2021).

In the post-Cold War and digital eras, the technological foundations established through these alliances transformed into powerful tools of digital authoritarianism. Syria's mukhabarat, once known for physical intimidation, transitioned to monitoring online dissent through spyware and social media infiltration. Having repressed opposition in the streets, Egypt's security apparatus now tracks activists across digital platforms, employing geolocation data and digital forensics to dismantle protest networks before they mobilize. Saudi Arabia, leveraging U.S. surveillance technologies, extends its digital reach globally, using both spyware and social media manipulation to control narratives and silence dissenting voices.

These examples illustrate how colonial-era intelligence structures, reshaped by Cold War geopolitics, have evolved into sophisticated instruments of digital repression. The legacy of surveillance as a control tool persists, but its methods have become more pervasive and advanced. The cases of Egypt, Syria, and Saudi Arabia reveal how post-colonial intelligence services, armed with both historical practices and modern digital tools, have adapted to the challenges of the digital age, merging traditional repression with cutting-edge technology.

The shift from analog to digital surveillance has increasingly intertwined colonial legacies with contemporary authoritarian practices. As these regimes refine their digital arsenals, the techniques once developed for state security increasingly serve as instruments of authoritarian control. This evolution became particularly evident after the Arab Spring.

3.3. Post-Arab Spring Surveillance States: Geopolitics and Internal Control

The Arab Spring of 2011 marked a turning point for intelligence strategies in Arab regimes. Having witnessed the power of digital platforms in mobilizing dissent, authoritarian governments across the Middle East and North Africa rapidly modernized their surveillance apparatuses. Social media monitoring, data mining, and artificial intelligence (AI) became central tools for state control. Bolstered by international partnerships, particularly with providers from the United States, China, and Russia, Arab intelligence services expanded their reach into digital spaces, transforming themselves into modern surveillance states (Gohdes, 2024).

Adopting advanced surveillance tools has been a defining development in post-Arab Spring intelligence operations. Social media, once a tool for protest coordination, became a primary

target for state surveillance. Governments embraced digital technologies such as AI-powered sentiment analysis and network mapping to monitor dissent and disrupt opposition networks.

Big data analytics further empower intelligence agencies by processing vast amounts of digital data from social platforms, messaging apps, and search engines. These technologies enable predicting protest hotspots and identifying influential activists, allowing preemptive arrests and digital shutdowns. For example, during the 2019 anti-government protests in Egypt, authorities deployed AI-driven social media tracking to identify protest organizers, leading to hundreds of preemptive arrests within hours.

International partnerships have been crucial in equipping Arab regimes with advanced surveillance capabilities, embedding their intelligence services within global geopolitical strategies. The United States has continued its strategic alliances with Saudi Arabia, the UAE, and Egypt, providing surveillance technologies and cybersecurity training under the guise of counterterrorism cooperation.

Meanwhile, China has promoted its model of digital authoritarianism, exporting surveillance technologies and expertise to Arab states through firms like Huawei and Hikvision. These companies have supplied facial recognition software and network monitoring systems, particularly to the UAE, where “smart cities” double as surveillance hubs. The Emirati government, for instance, has integrated Chinese facial recognition systems into public spaces, linking them to AI-driven databases that monitor citizen movements and flag “suspicious behavior” in real time (Jones, 2022).

Russia, similarly, has provided technical expertise and advanced cybersecurity tools, enabling Arab states to protect their digital infrastructure from Western scrutiny and sanctions. This multi-vector international support has collectively empowered Arab regimes to entrench digital authoritarianism while aligning with broader geopolitical strategies that favor state-centric control over digital freedoms.

The expansion of surveillance has profoundly impacted civil society, privacy, and individual freedoms across the Arab world. As digital monitoring intensifies, individuals and organizations operate under constant threat of surveillance and repression, fostering widespread self-censorship. The pervasive nature of surveillance has eroded social trust, as citizens fear that their private conversations on platforms like WhatsApp and Signal may be intercepted. This

culture of suspicion fractures social cohesion, as communities become divided and individuals retreat from political discourse, wary of state intervention and potential reprisals.

The transformation of Arab intelligence services into digital surveillance states aligns with a Constructivist perspective, which emphasizes how norms, identities, and state narratives shape behavior. Post-Arab Spring regimes have framed digital surveillance as a tool for control and a patriotic duty essential for national security and stability. By embedding surveillance into their national identity, these regimes present digital repression as a defense of state sovereignty.

Moreover, IR theories, namely, Constructivism (Wendt, 1999), helps explain how the alliances with China, Russia, and the United States influence the tools and the surveillance philosophies adopted by Arab regimes. From China, they import the discourse of "digital sovereignty" and surveillance-as-stability; from Russia, the model of securitized information control; and from the United States, the justification of surveillance under the umbrella of counterterrorism (Feldstein, 2021). These global narratives are internalized and adapted to local contexts, where mass surveillance becomes part of the state's identity as a protector of national security (Gohdes, 2024).

The post-Arab Spring evolution of intelligence services thus reflects a dual transformation: technological and ideological. Technologically, regimes have incorporated AI, big data, and spyware into their intelligence frameworks, creating predictive surveillance systems capable of suppressing dissent before it emerges (Jones, 2022). Ideologically, they have framed this digital authoritarianism as a necessary defense of sovereignty and stability, embedding it into their national identities. This fusion of global technology, geopolitical alliances, and internal control has redefined governance in the Arab world, establishing surveillance not only as a tool of repression but as a pillar of state power and legitimacy (Feldstein, 2021).

Conclusion

The transformation of Arab intelligence services into digital surveillance states reflects a broader trend where technological innovation, geopolitical alliances and internal control intersect. As this analysis highlights, surveillance technologies have become essential tools for authoritarian regimes to suppress dissent and extend their influence beyond national borders. Arab regimes have not only adopted digital tools for repression but also constructed surveillance as an element of state identity and sovereignty. The tension between cyber-optimism and cyber-pessimism, explored in this review, reflects how digital technologies serve

as both instruments of resistance and tools of authoritarian control. In addition, the case studies examined illustrate the concrete manifestations of digital surveillance across the MENA region. From Egypt's predictive arrests based on AI-driven social media monitoring to Syria's use of spyware and facial recognition during the civil war, and from Saudi Arabia's transnational repression through Pegasus to the UAE's smart city surveillance hubs, the cases analyzed demonstrate how digital tools fortify authoritarian governance.

A central theme emerging from this chapter is how Arab regimes use digital surveillance not only for domestic repression but also to consolidate their international standing. Strategic partnerships with technological powers such as the United States, China, and Russia have equipped these regimes with cutting-edge surveillance tools under the guise of counterterrorism and cybersecurity cooperation. These alliances are mutually beneficial: Arab states gain advanced capabilities to monitor dissent, while global powers secure military and economic influence in the MENA region. Moreover, these partnerships illustrate how digital surveillance has become a vector of global power. The United States provides counterterrorism tools and cybersecurity training, China exports digital authoritarianism through surveillance infrastructure and "safe city" projects, while Russia supplies cyber expertise and information control strategies. These alliances demonstrate how digital surveillance intertwines with global geopolitics, embedding the MENA region within broader struggles over digital power and influence.

The impact of this digital authoritarianism extends beyond borders, enabling regimes to engage in transnational repression. The Khashoggi case, where Saudi Arabia used Pegasus spyware to track dissidents abroad, exemplifies how digital surveillance merges internal security concerns with foreign policy objectives. Through digital tools, authoritarian control no longer ends at national borders but becomes a globalized mechanism of state power.

In conclusion, digital surveillance has become both a pillar of authoritarian power and a tool of global influence. The cases analyzed reveal that addressing this challenge requires robust international regulations, corporate accountability, and a renewed global commitment to digital rights. As technology increasingly defines state power and international relations, the contest over digital control will shape the future of freedom and repression in the 21st century.

We have thus explored the dynamics of digital authoritarianism, emphasizing how surveillance technologies serve as tools of repression and control within Arab regimes. However, while existing scholarship extensively analyzes the domestic implications of digital surveillance—such as its role in silencing dissent and shaping public discourse—there remains a significant

gap in understanding how these technologies influence international relations. Specifically, little attention has been given to how Arab authoritarian regimes strategically use surveillance not only for internal stability but also to strengthen geopolitical alliances and align with global powers. This gap invites further investigation into how surveillance practices are shaped by, and in turn shape, international partnerships. The following chapters will delve into this unexplored dimension by examining how Arab regimes leverage surveillance technologies within their foreign policy strategies. By focusing on case studies from Egypt, Syria, and Saudi Arabia—each aligned with different global powers (the United States, Russia, and China, respectively)—this research aims to reveal how surveillance functions not just as a domestic tool but as an instrument of geopolitical influence and diplomacy.

Chapter 2 – Research Design

Introduction

The main research puzzle of this thesis is to understand how surveillance technologies are employed by Arab authoritarian regimes, particularly Egypt and Saudi Arabia, to enhance their economic and technological partnerships with global powers like the USA and China. Despite growing academic interest in surveillance and authoritarianism, there is a significant gap in the literature concerning the geopolitical dimension of surveillance technologies. Most existing studies focus on domestic repression, with little attention given to how these technologies can serve as leverage to strengthen foreign relations, especially with major powers like the USA and China. This gap is particularly relevant in today's geopolitical landscape, where technological cooperation and economic alliances are becoming as important as traditional political and military agreements. By analyzing the way Egypt and Saudi Arabia use surveillance technology as a diplomatic instrument, this thesis aims to provide insights into how these regimes navigate international relations and secure investment, technology transfers, and strategic alliances. The findings will contribute to a better understanding of the role of digital diplomacy in shaping the global balance of power.

2.1. Hypothesis formulation

The research question guiding this study is: "*How do Arab authoritarian regimes leverage surveillance technology to strengthen their economic and technological partnerships with global powers?*"

This question explores how surveillance technologies have become central to the diplomatic strategies of authoritarian regimes, specifically Egypt and Saudi Arabia, in their relations with the United States and China. While traditionally employed to maintain domestic control and suppress dissent, these technologies are now instrumental in advancing international cooperation. They give these regimes political and strategic leverage, enabling them to engage global powers on security, economic development, and technological innovation (Feldstein, 2019).

In the current geopolitical context, surveillance has evolved into a multifaceted tool—essential for consolidating power internally and shaping international relations. By incorporating advanced monitoring systems and digital control infrastructures, Egypt and Saudi Arabia position themselves as key partners to global actors with strong interests in the Middle East.

These regimes increasingly align with global priorities in counterterrorism and cybersecurity, enhancing their perceived reliability and strategic value (Greitens, 2020).

Egypt, a long-standing ally of the United States, has progressively integrated surveillance systems into its national security apparatus. Technologies for monitoring online activity, controlling digital communication, and tracking civilian behaviour serve both to reinforce the regime's authority and to present Egypt as a capable and cooperative partner in regional security. For instance, Egypt has collaborated with foreign firms to acquire tools such as deep packet inspection, which is used to censor content and track opposition (Feldstein, 2019).

Saudi Arabia, meanwhile, situates surveillance technology within its broader modernization project, Vision 2030. This national strategy seeks to diversify the economy and reduce dependence on oil, partly through the development of advanced digital systems. Surveillance plays a key role in this transformation, underpinning smart cities, predictive policing, and biometric identity initiatives. These tools extend the regime's domestic reach but also demonstrate a commitment to modernization, appealing to both Western and Eastern partners. The kingdom maintains robust military and intelligence ties with the United States, but in recent years has also expanded its engagement with China. Under the Belt and Road Initiative framework, China has provided Saudi Arabia with critical surveillance technologies and digital infrastructure, reinforcing bilateral ties. This partnership allows Saudi Arabia to benefit from Chinese expertise and investment, while offering China access to one of the most influential states in the Arab world (Liu, 2019; Rolland, 2019).

These dynamics illustrate how surveillance technology facilitates internal governance and external alignment. Egypt and Saudi Arabia use these tools to position themselves as technologically capable and politically reliable, securing economic advantages and strategic partnerships. These regimes build on long-standing security alliances with the United States, now strengthened by digital cooperation in intelligence and counterterrorism (Feldstein, 2019). China, engages in reciprocal exchanges involving infrastructure, surveillance systems, and long-term investments that reflect broader geopolitical shifts (Liu, 2020).

In this context, surveillance technologies are no longer limited to their traditional role in authoritarian governance. They have become strategic assets through which Arab regimes navigate complex international landscapes, secure foreign investment, and assert their place in global technological networks (Greitens, 2020). The ability to control information, manage populations, and align with external priorities has become a form of diplomatic capital that Egypt and Saudi Arabia have learned to deploy with increasing sophistication.

Building on the research question and the analysis of how surveillance technology plays a role in enhancing international relations, this study proposes the following hypotheses:

- *H1a:* Higher investments in surveillance technology by Egypt and Saudi Arabia correlate with increased technological cooperation with the USA and China.
    - Dependent Variable: Technological cooperation with the USA and China
    - Independent Variable: Adoption of surveillance technologies by Egypt and Saudi Arabia

This hypothesis examines the relationship between Egypt's and Saudi Arabia's adoption of surveillance technologies and their levels of technological cooperation with global powers, specifically the United States and China. The *independent variable* in this analysis is the extent to which these states invest in and adopt surveillance technologies. The *dependent variable* is the degree of technological cooperation with the USA and China, which can be observed through bilateral tech agreements, joint research initiatives, or military-tech transfers.

The underlying argument is that as Egypt and Saudi Arabia deepen their reliance on surveillance infrastructure, they become more enmeshed in the technological ecosystems of the powers supplying these tools—namely, the USA and China. This hypothesis seeks to assess whether the growing investments in surveillance infrastructure by Egypt and Saudi Arabia are associated with the deepening of technological partnerships with major global powers. The measurement will focus on indicators such as the number and significance of collaborative technological initiatives, bilateral technology transfer agreements, and the formation of joint ventures, especially in security technology, telecommunications, and smart infrastructure development.

- *H1b:* Higher investments in surveillance technology by Egypt and Saudi Arabia correlate with increased economic agreements with the USA and China.
    - Dependent Variable: Economic cooperation with the USA and China
    - Independent Variable: Adoption of surveillance technologies by Egypt and Saudi Arabia.

This hypothesis explores the potential link between surveillance technology investments and broader patterns of international economic cooperation. The *independent variable* is the level of investment in surveillance technologies by Egypt and Saudi Arabia, encompassing the acquisition of advanced monitoring systems, cybersecurity infrastructure, and partnerships with global surveillance firms. The *dependent variable* is the extent of economic cooperation with the United States and China, measured through trade agreements, foreign direct investment,

and bilateral economic initiatives. The core argument is that as these states expand their surveillance capabilities—often relying on technology from global powers—they may simultaneously open doors to deeper economic ties. This hypothesis aims to explore the extent to which the adoption of surveillance technologies influences the economic dimension of international cooperation. It will examine whether such adoption contributes to increased trade deals, bilateral investment flows, infrastructure development projects, and broader economic partnerships. Particular attention will be paid to economic initiatives that explicitly or implicitly involve surveillance-related technologies, cybersecurity infrastructure, and digital governance frameworks.

2.2. Research Methods

This study employs a comparative and quantitative approach to analyze the role of surveillance technology in strengthening the economic and technological partnerships between Arab authoritarian regimes (i.e., Egypt and Saudi Arabia) and global powers, namely the USA and China.

The comparative aspect of the methodology focuses on contrasting the surveillance strategies, technological investments, and diplomatic engagements of Egypt and Saudi Arabia. The quantitative analysis will assess the relationship between the adoption of surveillance technologies and the strengthening of economic and technological cooperation with these global powers.

This research will examine the two countries' adoption of surveillance technologies, including facial recognition, surveillance cameras, social media monitoring, and spyware. The analysis will also consider the investments made in surveillance infrastructure and the extent of cooperation with the USA and China in technology, security, and economic development. The study will compare the two regimes to explore how their adoption of surveillance technologies influences their diplomatic, economic, and technological relationships with these global powers.

To comprehensively investigate the dynamics of political and internet freedoms, the contours of digital repression, and the geopolitical influences on surveillance practices within Saudi Arabia and Egypt, this thesis relies upon a robust and diverse assemblage of quantitative and qualitative data repositories. The initial exploration into the overarching political and internet freedom landscapes (i.e., *Part 1*) leverages the longitudinal data from the Varieties of Democracy (V-Dem) project, specifically its core dataset, to meticulously track nuanced shifts

in various dimensions of political liberties over an extended temporal horizon. Complementing this, Freedom House indicators provide critical assessments: its dataset of Aggregate Category and Subcategory Scores from the Freedom in the World reports (2003-2024) is employed to evaluate the trajectory of aggregated freedom scores, offering a macro-level perspective on the status of liberty, while its Freedom on the Net country score data for 2024 offers a contemporaneous analysis of internet freedom. Further granularity on the modus operandi of online censorship and control is derived from Freedom House's 2024 data detailing key internet controls, which delineates specific tactics of internet control implemented in that year.

Progressing to the analysis of digital repression with a specific focus on digital surveillance (i.e., *Part 2*), the study incorporates Steven Feldstein's Digital Repression Index data (covering 2003-2022), a composite measure enabling an assessment of the evolution of both digital repression activities and the state's capacity for such repression within the two case studies. To dissect the constituent elements of these broader trends, particularly the instrumental role of surveillance, the research draws upon the disaggregated indices contained within the Digital Society Project's comprehensive dataset, which informs Feldstein's Digital Repression Index and allows for a more granular examination of surveillance mechanisms.

The investigation into international cooperation and the external facilitation of surveillance capabilities (i.e., *Part 3*) utilizes several specialized sources. Feldstein-specific analyses, including the AI Surveillance Index data for 2022 and data on the deployment of invasive spyware compiled in 2023, are instrumental in identifying the prevalence and nature of advanced digital surveillance tools within Saudi Arabia and Egypt, and assessing potential involvement of international actors such as China and the United States. The role of China is further scrutinized through AidData's Global Chinese Development Finance Dataset, which is interrogated for evidence of Chinese investments related to surveillance infrastructure, particularly in Egypt. Contextual information regarding Saudi-Chinese bilateral relations, particularly within the framework of the Belt and Road Initiative, is sourced from the Hong Kong Trade Development Council's Belt and Road Portal, providing insights into broader technological and infrastructural partnerships. Finally, information pertaining to the United States' surveillance engagements or policies concerning Egypt is informed by materials attributable to the U.S. State Department. This multi-faceted empirical strategy, triangulating data from esteemed international indices, academic research projects, and official sources, provides a rigorous foundation for the ensuing analysis of state control in the digital age.

2.3. Scope

This chapter has outlined the conceptual and methodological framework of the study, examining how surveillance technologies are leveraged by authoritarian regimes—specifically Egypt and Saudi Arabia—to foster economic and technological partnerships with global powers. It has introduced the research question, presented the hypotheses, and described the comparative and quantitative approach adopted for the analysis. It also reviewed the data sources selected to measure the relationship between surveillance investments and international cooperation.

Taken together, this chapter establishes a robust theoretical and empirical foundation for exploring how digital surveillance serves as both an instrument of domestic control and a strategic asset in international diplomacy. By positioning surveillance technologies at the intersection of authoritarian governance and global geopolitics, the study advances a novel analytical lens—one that moves beyond traditional narratives of repression to consider how authoritarian regimes use digital tools to signal reliability, modernity, and alignment with international priorities such as cybersecurity, counterterrorism, and technological innovation. Egypt and Saudi Arabia, despite differing in historical alliances and strategic orientation, converge in their instrumentalization of surveillance as a form of "digital diplomacy" aimed at deepening bilateral ties, attracting foreign investment, and embedding themselves into global technological ecosystems.

The hypotheses developed in this chapter reflect a dual-layered logic. First, that the proliferation of surveillance infrastructures within these regimes is not merely a response to internal security imperatives, but also a calculated move to facilitate technological and economic engagement with powerful global actors. Second, that such engagement is not passive but shaped by the regimes' ability to present themselves as capable partners in digital governance—thus redefining the strategic value of authoritarian states in the evolving geopolitical order. By testing these propositions through empirical data and cross-case comparisons, the study seeks to uncover the political economy underlying the global circulation of surveillance technologies, and the emergent logics of authoritarian collaboration with democratic and authoritarian powers alike.

Furthermore, the methodological design presented in this chapter ensures analytical rigor and comparative depth. By integrating longitudinal and cross-sectional data from a range of established sources—including V-Dem, Freedom House, the Digital Repression Index, the Digital Society Project, and datasets on international surveillance cooperation—the study offers

a comprehensive framework for assessing both domestic repression and international engagement. The inclusion of datasets specific to spyware deployment, AI surveillance, and foreign investment further enables the analysis to capture the transnational dimensions of surveillance adoption, and to map the flows of technology, capital, and influence between Arab regimes and global powers.

Building on this foundation, the next chapter will shift from conceptual groundwork to empirical exploration. It will delve into the specific trajectories of Egypt and Saudi Arabia in their adoption of surveillance technologies, tracing how these regimes have institutionalized digital monitoring systems, and how such systems are embedded in broader strategies of economic development, security cooperation, and international diplomacy. Particular attention will be paid to the material flows—such as financial investments, technology transfers, and bilateral agreements—that accompany surveillance infrastructure, and the geopolitical narratives that legitimize them. Through a comparative lens, the chapter will identify key similarities and divergences between the two case studies, shedding light on how each regime operationalizes surveillance as a strategic tool in contemporary authoritarian governance and global power dynamics.

Chapter 3 – A comparative analysis of Egypt and Saudi Arabia surveillance systems

Introduction

This chapter is structured into three main sections. The first section examines the relationship between Egypt and Saudi Arabia's investments in surveillance technology, as part of their expanding technological partnership with the United States and China. The second section focuses on business partnerships with global players and their increasing surveillance technological activities. Finally, the final section examines surveillance technologies as both internal control mechanisms, referring to their use for improving international diplomatic relations, resulting in cooperative and beneficial economic and technological links for the ruling regime.

3.1. Part 1 – Political Freedom and Internet Freedom

This section provides a comprehensive overview of political freedom and internet freedom in Saudi Arabia and Egypt, drawing on multiple reputable data sources for a thorough assessment. To capture trends over time, it presents changes in political rights and civil liberties from 2003 to 2024 using the Varieties of Democracy (V-Dem) dataset (V-Dem Institute, 2024a).

Complementing this longitudinal view, Freedom House scores offer an evaluation of the overall state of freedom in both countries throughout the same period. For a detailed snapshot of the current digital environment, the analysis incorporates Freedom House's 2024 internet freedom scores, which include aggregated measures of online openness alongside specific tactics of internet control (Freedom House, 2024). Together, these datasets provide a nuanced understanding of how political and digital freedoms have evolved and currently manifest in Saudi Arabia and Egypt.

3.1.1. Measuring Democracy

The V-Dem project offers one of the most detailed global datasets on democracy, measuring multiple dimensions of political regimes through various indices. In this analysis we consider indices measuring Electoral Democracy (*v2x_polyarchy*), Liberal Democracy (*v2x_libdem*), Participatory Democracy (*v2x_partipdem*), Deliberative Democracy (*v2x_delibdem*), and Egalitarian Democracy (*v2x_egaldem*).

Between 2000 and 2024, Egypt and Saudi Arabia have consistently ranked among the world's most authoritarian regimes. Egypt experienced brief episodes of democratic opening, most notably during the Arab Spring, but these periods were short-lived and later reversed. Saudi

Arabia, instead, maintained a highly centralized and autocratic regime throughout the entire period.

The *Electoral Democracy Index* gauges the extent to which political leaders are selected through genuine multiparty elections characterised by freedom and fairness. Egypt's score remained low from 2000 to 2010, reflecting limited electoral competition and a lack of genuine pluralism. It rose significantly during the Arab Spring (2011–2012), corresponding to a brief phase of increased political openness and competitive elections. However, following the military takeover in 2013, this progress was undone, and by 2024, Egypt's score had fallen back to 0.186, signalling severely restricted electoral pluralism. Saudi Arabia's score has remained consistently low, at 0.015, throughout this period, reflecting the absence of competitive elections and the enduring absolute monarchy, with no evident progress toward electoral reform.

The Liberal Democracy Index focuses on protections for individual and minority rights, the rule of law, and constraints on executive power. Egypt's score peaked during the brief democratic transition around 2012–2013 but collapsed soon after. By 2024, Egypt scored 0.129, indicating weak civil liberties and judicial oversight heavily undermined by executive dominance. Saudi Arabia's score has remained below 0.05 consistently, registering 0.047 in 2024, reflecting a regime marked by severe limitations on core liberties, the absence of an effective rule of law, and virtually no institutional constraints on executive authority.

The *Participatory Democracy Index* measures the degree to which citizens actively engage in political decision-making beyond elections through civil society, local governance, and other channels. Egypt experienced gains in political participation following the 2011 revolution; however, these were reversed after the military reasserted its control. By 2024, Egypt's score had fallen to 0.079, indicating very severe repression of grassroots political engagement and shrinking spaces for participation. In Saudi Arabia, participatory democracy remains almost entirely absent, with a 2024 score of 0.021, as political decision-making is strictly top-down and civil society input minimal.

The *Deliberative Democracy Index* evaluates whether political decisions are reached through respectful public reasoning aimed at the common good. Egypt experienced modest improvements in 2012, but these gains were rolled back as authoritarianism strengthened. The 2024 score of 0.102 points to minimal transparency, restricted debate, and a lack of meaningful deliberative processes. Saudi Arabia's score of 0.065 in 2024 indicates an almost total absence of public consultation and contestation, with decisions made exclusively by a small elite and

no space for open discussion. The *Egalitarian Democracy Index* tracks equal access to power and political influence across different social groups. Both Egypt and Saudi Arabia demonstrate persistent structural inequalities, with 2024 scores of 0.112 and 0.113 respectively. These low scores reflect entrenched barriers to political inclusion based on factors such as gender, class, geography, and ethnicity.

Figure 1 illustrates the trajectories of the Liberal Democracy Index for Egypt and Saudi Arabia between 2000 and 2024, offering a longitudinal perspective on the evolution of democratic governance in both states. *Figure 2* complements this analysis by depicting the Freedom of Expression and Alternative Sources of Information Index over the same timeframe. This index specifically measures the extent to which citizens can access independent media, voice dissenting opinions, and receive uncensored information. The precise index values corresponding to these trends are provided in *Table 1*, which serves as a reference for interpreting the patterns visualized in the figures.

year	v2x_libdem_EGY	v2x_libdem_SAU	v2x_freexp_altinf_EGY	v2x_freexp_altinf_SAU
2000	0,16	0,04	0,36	0,11
2001	0,15	0,04	0,36	0,11
2002	0,15	0,04	0,36	0,11
2015	0,10	0,05	0,16	0,09
2016	0,12	0,05	0,16	0,09
2017	0,12	0,04	0,16	0,08
2018	0,11	0,04	0,16	0,09
2019	0,12	0,05	0,14	0,09
2020	0,12	0,05	0,16	0,09
2021	0,12	0,05	0,15	0,09
2022	0,13	0,05	0,16	0,09
2023	0,13	0,05	0,17	0,09
2024	0,13	0,05	0,19	0,09

Table 1. V-Dems Democracy Indexes (2000-2024)

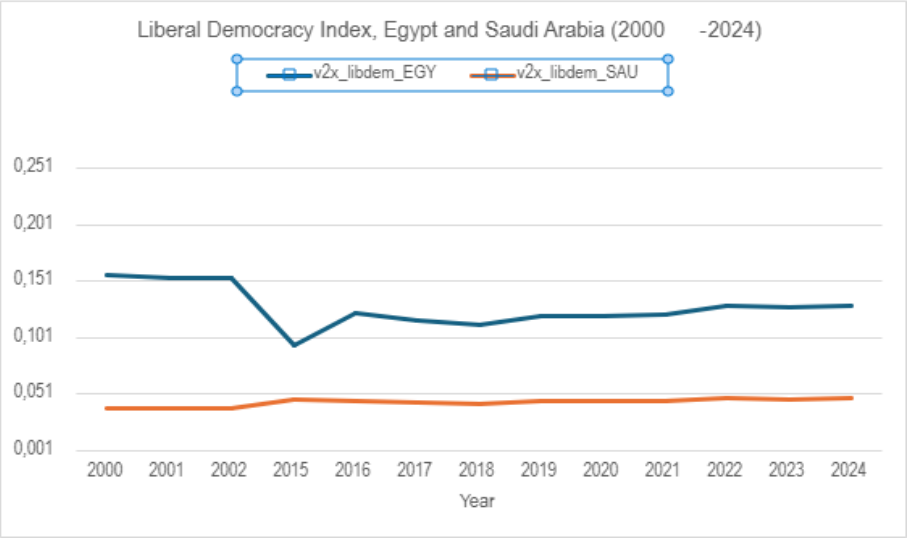

Figure 1. Liberal Democracy Index (Egypt and Saudi Arabia) 2000-2024

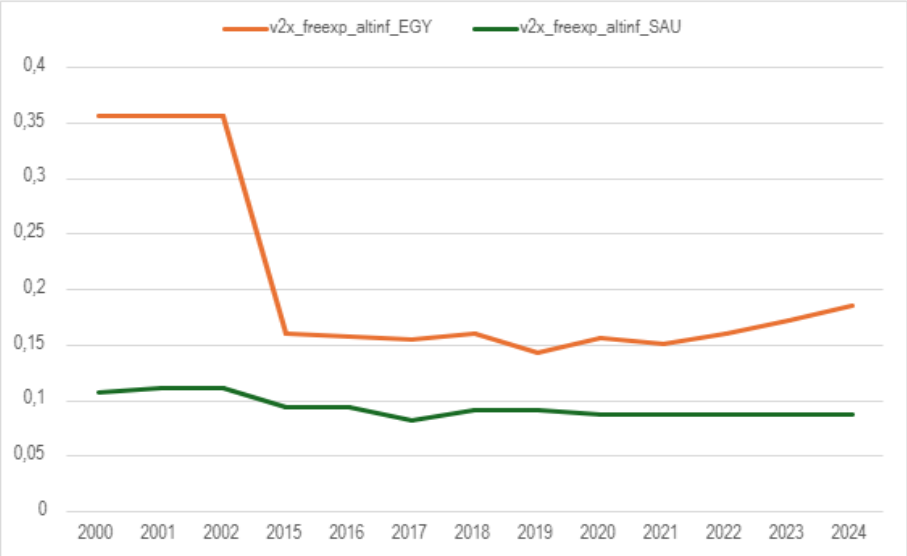

Figure 2: Freedom of Expression (Egypt and Saudi Arabia), 2020-2024

Overall, neither Egypt nor Saudi Arabia has shown sustained progress toward democratization over the past 25 years. Egypt's political trajectory is marked by brief democratic experiments quickly overturned by military takeovers. Saudi Arabia has institutionalised an absolute monarchy characterised by the absence of electoral and participatory processes, systematic repression of civil society liberties, and tight restrictions on political rights. Despite some differences in their paths, both regimes exhibit broad, systemic obstacles to political openness, inclusion, and democratic governance.

These overarching trends are empirically assessed through the data presented in *Table 2* and *Table 3*, which report the annual values of key V-Dem democracy indexes for Egypt and Saudi Arabia, respectively, over the 2000–2024 period. These tables provide a detailed account of the

indicators underpinning the broader patterns of authoritarian resilience discussed above, including measures of electoral democracy, political pluralism, and civil liberties.

year	v2x_polyarchy	v2x_libdem	v2x_partipdem	v2x_delibdem	v2x_egaldem
2000	0,22	0,16	0,08	0,15	0,10
2001	0,21	0,15	0,08	0,15	0,09
2002	0,21	0,15	0,08	0,15	0,09
2015	0,16	0,10	0,05	0,11	0,08
2016	0,18	0,12	0,06	0,11	0,09
2017	0,18	0,12	0,06	0,11	0,09
2018	0,18	0,11	0,06	0,10	0,10
2019	0,17	0,12	0,08	0,10	0,10
2020	0,18	0,12	0,07	0,11	0,11
2021	0,18	0,12	0,07	0,11	0,10
2022	0,18	0,13	0,08	0,10	0,10
2023	0,19	0,13	0,08	0,10	0,11

Table 2: V-Dem Democracy Indexes (Egypt)

year	v2x_polyarchy	v2x_libdem	v2x_partipdem	v2x_delibdem	v2x_egaldem
2000	0,02	0,04	0,02	0,04	0,10
2001	0,02	0,04	0,02	0,04	0,10
2002	0,02	0,04	0,02	0,04	0,10
2015	0,02	0,05	0,03	0,05	0,11
2016	0,02	0,05	0,03	0,05	0,11
2017	0,02	0,04	0,02	0,05	0,11
2018	0,02	0,04	0,03	0,05	0,11
2019	0,02	0,05	0,02	0,05	0,11
2020	0,02	0,05	0,02	0,06	0,11
2021	0,02	0,05	0,02	0,06	0,11
2022	0,02	0,05	0,03	0,07	0,11
2023	0,02	0,05	0,02	0,07	0,12
2024	0,02	0,05	0,02	0,07	0,11

Table 3: V-Dem Democracy Indexes (Saudi Arabia)

Complementing these tabular datasets, *Figure 3* and *Figure 4* offer a longitudinal visualisation of the same indexes in each country. Together, this analysis demonstrates the entrenched nature of autocratic governance in both regimes and underscore the lack of meaningful progress toward democratisation over the past two decades. More precisely, the longitudinal line graphs in *Figure 3* and *Figure 4* illuminate these trends by tracing the evolution of key V-Dem democracy indicators over time. In the case of Egypt (*Figure 3*), the data reveal a progressive decline in democratic measures from 2000 to 2015, culminating in the lowest recorded values during this period—coinciding with the aftermath of the Arab Spring and subsequent military consolidation of power. From 2015 onward, the trend stabilizes, reflecting a period of authoritarian entrenchment with little to no democratic recovery. In contrast, Saudi Arabia's trajectory (*Figure 4*) is marked by a consistent stability across the entire 2000–2024 timeframe, but at persistently lower levels than those reached by Egypt, even at its most repressive. These longitudinal patterns, when read alongside the detailed annual values in *Table 2* (i.e., Egypt)

and *Table 3* (i.e., Saudi Arabia), underscore the structural nature of authoritarian governance in both regimes and the absence of meaningful democratic opening over the past two decades.

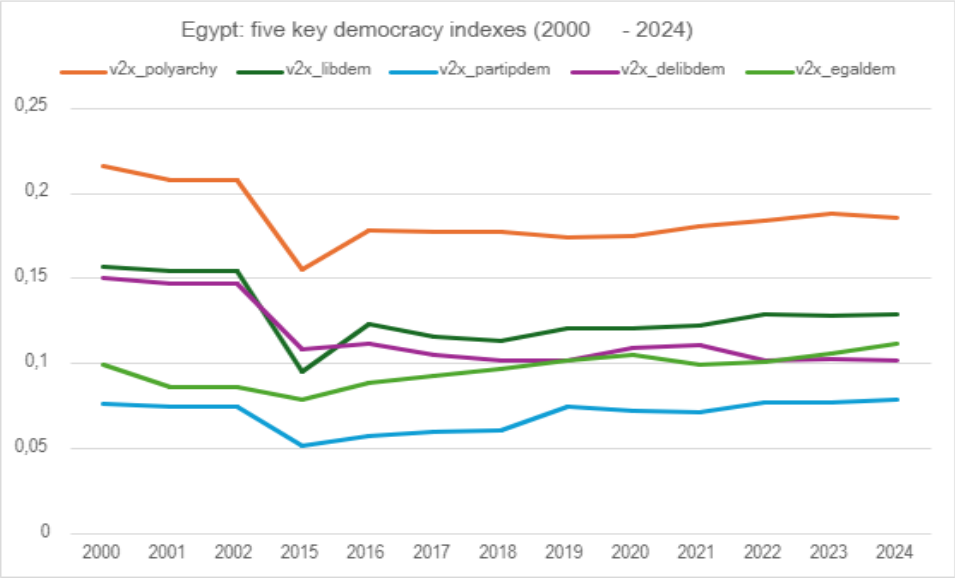

Figure 3: Egypt key democracy indexes (2000-2024)

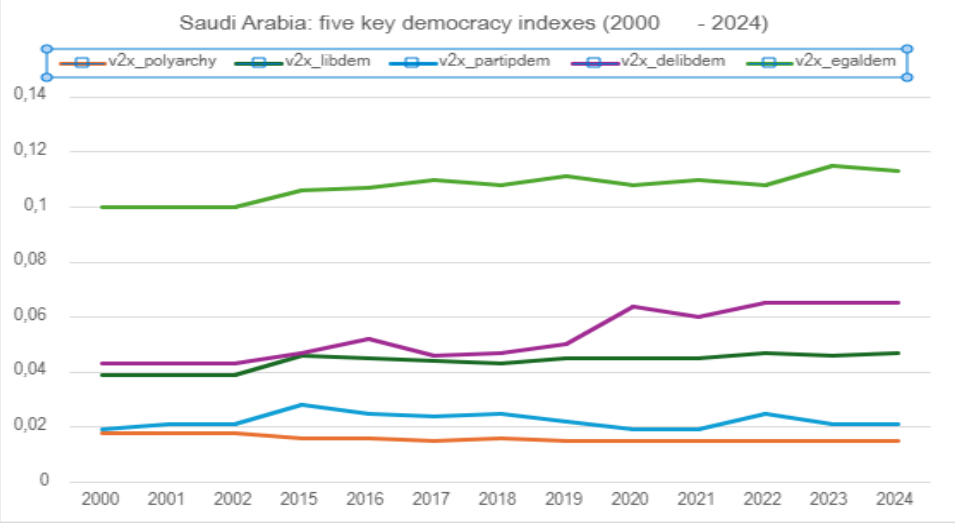

Figure 4: Saudi Arabia: five key democracy indexes (2020-2024)

3.1.2. Measuring Political Rights and Freedoms

This chapter further examines the status of freedom in Egypt and Saudi Arabia by using Freedom House scores, complementing the earlier analysis of political freedoms based on the Varieties of Democracy (V-Dem) dataset. Freedom House provides detailed assessments of political rights and civil liberties, producing scores that allow tracking freedom trends over time. Its well-known classification system categorizes countries as "Free," "Partly Free," or "Not Free" based on aggregated scores derived from comprehensive evaluations of political and civil liberties.

Between 2006 and 2024, Egypt's political landscape remained largely consistent. The country was rated as "Not Free" every year except in 2013, when it was classified as "Partly Free" due to political upheaval following the Arab Spring. Before 2011, Egypt was ruled by President Hosni Mubarak under an authoritarian regime that severely suppressed political activity and enforced intense oppression. Following the 2011 uprising, Egypt experienced a brief period of democratic opening that was abruptly ended by the 2013 military takeover led by General Abdel Fattah el-Sisi, which reinstated a dominant authoritarian regime. In contrast, Saudi Arabia remained firmly entrenched in a centralised autocratic system and was rated as "Not Free" throughout the entire period.

3.1.3. Measuring Internet Freedom

The report also analyzes internet freedom in both countries in 2024. Egypt and Saudi Arabia are ranked among the world's most restrictive countries in terms of internet freedom. Egypt scored 28 out of 100 (Freedom House, 2024b) indicating a highly oppressive online environment. The country faces moderate barriers to access (14/25), including infrastructural challenges and heavy state control over internet services, subject to stringent regulation and surveillance. Regarding content restrictions, Egypt scored 9/35, reflecting the government's tight control over online material, including blocking websites that promote opposition or dissent and censoring politically sensitive information. Most concerning is the score for violations of user rights, at 5/40, which highlights extensive online surveillance, frequent arrests of activists and journalists, and the use of surveillance technologies to monitor dissent. Between 2020 and 2024, Egypt's internet freedom score slightly improved from 26 to 28, but this marginal increase did not signal any substantive progress toward greater digital freedom (Freedom House, 2024b).

Saudi Arabia's internet freedom score in 2024 was slightly lower at 25 out of 100 (Freedom House, 2024b). The country faces moderate obstacles to access (13/25), with the government maintaining strict control over internet infrastructure. Content restrictions are particularly severe, with the government blocking politically sensitive material—especially criticism of the monarchy and issues related to human rights, religion, and political dissent. Violations of user rights are on par with Egypt's, also scoring 5/40, as users are frequently imprisoned for online activism or criticizing the regime. Unlike Egypt, Saudi Arabia's internet freedom score declined slightly from 26 in 2020 to 24 in 2024, indicating growing repression of online content and activities (Freedom House, 202b). Both countries thus rely heavily on digital surveillance and

censorship tools to control their populations' online behavior. These technologies are central to the regimes' efforts to consolidate power domestically and manage public discourse.

Moreover, Freedom House has documented five key internet control measures employed by both countries, reinforcing their classification as "Not Free" (Freedom House, 2024c). Both Egypt and Saudi Arabia impose bans on social media and messaging services during protests and elections, restrict political and religious content, and aggressively promote pro-government online commentators who disseminate official narratives and attack dissenting voices. Journalists, activists, and ordinary users face imprisonment merely for sharing critical content. Reports of torture, abuse in detention, and deaths in custody have also been documented (Freedom House, 2024c).

In conclusion, despite some differences in the specifics of their digital spaces, Egypt and Saudi Arabia exhibit similar patterns of digital repression. Both regimes deploy extensive monitoring systems to oversee and control cyberspace, impose severe restrictions on internet access, and harshly punish any form of digital opposition.

3.2. Part 2 – Digital Repression in Egypt and Saudi Arabia

This section examines digital repression in Egypt and Saudi Arabia using data from the Digital Society Project, focusing on the Digital Repression Index (DRI) and the Digital Repression Capacity Index (DRCI), along with specific indicators measuring filtering capacity, shutdown capacity, regulatory capacity, and the use of alternative government-controlled social media accounts.

The Digital Society Project (DSP), an initiative under the Varieties of Democracy (V-Dem) framework that compiles expert-coded data on the intersection of digital technologies and political practices. The DSP monitors various forms of online censorship, surveillance, and control mechanisms implemented by governments worldwide. Building on this dataset, Steven Feldstein has developed the Digital Repression Index (DRI), a composite measure that captures the extent to which states engage in repressive digital activities such as filtering, monitoring, content manipulation, and targeting of online dissent. Complementing this, the Digital Repression Capacity Index (DRCI) assesses a state's infrastructural and regulatory capacity to execute these repressive measures.

These indices offer a valuable longitudinal perspective for examining how digital repression evolves in response to political developments and technological advancements.

3.2.1. Digital Repression in Practice and in Capacity

In Egypt, digital repression has been a consistent feature of governance since the early 2000s. In 2003, Egypt's DRI stood at 1.427—well above the global average—indicating an early adoption of repressive digital practices. The index steadily rose over the years, especially after the 2013 military coup, peaking at 1.574 in 2020 and remaining elevated at 1.523 in 2022. These figures confirm that digital repression in Egypt is not merely reactive to unrest but is deeply embedded in the state's broader strategy to maintain control over the population. The increase in the DRI reflects intensified censorship, surveillance, and arrests aimed at suppressing dissent and preserving political stability.

Alongside rising repression, Egypt's capacity to implement digital control measures also expanded. In 2003, the country's DRCI was 0.724, indicating a moderate ability to control the digital space. This capacity grew steadily, reaching 1.196 in 2014, 1.351 in 2020, and stabilizing at 1.103 in 2022. This upward trend reflects significant investments in surveillance infrastructure and cyber capabilities, especially following the Arab Spring, underscoring the regime's long-term commitment to controlling digital activity as social media platforms increasingly became key channels for political dissent and mobilization.

Similarly, Saudi Arabia has demonstrated a persistent and robust use of digital repression. Its DRI in 2003 was 1.477—higher than Egypt's—signaling an early and strong adoption of digital repression strategies. The index remained high over the years, peaking at 1.774 in 2016 and staying above 1.7 in subsequent years. These values highlight how digital repression has become a standard governance tool in Saudi Arabia, particularly under the leadership of Crown Prince Mohammed bin Salman. Saudi Arabia's DRCI follows a comparable trajectory, evidencing a highly developed capacity for digital repression. With a DRCI of 1.128 in 2013, Saudi Arabia already possessed a solid digital repression infrastructure, which further expanded to 1.743 in 2016 and 1.758 in 2022. This data positions Saudi Arabia among the countries with the most advanced digital repression systems worldwide.

When comparing Egypt and Saudi Arabia, clear similarities and differences emerge in both the intensity and evolution of digital repression. While both countries exhibit consistently high levels of digital control, Saudi Arabia has maintained slightly higher DRI and DRCI scores throughout the period, indicating a more entrenched and technologically advanced system of digital authoritarianism. Egypt, on the other hand, shows a more reactive pattern, with sharp increases in both indices following moments of political instability—most notably the 2013 military coup. This suggests that while repression in Egypt is deeply institutionalized, it is also

more tightly linked to periods of perceived regime vulnerability. In contrast, Saudi Arabia's approach appears more proactive and structurally embedded, reflecting its long-standing efforts to construct a sophisticated digital control apparatus as part of its broader state modernization and centralization strategy.

These trends are illustrated in *Figures 5*, which show the changes in the Digital Repression Index (DRI) and the Digital Repression Capacity Index (DRCI) for Egypt and Saudi Arabia, respectively, from 2003 to 2022. For a more detailed, country-specific view, *Figure 6* charts the evolution of both DRI and DRCI in Egypt and Saudi Arabia over the time frame 2003-2022. All corresponding yearly values for both indices are presented in *Table 4*, offering a comprehensive overview that enables year-by-year and country-to-country comparisons.

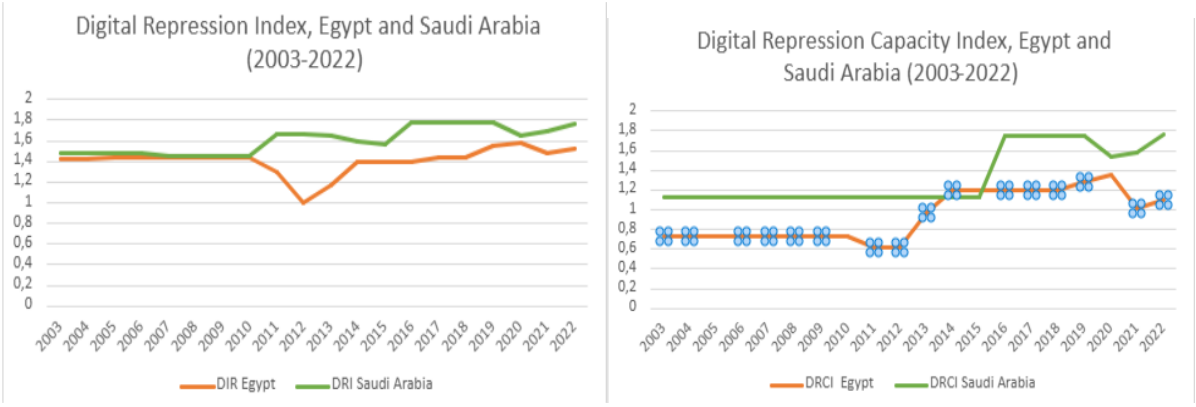

Figure 5: DRCI and DRI (2003-2022)

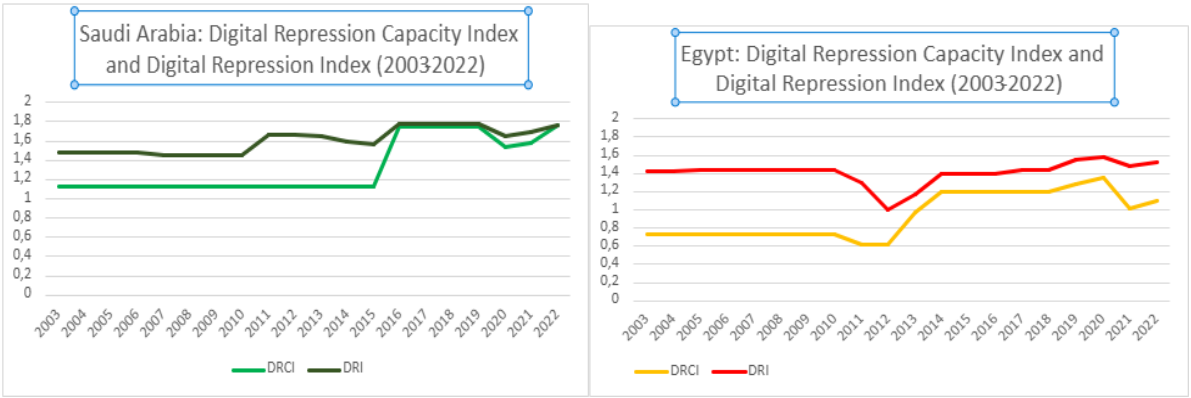

Figure 6: DRI and DRI (2003-2022)

In the case of Egypt, digital repression has followed a fluctuating trajectory shaped by the country's political instability and regime transitions. From 2003 to 2010, the DRI remained consistently high, ranging between 1.43 and 1.44, reflecting entrenched digital authoritarian practices under President Hosni Mubarak. A notable decline occurred in 2011 (1.30) and 2012

(0.99), coinciding with the aftermath of the Arab Spring and a brief period of democratic opening. However, this trend was short-lived. Following the 2013 military coup led by General Abdel Fattah el-Sisi, the DRI rose sharply, peaking at 1.57 in 2020 before slightly declining to 1.52 in 2022. This resurgence underscores a return to and intensification of digital repression, consistent with the regime's broader efforts to neutralize dissent and re-establish authoritarian control.

Similarly, Egypt's DRCI exhibits a clear upward trend, indicating the state's growing technical and institutional capacity to enforce digital control. Between 2003 and 2010, the DRCI remained stable at 0.72, suggesting a moderate level of infrastructural readiness. However, the index declined in 2011–2012 (0.62), reflecting the temporary weakening of state authority. Post-2013, the DRCI rose significantly, reaching 1.20 in 2014 and peaking at 1.35 in 2020, before stabilizing at 1.10 in 2022.

In contrast, Saudi Arabia presents a more stable and consistently high level of digital repression throughout the period. The DRI remained above 1.44 from 2003 onward, increasing steadily from 1.48 in the early 2000s to a peak of 1.77 between 2016 and 2018. The index remained elevated in subsequent years, reaching 1.68 in 2022. The DRCI in Saudi Arabia similarly reflects a strong and expanding capacity for digital repression. From 2003 to 2012, the index was consistently high at 1.13, indicating an early and robust infrastructure. Starting in 2013, the DRCI experienced a marked increase, rising to 1.28 and reaching 1.76 by 2022. This upward trajectory evidence significant state investment in cyber capabilities, positioning Saudi Arabia among the most technologically equipped authoritarian regimes globally. Egypt has undergone more pronounced fluctuations linked to periods of political transformation. Nonetheless, by the end of the observation period, both regimes converge toward similar patterns of high repression and advanced capacity, illustrating the entrenchment of digital authoritarianism as a central governance strategy.

year	Digital Repression Capacity Index Egypt	Digital Repression Capacity Index Saudi Arabia	Digital Repression Index Egypt	Digital Repression Index Saudi Arabia
2003	0,72	1,13	1,43	1,48
2004	0,72	1,13	1,43	1,48
2005	0,72	1,13	1,44	1,48
2006	0,72	1,13	1,44	1,48
2007	0,72	1,13	1,44	1,44
2008	0,72	1,13	1,44	1,44
2009	0,72	1,13	1,44	1,44
2010	0,72	1,13	1,44	1,44
2011	0,62	1,13	1,30	1,66
2012	0,62	1,13	0,99	1,66
2013	0,97	1,13	1,16	1,65
2014	1,20	1,13	1,39	1,59
2015	1,20	1,13	1,39	1,56
2016	1,20	1,74	1,39	1,77
2017	1,20	1,74	1,43	1,77
2018	1,20	1,74	1,43	1,77
2019	1,28	1,74	1,56	1,77
2020	1,35	1,54	1,57	1,66
2021	1,02	1,58	1,48	1,70
2022	1,10	1,76	1,52	1,76

Table 4: DRI and DRCI (2003-2022)

3.2.2. Egypt's Digital Repressive Tookit

To understand how digital repression operates in practice, three main surveillance indicators must be considered: government monitoring of social media, promotion of domestic digital platforms, and arrests related to online activity. In Egypt, government monitoring (*v2smgovsmmon*) has remained consistently high over the past decade, fluctuating between 1.597 and 1.685. The promotion of domestic platforms (*v2smgovdom*) has steadily increased, reaching 2.381 from 2019 to 2022. Arrests for online activity (*v2smarrest*) rose to 2.322 in 2019 and remained at that level through 2022.

These figures demonstrate that both surveillance and punitive measures targeting digital behavior are central components of the Egyptian state's repressive framework. *Table 5* and *Figure 7* present a detailed view of the evolution of Egypt's digital repression toolkit between 2003 and 2022, as captured by disaggregated indicators from the Digital Society Project and compiled into the Digital Repression Index. These indicators track specific mechanisms of digital control, including the capacity to filter political content online (*v2smgovfilpre*), shut down internet access (*v2smgovshut*), use pro-government online actors (*v2smgovsmmon*), regulate digital content and media (*v2smgovsmenprc*), and directly punish online dissent through arrests (*v2smarrest*), party dominated narratives across the media sphere (*v2smpardom*), or other coercive measures.

year	v2smgovfilprc	v2smgovshut	v2smgovsm	v2smgovsmcenprc	v2smgovdom	v2smpardom	v2smarrest	v2smgovsmmon	Digital Repression Index
2003	1,94	-0,06	1,52	1,79	1,19	1,39	1,86	1,92	1,43
2004	1,94	-0,06	1,52	1,79	1,19	1,39	1,86	1,92	1,43
2005	2,09	-0,06	1,52	1,79	1,19	1,39	1,78	1,92	1,44
2006	2,09	-0,06	1,52	1,79	1,19	1,39	1,78	1,92	1,44
2007	2,09	-0,06	1,52	1,79	1,19	1,39	1,78	1,92	1,44
2008	2,09	-0,06	1,52	1,79	1,19	1,39	1,78	1,92	1,44
2009	2,09	-0,06	1,52	1,79	1,19	1,39	1,78	1,92	1,44
2010	2,09	-0,06	1,52	1,79	1,19	1,39	1,78	1,92	1,44
2011	0,89	0,87	1,59	1,52	1,31	1,44	1,19	1,10	1,30
2012	0,90	-0,94	0,44	1,52	1,48	1,44	1,09	1,60	0,99
2013	1,06	-0,94	0,78	1,52	1,78	1,44	1,94	1,60	1,16
2014	1,98	0,41	0,96	1,22	1,78	1,16	1,95	1,69	1,39
2015	1,98	0,41	0,96	1,22	1,78	1,16	1,95	1,69	1,39
2016	1,98	0,41	0,96	1,22	1,78	1,16	1,95	1,69	1,39
2017	1,98	0,41	1,28	1,22	1,78	1,16	1,95	1,69	1,43
2018	1,98	0,41	1,28	1,22	1,78	1,16	1,95	1,69	1,43
2019	2,11	0,99	1,02	1,22	2,38	1,16	2,32	1,38	1,56
2020	1,65	0,99	1,40	1,22	2,38	1,12	2,32	1,62	1,57
2021	2,35	0,32	0,68	1,22	2,38	1,12	2,32	1,62	1,48
2022	2,35	0,32	1,01	1,22	2,38	1,12	2,32	1,62	1,52

Table 5: Egypt's Digital Repressive Toolkit (2003-2022)

A longitudinal examination of Table 5 reveals several key trends. Egypt's filtering capacity (*v2smgovfilpre*) remained high and relatively stable from 2003 to 2010, ranging from 1.94 to 2.09. However, it dropped significantly in 2011 (0.89) and 2012 (0.87), aligning with the brief democratic opening during the post-Mubarak transition. However, this indicator resurged post-2013, reaching 2.35 by 2021 and 2022, signaling a renewed commitment to online censorship. A similar pattern is evident in the government's ability to shut down digital communications (*v2smgovshut*), which was negligible before 2015 but rose sharply thereafter, peaking at 0.99 in 2019 before slightly declining to 0.32 in 2022—reflecting increased, though still episodic, reliance on internet shutdowns.

The use of pro-government commentators (*v2smgovsmmon*) remained high and constant across the two decades, indicating persistent reliance on state-sponsored narratives to shape online discourse. Indicators related to regulatory capacity (*v2smgovsmenprc*) and control over online media outlets (*v2smgovdom*) demonstrate a progressive strengthening, especially post-2013, with both reaching their peak values (1.22 and 2.38, respectively) in the later years of the dataset. Furthermore, coercive tactics such as online-related arrests (*v2smarrest*) spiked after 2013, with values reaching 2.32 in 2021, underlining the regime's increasing use of punitive methods to deter digital dissent.

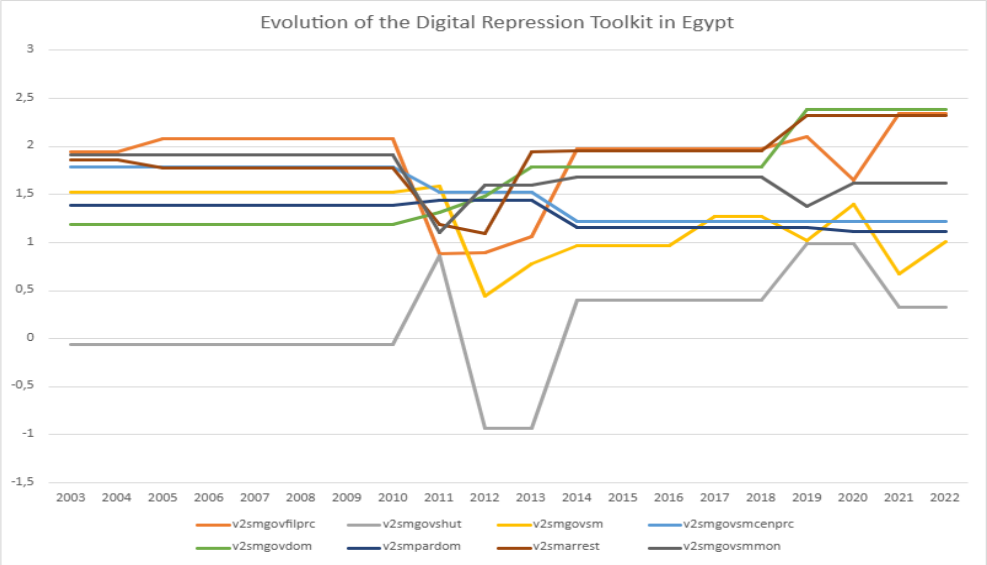

Figure 7: Egypt Digital Repressive Toolkit (2003-2022)

Table 6 and *Figure 8* illustrate the development of Egypt's Digital Repression Capacity Index (DRCI) between 2003 and 2022 by disaggregating its four core components: government filtering capacity (*v2smgovfilcap*), internet shutdown capacity (*v2smgovshutcap*), cybersecurity capacity (v2smgovcapsec), and regulatory capacity over digital platforms (*v2smregcap*). These indicators offer a granular view of the institutional, technical, and regulatory capabilities underpinning Egypt's ability to control its digital environment. From 2003 to 2010, Egypt's digital repression capacity remained largely static, with the DRCI consistently at 0.72. This reflects a moderate but stable baseline capacity, largely built around filtering (*v2smgovfilcap* = 0.63) and modest regulatory oversight (*v2smregcap* = 1.45). However, the sharp decline in 2011 and 2012—years marked by political upheaval and a brief democratic transition—reveals a momentary weakening of state control over digital space. Notably, filtering and shutdown capacity dropped (to 0.52 and -0.67, respectively), and the overall DRCI fell to its lowest levels (0.62 in 2011 and 0.63 in 2012), highlighting the temporary disruption of the state's digital apparatus. A turning point occurred in 2013, when the military-led reassertion of authoritarian control led to a significant increase in digital repression capacity. Filtering capacity jumped from 0.52 to 1.47, and the DRCI rose to 0.97. This upward trajectory continued sharply in 2014 and stabilized at 1.20 between 2014 and 2018, corresponding to major state investments in digital governance mechanisms. During this period, all core indicators reached higher values: shutdown capacity turned positive (0.76), cybersecurity infrastructure was reinforced (v2smgovcapsec ≈ 1.01), and regulatory authority remained constant. A second growth phase in capacity was observed between 2019 and 2020, with the DRCI peaking at 1.35 in 2020. This increase was largely driven by enhancements in cybersecurity (*v2smgovcapsec* = 1.59) and

sustained regulatory strengthening (*v2smregcap* = 1.56). Although a slight decline is seen in 2021 (DRCI = 1.02), the index remains elevated relative to the early 2000s, indicating a robust and durable infrastructure of digital repression. By 2022, filtering capacity dropped to 0.74 from its earlier highs, but both shutdown and cybersecurity capabilities remained strong, keeping the DRCI at a relatively high 1.10.

year	v2smgovfilcap	v2smgovshutcap	v2smgovcapsec	v2smregcap	Digital Repression Capacity Index
2003	0,63	-0,43	1,02	1,45	0,72
2004	0,63	-0,43	1,02	1,45	0,72
2005	0,63	-0,43	1,02	1,45	0,72
2006	0,63	-0,43	1,02	1,45	0,72
2007	0,63	-0,43	1,02	1,45	0,72
2008	0,63	-0,43	1,02	1,45	0,72
2009	0,63	-0,43	1,02	1,45	0,72
2010	0,63	-0,43	1,02	1,45	0,72
2011	0,52	-0,67	0,83	1,45	0,62
2012	0,52	-0,67	0,83	1,45	0,62
2013	1,47	-0,09	0,83	1,45	0,97
2014	1,70	0,76	1,01	1,45	1,20
2015	1,70	0,76	1,01	1,45	1,20
2016	1,70	0,76	1,01	1,45	1,20
2017	1,70	0,76	1,01	1,45	1,20
2018	1,70	0,76	1,01	1,45	1,20
2019	1,70	0,89	1,35	1,45	1,28
2020	1,70	0,89	1,59	1,56	1,35
2021	0,74	0,89	1,23	1,56	1,02
2022	0,74	0,89	1,69	1,56	1,10

Table 6: Egypt's Digital Repressive Capacity Toolkit (2003-2022)

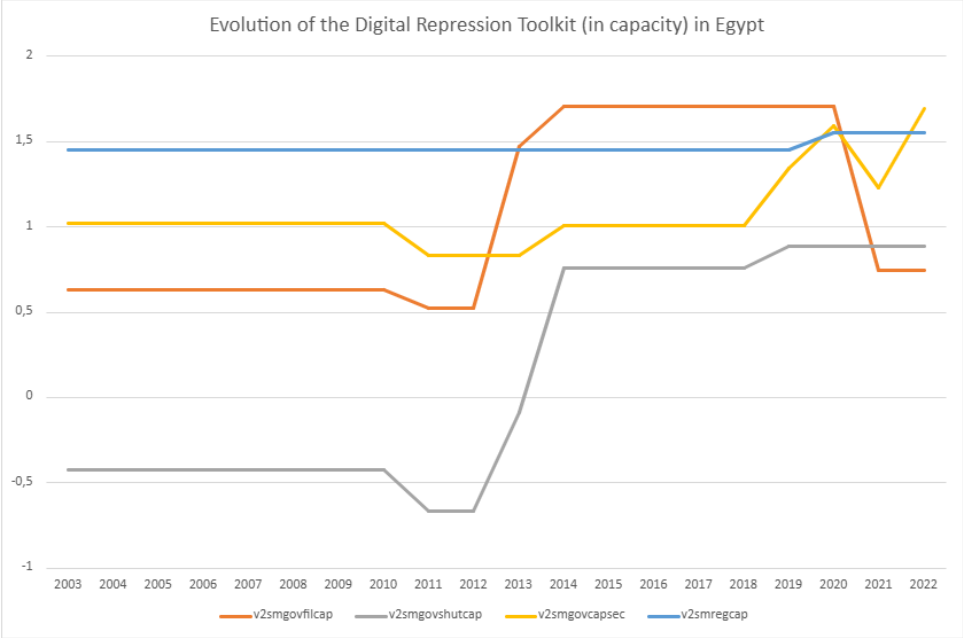

Figure 8: Egypt's Digital Repressive Capacity Toolkit (2003-2022)

3.2.3. Saudi Arabia's Digital Repressive Tookit

In Saudi Arabia, these surveillance indicators reach even higher intensities. Social media monitoring peaked at 3.431 between 2016 and 2019, placing it among the highest levels recorded worldwide. This indicates that Saudi Arabia has developed one of the most advanced

surveillance infrastructures globally, enabling it to closely track online discussions and suppress political opposition, especially criticism directed at the monarchy. The promotion of domestic digital platforms also remained strong, with scores exceeding 2.4 from 2013 to 2015, reinforcing the kingdom's strategy to shape the digital environment in alignment with state interests. Arrests related to online expression stayed consistently high at 1.977 from 2013 through 2022, underscoring how legal enforcement against digital dissent has been a continuous and central element of Saudi Arabia's approach to controlling online speech and preserving political stability. These patterns reveal a precise alignment between the capacity for digital repression and its active deployment in both Egypt and Saudi Arabia. While some states may possess sophisticated technological tools for repression but choose not to fully utilize them, both Egypt and Saudi Arabia consistently leverage their extensive repressive infrastructures to dominate the digital sphere and silence dissent.

Table 7 and *Figure 9* display the evolution of the digital repression toolkit in Saudi Arabia from 2003 to 2022, alongside the aggregated Digital Repression Index. The longitudinal analysis reveals significant shifts in Saudi Arabia's digital repression strategies. For instance, *v2smgovfilprc* saw a notable increase, moving from 2.05 in 2003 to 3.43 by 2022, indicating a hardening stance on online censorship. Similarly, *v2smgovshut* fluctuated but remained a potent tool, reaching 2.38 in 2016 before settling at 1.33 in later years. The deployment of pro-government online actors to influence narratives (*v2smgovsmmon*) also shows a marked rise, from 2.45 in 2003 to 3.39 in 2021 and 2022, suggesting a more sophisticated and pervasive online narrative control. While direct punishment of activism on social media (*v2smarrest*) remained consistently high at 1.98 for most of the period, the *v2smpardom* indicator showed a slight decline from -1.34 to -1.68, hinting at a potential shift in how information is controlled or measured. Overall, the Digital Repression Index itself demonstrates an upward trend, rising from 1.48 in 2003 to 1.76 in 2022, underscoring a consistent expansion and refinement of Saudi Arabia's digital control capabilities over two decades.

year	v2smgovfilprc	v2smgovshut	v2smgovsm	v2smgovsmcenprc	v2smgovdom	v2smpardom	v2smarrest	v2smgovsmmon	Digital Repression Index
2003	2,05	1,26	1,78	1,05	1,48	-1,34	1,98	2,45	1,48
2004	2,05	1,26	1,78	1,05	1,48	-1,34	1,98	2,45	1,48
2005	2,05	1,26	1,78	1,05	1,48	-1,34	1,98	2,45	1,48
2006	2,05	1,26	1,78	1,05	1,48	-1,34	1,98	2,45	1,48
2007	2,05	1,26	1,55	1,05	1,48	-1,34	1,98	2,45	1,44
2008	2,05	1,26	1,55	1,05	1,48	-1,34	1,98	2,45	1,44
2009	2,05	1,26	1,55	1,05	1,48	-1,34	1,98	2,45	1,44
2010	2,05	1,26	1,55	1,05	1,48	-1,34	1,98	2,45	1,44
2011	2,05	1,79	1,74	1,16	2,42	-1,34	1,98	2,45	1,66
2012	2,05	1,79	1,74	1,16	2,42	-1,34	1,98	2,45	1,66
2013	2,05	1,79	1,74	1,04	2,42	-1,34	1,98	2,45	1,65
2014	2,05	1,24	1,74	1,04	2,42	-1,34	1,98	2,45	1,59
2015	2,05	1,24	1,56	1,04	2,42	-1,34	1,98	2,45	1,56
2016	2,05	2,38	1,57	1,30	2,35	-1,34	1,98	3,43	1,77
2017	2,69	1,51	1,73	1,30	2,35	-1,34	1,98	3,43	1,77
2018	2,69	1,51	1,73	1,30	2,35	-1,34	1,98	3,43	1,77
2019	2,69	1,51	1,73	1,30	2,35	-1,34	1,98	3,43	1,77
2020	2,64	1,33	1,73	1,26	2,01	-1,34	1,98	2,78	1,66
2021	2,64	1,33	1,73	1,26	2,01	-1,34	1,98	3,39	1,70
2022	3,43	1,33	1,69	1,26	2,01	-1,68	1,98	3,39	1,76

Table 7: Saudi Arabia's Digital Repressive Toolkit (2003-2022)

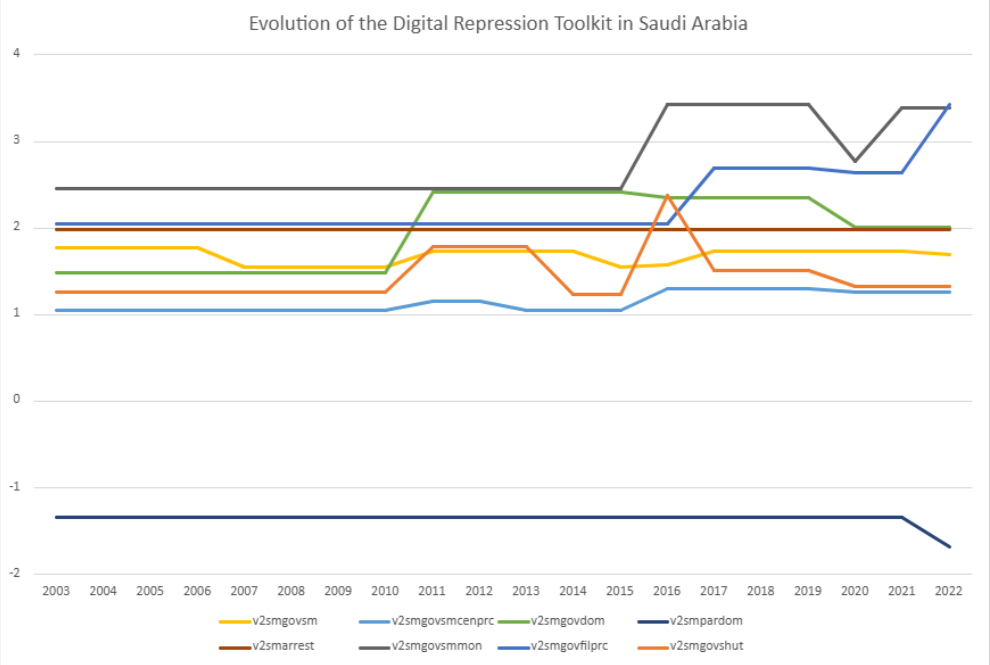

Figure 9: Saudi Arabia's Digital Repressive Toolkit (2003-2022)

Table 8 and *Figure 10* illustrate the evolution of Saudi Arabia's Digital Repression Capacity Index (DRCI) from 2003 to 2022. The analysis reveals a significant surge in Saudi Arabia's digital repression capacity, particularly after 2015. For example, *v2smgovfilcap* jumped from a stable 1.30 between 2003 and 2015 to 2.40 from 2016 onwards, indicating a substantial enhancement in the ability to block undesirable content. Similarly, shutdown capacity (*v2smgovshutcap*) saw a dramatic increase, rising from 0.73 in the earlier period to 1.34 in 2016-2019, and then reaching a peak of 2.18 in 2022, suggesting an intensified capability to disrupt internet access. Cybersecurity capacity (*v2smgovcapsec*) also showed marked improvement, moving from 1.50 in the 2003-2015 period to 1.88 between 2016 and 2019, and

then slightly declining to 1.73 in the subsequent years. Regulatory capacity on social media (*v2smregcap*) increased from 1.31 to 1.84 in 2016, then stabilized at 1.54 from 2020 onwards, reflecting a strengthened legal and administrative framework for controlling online discourse. Overall, the Digital Repression Capacity Index itself demonstrates a clear upward trajectory, rising from 1.13 in 2003 to 1.76 in 2022. This longitudinal analysis underscores a deliberate and sustained investment by Saudi Arabia in expanding its technical and regulatory infrastructure for digital control, signifying a growing sophistication in its approach to digital repression.

year	v2smgovfilcap	v2smgovshutcap	v2smgovcapsec	v2smregcap	Digital Repression Capacity Index
2003	1,30	0,73	1,50	1,31	1,13
2004	1,30	0,73	1,50	1,31	1,13
2005	1,30	0,73	1,50	1,31	1,13
2006	1,30	0,73	1,50	1,31	1,13
2007	1,30	0,73	1,50	1,31	1,13
2008	1,30	0,73	1,50	1,31	1,13
2009	1,30	0,73	1,50	1,31	1,13
2010	1,30	0,73	1,50	1,31	1,13
2011	1,30	0,73	1,50	1,31	1,13
2012	1,30	0,73	1,50	1,31	1,13
2013	1,30	0,73	1,50	1,31	1,13
2014	1,30	0,73	1,50	1,31	1,13
2015	1,30	0,73	1,50	1,31	1,13
2016	2,40	1,34	1,88	1,84	1,74
2017	2,40	1,34	1,88	1,84	1,74
2018	2,40	1,34	1,88	1,84	1,74
2019	2,40	1,34	1,88	1,84	1,74
2020	2,40	0,97	1,53	1,54	1,54
2021	2,40	0,97	1,73	1,54	1,58
2022	2,40	2,18	1,73	1,54	1,76

Table 8: Saudi Arabia's Digital Repressive Toolkit (2003-2022)

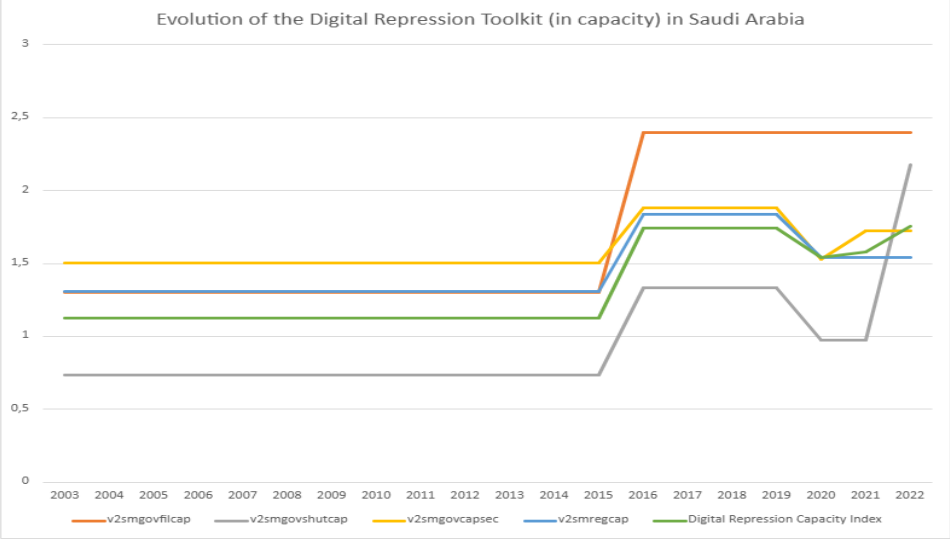

Figure 10: Saudi Arabia's Digital Repressive Toolkit (2003-2022)

3.2.4. Key Dimensions in Digital Repression

In addition to these key indicators, this analysis also considers four other crucial dimensions of digital repression: filtering capacity, shutdown capacity, regulatory capacity, and the use of

alternative government-controlled social media accounts. Egypt's filtering capacity (*v2smgovfilcap*) peaked at 2.058 in 2020 before declining to 1.216 from 2021 onward. This drop suggests that while the state still retains the ability to filter content, it may have shifted towards more targeted and less overt forms of control, focusing on specific individuals or topics. Egypt's shutdown capacity (*v2smgovshutcap*) has remained relatively low at 0.624, indicating that although the government can execute internet blackouts, it rarely relies on full-scale shutdowns even during politically sensitive times. The regulatory capacity (*v2smregcap*) has been steady at 1.203 from 2020 through 2024, reflecting a solid legal framework enabling the implementation of digital regulations. Notably, Egypt's use of alternative government-controlled social media accounts (*v2smgovsmalt*) has stayed low at -0.879 during the same period, implying that the regime favors more direct repression methods—such as surveillance and arrests—over covert manipulation through fake accounts. *Figure 11* displays the longitudinal analysis of the evolution of these key indexes in Egypt from 2000 to 2024, with *Table 10* providing the reference values for completeness.

year	v2smgovfilcap	v2smgovshutcap	v2smregcap	v2smgovsmalt
2000	0,12	0,12	1,29	-0,63
2001	0,12	0,12	1,29	-0,63
2002	0,12	0,12	1,29	-0,63
2003	0,12	0,12	1,29	-0,63
2004	0,12	0,12	1,29	-0,63
2005	0,12	0,12	1,29	-0,63
2006	0,12	0,12	1,29	-0,63
2007	0,51	0,51	1,29	-0,63
2008	0,51	0,51	1,29	-0,63
2009	0,51	0,51	1,29	-0,63
2010	0,67	0,67	1,29	-0,63
2011	0,55	0,55	1,29	-0,29
2012	0,55	0,55	1,29	-0,29
2013	1,37	1,37	1,29	-0,29
2014	2,06	2,06	1,29	-0,58
2015	2,06	2,06	1,29	-0,58
2016	2,06	2,06	1,29	-0,58
2017	2,06	2,06	1,29	-0,58
2018	2,06	2,06	1,29	-0,58
2019	2,06	2,06	1,29	-0,58
2020	2,06	2,06	1,20	-0,88
2021	1,22	0,62	1,20	-0,88
2022	1,22	0,62	1,20	-0,88
2023	1,22	0,62	1,20	-0,88
2024	1,22	0,62	1,20	-0,88

Table 9: Egypt Key Idexes of Digital Repression (2000-2024)

These figures collectively suggest a calculated and adaptive approach by the Egyptian regime to digital control. The decline in filtering capacity post-2020, coupled with consistently low shutdown capacity and the preference for direct repression over online manipulation, indicates a strategic shift towards more precise and less disruptive methods of digital authoritarianism. This implies that Egypt is refining its digital control strategies, moving away from broad, blunt

instruments towards more sophisticated and potentially less visible forms of surveillance and enforcement that may better align with maintaining a semblance of stability while still quashing dissent.

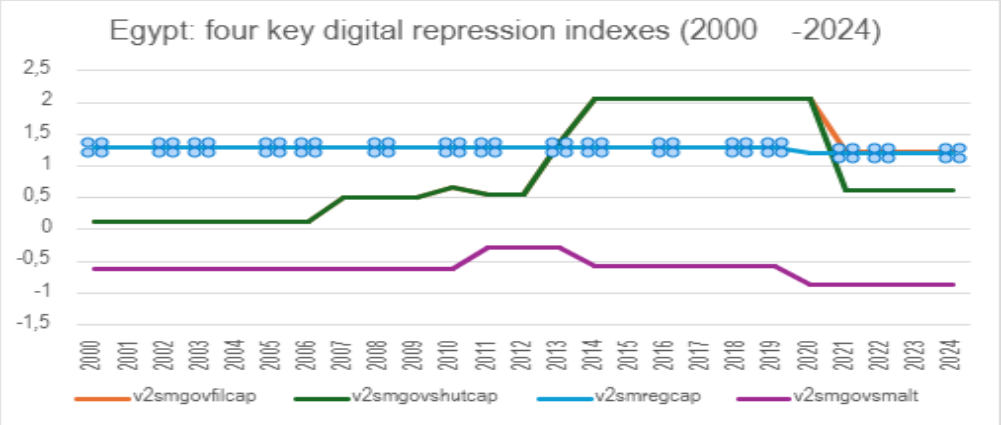

Figure 11: Egypt Key Idexes of Digital Repression (2000-2024)

Saudi Arabia demonstrates an even more advanced approach to digital repression. Its filtering capacity (*v2smgovfilcap*) remained high, reaching 2.559 between 2020 and 2023, before slightly declining to 2.063 in 2024. This elevated level of filtering reflects the kingdom's strong control over online content and its efforts to ensure digital information aligns closely with the state's official narrative. The shutdown capacity (*v2smgovshutcap*) increased markedly from 1.814 in 2020–2021 to 2.266 during 2022–2024, highlighting the state's enhanced ability to carry out comprehensive internet shutdowns in times of unrest or political dissent. Saudi Arabia's regulatory capacity (*v2smregcap*) also grew, rising from 1.838 in 2020 to 2.153 in 2022–2024, underscoring the robustness of its legal framework for digital repression. Finally, the kingdom's use of alternative government-controlled social media accounts (*v2smgovsmalt*) remained extremely low, with values ranging from -1.983 to -2.238, indicating a preference for overt control methods such as direct surveillance rather than covert manipulation via fake accounts.

Figure 12 display the longitudinal analysis of the evolution of these key indexes in Saudi Arabia from 2000 to 2024, with *Table 10* providing the reference values for completeness. The consistently high filtering capacity, coupled with a significant increase in shutdown and regulatory capacities, points to a regime that prioritizes comprehensive and direct control over the digital sphere. The extremely low reliance on covert social media manipulation further emphasizes a preference for overt, state-led repression, indicating a deep integration of digital control within the broader framework of state power and its legal apparatus. This suggests Saudi

Arabia is not just reactive but proactively building a robust and resilient digital authoritarian infrastructure to maintain its political and social order.

year	v2smgovfilcap	v2smgovshutcap	v2smregcap	v2smgovsmalt
2000	1,36	0,50	0,99	-2,16
2001	1,36	0,50	0,99	-2,16
2002	1,36	0,50	0,99	-2,16
2003	1,36	0,50	0,99	-2,16
2004	1,36	0,50	0,99	-2,16
2005	1,36	0,50	0,99	-2,16
2006	1,36	0,50	0,99	-2,16
2007	1,36	0,50	0,99	-2,16
2008	1,36	0,50	0,99	-2,16
2009	1,36	0,50	0,99	-2,16
2010	1,36	0,50	0,99	-2,16
2011	1,36	0,50	0,99	-2,16
2012	1,64	0,50	1,22	-2,16
2013	1,64	0,50	1,22	-2,16
2014	1,64	0,50	1,22	-2,16
2015	1,93	0,83	1,57	-2,16
2016	2,56	1,20	2,02	-2,32
2017	2,56	1,20	2,02	-2,32
2018	2,56	2,29	2,02	-2,32
2019	2,56	2,29	2,02	-2,32
2020	2,56	1,81	1,84	-1,98
2021	2,56	1,81	1,84	-1,98
2022	2,56	2,27	2,15	-2,24
2023	2,56	2,27	2,15	-2,24
2024	2,06	2,27	2,15	-2,24

Figure 12: Saudi Arabia Key Idexes of Digital Repression (2000-2024)

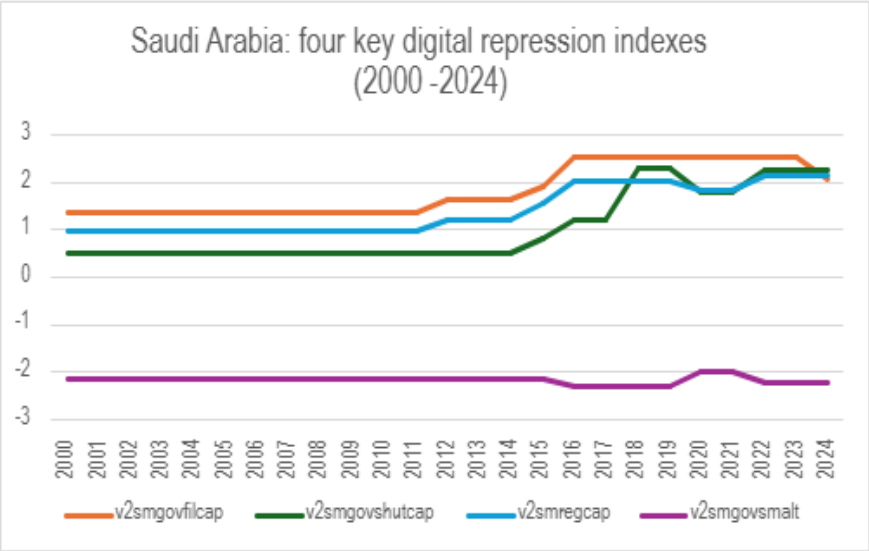

Figure 13: Saudi Arabia Key Idexes of Digital Repression (2000-2024)

In conclusion, Egypt and Saudi Arabia have developed their own sophisticated systems of digital repression. However, while Egypt's approach has evolved over time, Saudi Arabia has maintained a highly advanced and consistent strategy of digital repression.

3.3. Part 3 – Geopolitical Relationships with China and the US

This section examines the increasing adoption of AI surveillance technologies in Egypt and Saudi Arabia, with a focus on how their digital repression strategies are shaped by geopolitical

relationships, particularly those with the United States and China. By analyzing 2021 data, it highlights how these technologies are leveraged to bolster state control, with a particular emphasis on the role of strategic international partnerships—especially with China—in enhancing their surveillance capabilities.

In 2021, Saudi Arabia recorded a Digital Repression Index (DRI) of 1.501954, indicating a high level of digital control. This aligns with its Freedom on the Net status, where it was classified as "Not Free," with a score of 24, reflecting significant restrictions on online freedoms. Saudi Arabia's military expenditures, totalling $67.55 billion in 2018, ranked the country third globally, highlighting its substantial investments in defence and digital surveillance infrastructure.

A pivotal factor in the evolution of AI surveillance in Saudi Arabia is the relationship with China. As a participant in China's Belt and Road Initiative (BRI), Saudi Arabia has gained access to China's advanced surveillance technologies. Notably, companies like Hikvision, a Chinese multinational, provide vital technologies for Saudi Arabia's surveillance infrastructure, including video analytics and crowd monitoring systems. These technologies are integral to Saudi Arabia's AI-powered policing efforts and its broader strategy to control public and private spaces through digital means.

China's Ongoing Developmental Initiative (ODI) further bolsters Saudi Arabia's digital surveillance capacity by facilitating access to advanced high-tech infrastructure. In addition to Chinese partnerships, Saudi Arabia has collaborated with international technology companies such as NEC (Japan), BriefCam (Israel), and Hugslock (Hong Kong) to expand its surveillance systems. These collaborations allow Saudi Arabia to integrate a diverse array of surveillance technologies that reinforce its efforts to maintain state control. For example, NEC's AI-powered video analytics are essential for monitoring public spaces, analyzing behavior patterns, and identifying individuals, particularly in crowded settings like airports. Similarly, BriefCam's tools enable rapid video content review and analysis, playing a critical role in urban surveillance. Hugslock specializes in crowd monitoring and real-time detection of security threats, further enhancing Saudi Arabia's surveillance capabilities.

According to the Belt and Road Portal, Saudi Arabia's economy remains heavily dependent on oil, holding the world's largest proven crude oil reserves. However, the ongoing Vision 2030 reforms—designed to diversify the economy—are expected to foster growth in the short to medium term. Despite these efforts, the country's public finances remain sensitive to global energy price fluctuations and oil production cuts. These economic pressures may accelerate the

implementation of Vision 2030 reforms, driving Saudi Arabia to bolster its non-oil sectors, including AI surveillance and cybersecurity, while deepening its cooperation with global powers such as China.

While Egypt's digital repression is similarly significant, its DRI of 1.269670 in 2021 suggests slightly lower levels of repression compared to Saudi Arabia. Nevertheless, Egypt was also classified as "Not Free" on the Freedom on the Net index, with a score of 26, reflecting considerable restrictions on online freedoms. Egypt's military spending in 2018 was much lower, at $3.11 billion, placing it 51st globally in military expenditure. However, Egypt's growing ties with China, particularly in the realm of digital infrastructure development, highlight the strategic importance of these relations. Chinese companies, notably Huawei, play a pivotal role in Egypt's surveillance capabilities. Huawei's technologies, including facial recognition systems and social media monitoring tools, are integrated into Egypt's Safe City projects, which aim to enhance surveillance and control in urban areas. Additionally, Honeywell, an American company, complements Huawei's systems, further strengthening Egypt's national security infrastructure.

China's contributions to Egypt's technological advancement go beyond telecommunications and monitoring. Substantial financial support, including the $500 million syndicated loan to Telecom Egypt in 2018, has supported Egypt's extension of its 4G network, which holds prime importance in terms of its competitiveness in the digital age. The loan, facilitated by the Industrial and Commercial Bank of China (ICBC), allowed Telecom Egypt to cover its operational costs and fund extended investments in key infrastructure, including Egypt's digital communications capacities.

Egypt, as reported by the U.S. State Department, has also depended upon U.S. companies, including Honeywell, for crucial security and monitoring technologies, which supplement those given by Chinese companies. These partnerships only serve to point towards an increasingly dominant role for both China and the U.S. in determining Egypt's digital future, though in different areas of technology.

China's reach also covers Egypt's space industry. One of its high-profile projects was the building of the Egyptian Satellite Assembly, Integration, and Testing Center in New Cairo, funded by a RMB 146 million (or about $23 million) grant from China's government. This facility allows Egypt to have its own infrastructure to assemble, integrate, and test its own satellites, giving Egypt more autonomy in space activities. This is a distinct illustration of

China's sustained strategic interest in Egypt, which is to advance the technological capabilities of Egypt in telecommunications as well as space systems.

Aside from these infrastructure developments, China has also funded Egypt's satellite remote sensing facilities. It committed a grant of RMB 30 million (around $4.5 million) in 2015 to assist Egypt's National Authority for Remote Sensing and Space Sciences (NARSS), increasing the nation's capabilities in Earth observation as well as in monitoring of the environment.

Egypt's increasing cooperation with China mirrors a wider geopolitical trend towards more integration between China and Middle Eastern countries. China's technological collaborations, particularly in telecommunications, artificial intelligence monitoring, and satellite technology, are a foundation of Egypt's efforts to modernize itself and a key component in its national strategy. China's foray into Egypt's technology infrastructure also forms part of its wider Belt and Road project aimed at deeper connectivity and economic integration in Africa and the Middle East.

Although a role for the United States exists in the world of surveillance, via entities such as Honeywell, its presence in Saudi Arabia's and Egypt's surveillance system is less overt than China's. Furthermore, both Egypt and Saudi Arabia have depended upon spyware to expand their monitoring ambitions. Commercial spyware companies such as NSO Group (Israel), FinFisher (Germany), and Hacking Team (Italy) have been connected to spying activities in both nations, which underlines international aspects of digital repression. Pegasus spyware has been employed in Egypt to spy on dissidents as well as to watch over political opponents. Saudi Arabia, in turn, used NSO Group’s capabilities to hack dissident cellphones, which once more illustrates that these nations are utilizing both internal as well as international technology to exert control over their people.

In conclusion, the data show that Egypt and Saudi Arabia’s adoption of AI surveillance technologies is shaped by a complex network of international partnerships beyond just major powers like the United States and China. These diverse collaborations play a crucial role in defining their surveillance strategies, allowing both countries to strengthen domestic control while broadening their global ties. As they further develop AI-driven monitoring systems, these alliances will likely continue to evolve, enhancing their influence in the digital age.

3.4. Evaluation of Hypothesis

The central research inquiry animates this investigation: *How do Arab authoritarian regimes leverage surveillance technology to strengthen their economic and technological partnerships*

with global powers? This inquiry is pivotal for elucidating the dual utility of surveillance technology by Egypt and Saudi Arabia: as an instrument for domestic regulatory consolidation and concurrently as a conduit for augmenting strategic alliances with prominent global actors, notably the United States and China.

The investigative framework is structured by two primary hypotheses:

- *H1a*: Augmented investments in surveillance technology by Egyptian and Saudi Arabian state apparatuses are posited to correlate with an intensification of technological cooperation with the United States and the People's Republic of China.
- *H1b*: Elevated investments in surveillance technology by these regimes are hypothesized to correspond with an expansion of economic agreements with the United States and the People's Republic of China.

The empirical examination of these hypotheses concentrates on the independent variable, defined as the adoption of and investment in surveillance technologies, and its relationship with the dependent variables: the scope and depth of technological and economic cooperation with the United States and China. Preceding sections have delineated the mechanisms through which both regimes have integrated surveillance technologies, serving the dual purpose of consolidating domestic sovereign control and cultivating more profound engagements with these hegemonic powers.

3.4.1. Technological Cooperation

Hypothesis H1a posits that augmented state investments in surveillance technologies by Egypt and Saudi Arabia serve to deepen their technological interdependence and collaborative ventures with the United States and China. A greater reliance by these regimes on sophisticated surveillance apparatuses is presumed to facilitate their progressive integration into the expansive technological ecosystems architected by these global powers.

In the Egyptian context, technological cooperation with the United States manifests, inter alia, through strategic agreements with multinational corporations such as Honeywell, a purveyor of critical security technologies. These collaborations are instrumental not only in augmenting Egypt’s indigenous surveillance infrastructure but also in fortifying bilateral ventures, facilitating military-technology transfers, and advancing collaborative cybersecurity initiatives. Egypt’s strategic engagement with China, notably its participation within the framework of the Belt and Road Initiative (BRI), has been a significant catalyst for its technological advancement. Prominent Chinese enterprises, exemplified by Huawei, furnish advanced

surveillance capabilities, encompassing facial recognition systems and social media monitoring apparatuses, thereby further entrenching Egypt within China's sphere of technological influence. This bilateral relationship has consequently fostered numerous joint ventures and facilitated technology transfers, particularly within the telecommunications sector and the domain of digital governance.

Analogously, Saudi Arabia has systematically expanded its technological cooperation with both global powers, underpinned by substantial state investments in its national surveillance infrastructure. Partnerships with leading technology firms, including Hikvision and NEC, exemplify the Kingdom's strategic commitment to developing robust surveillance systems congruent with its overarching internal security objectives. These engagements underscore Saudi Arabia's multifaceted strategy of deepening technological cooperation with China, whilst concurrently sustaining established ties with the United States through corporations like Honeywell, which provide critical surveillance and cybersecurity solutions. An observable growth in bilateral agreements, joint research initiatives, and military-technology transfers serves as a tangible reflection of this expanding technological cooperation. Consequently, the escalating investments in surveillance technologies by both Egypt and Saudi Arabia appear to have substantively facilitated their deeper integration into the technological ecosystems of the United States and China, thereby reinforcing multifaceted bilateral cooperation.

3.4.2. Economic Cooperation

Hypothesis H1b investigates the proposition that the adoption and deployment of surveillance technologies by Egypt and Saudi Arabia correlate with an augmentation of economic cooperation with the United States and China. It is posited that as these nations bolster their surveillance capacities, they concurrently endeavor to deepen economic interdependencies through expanded trade agreements, increased inflows of foreign direct investment (FDI), and the execution of significant infrastructure projects, particularly those with embedded surveillance-related technological components.

Within the Egyptian context, investments in surveillance technologies are observed to have concurrently reinforced both technological and economic cooperation frameworks with China and the United States. The provision of a $500 million syndicated loan to Telecom Egypt by the Industrial and Commercial Bank of China (ICBC) in 2018 serves as a salient example of the intertwining of digital infrastructure investments with broader economic agreements. This financial instrument enabled the substantive expansion of Egypt's 4G network infrastructure,

thereby enhancing its competitive posture within the global digital economy. The integration of Chinese technological systems has further catalyzed trade and investment flows, contributing significantly to smart city development initiatives and cybersecurity enhancement projects articulated within Egypt's BRI-aligned national development strategies. Economic cooperation with the United States is analogously buttressed through strategic partnerships with American corporations, such as Honeywell, which furnish essential security and surveillance technologies. These collaborations constitute an integral component of Egypt's overarching economic strategy, aimed at securing access to foreign direct investment, fostering infrastructure development projects, and facilitating technology exchanges, all of which contribute to the deepening of bilateral ties with the United States.

Saudi Arabia's ambitious 'Vision 2030' economic diversification agenda similarly integrates substantial investments in surveillance technology, a factor that appears to reinforce economic cooperation with both China and the United States. Chinese enterprises, including prominent entities like Huawei and Hikvision, have made significant contributions to the Kingdom's smart city initiatives and the expansion of its cybersecurity and telecommunications sectors, thereby attracting considerable Chinese investment into non-oil segments of the Saudi economy. Concurrently, Saudi Arabia cultivates robust economic linkages with the United States, particularly within the strategic domains of defense, cybersecurity, and technology transfer, wherein corporations such as Honeywell and NEC assume pivotal roles. Such collaborations have demonstrably resulted in expanded trade agreements, augmented investment inflows, and significant infrastructure development, thereby further solidifying multifaceted economic cooperation with both global powers.

Conclusion

The findings confirm that growing investments in surveillance technologies by Egypt and Saudi Arabia serve not only to reinforce domestic control but also to foster deeper technological and economic cooperation with the USA and China. Adoption of advanced surveillance systems has integrated these countries more closely into the technological ecosystems of these global powers, enabling joint ventures, bilateral agreements, and military-technology collaborations that strengthen technological ties. Simultaneously, the economic benefits of these investments are evident in increased FDI, trade agreements, and infrastructure projects, particularly in telecommunications, cybersecurity, and smart infrastructure. Surveillance technology thus emerges as both an instrument of internal governance and a lever for enhancing international

cooperation, positioning Egypt and Saudi Arabia as influential actors in the global digital economy and geopolitical landscape.

Conclusion

This thesis has investigated the multifaceted role of digital surveillance technologies in authoritarian regimes of the Middle East and North Africa, focusing on Egypt and Saudi Arabia as emblematic cases. By combining a thorough theoretical framework with a comprehensive empirical analysis, it has shown how digital surveillance operates as both an instrument of domestic political repression and a strategic asset leveraged to foster technological and economic cooperation with major global powers.

The shift from traditional surveillance methods to advanced digital technologies—such as artificial intelligence, biometrics, spyware, and big data analytics—has fundamentally transformed authoritarian governance. These technologies enable regimes to monitor, predict, and suppress dissent with unprecedented precision and scope, reinforcing state control over society while projecting an image of technological sophistication internationally.

Empirical findings demonstrate that increased investment in digital surveillance infrastructure by Egypt and Saudi Arabia closely correlates with deeper technological and economic partnerships with the United States and China. These relationships reflect a form of "digital diplomacy" where surveillance capacity serves as diplomatic capital, signaling reliability and modernity to powerful external actors. This dynamic illustrates the intertwining of internal authoritarian control with external geopolitical strategy in the digital age.

Nevertheless, this thesis acknowledges the broader complexity of international relationships. While the United States and China are key exporters of surveillance technologies and major economic partners in these contexts, other global and regional partners—including Israel, European countries, Asia-Pacific countries, and private technology firms—also contribute significantly to the evolving surveillance ecosystem in the MENA region. Recognizing this multiplicity enriches our understanding of how digital authoritarianism is embedded within a diverse and competitive international technology landscape.

The paradoxical nature of digital technology—as both a platform for political mobilization and a tool of repression—has been a central theme. Although digital platforms initially offered new opportunities for activism and civic engagement, authoritarian regimes have adapted rapidly, employing sophisticated digital authoritarian toolkits comprising social media monitoring, algorithmic censorship, disinformation campaigns, and invasive spyware. These tools blur the boundaries between domestic governance and international relations, complicating efforts to uphold human rights and democratic freedoms.

Furthermore, the active involvement of major global powers and multinational corporations in facilitating surveillance infrastructure highlights significant ethical and political challenges. The transnational flow of surveillance technologies risks normalizing authoritarian control, fragmenting the global internet, and undermining international efforts to regulate digital rights and corporate accountability.

Addressing these challenges requires a coordinated international response that combines legal regulation, multilateral governance, corporate responsibility, and support for civil society resilience. Transparency in technology transfers, enforceable standards for ethical technology use, and mechanisms for digital rights protection are essential to curb the expansion of digital authoritarianism and preserve open and democratic digital spaces. While this study focused on two pivotal cases, its findings invite further comparative research across the region and beyond, as well as deeper exploration into emerging technologies, resistance strategies, and evolving geopolitical dynamics. Such research is vital to anticipate future developments and support effective policy-making.

In conclusion, digital surveillance in authoritarian regimes is a defining feature of contemporary governance and international relations, shaping power in the digital era with profound implications for human rights, democracy, and global order. This thesis contributes a nuanced understanding of these dynamics and calls for vigilant scholarship, informed policy, and global cooperation to ensure that technological progress supports freedom and justice rather than repression and division.

Bibliography

AidData. (2021). *Global Chinese Development Finance Dataset, Version 3.0*. AidDatasGlobalChineseDevelopmentFinanceDataset_v3.0.xlsx

Amnesty International. (2021). *The Pegasus Project*. Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally - Amnesty International

Amnesty International. (2023). *Predator Files.* Global: 'Predator Files' spyware scandal reveals brazen targeting of civil society, politicians and officials - Amnesty International

Brownlee, J. (2007). *Authoritarianism in an age of democratization*. Cambridge University Press.

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Angiolillo, F., Bernhard, M., Cornell, A., Fish, M. S., Fox, L., Gastaldi, L., Gjerløw, H., Glynn, A., God God, A., Grahn, S., Hicken, A., Kinzelbach, K., Krusell, J., Marquardt, K. L., McMann, K., Mechkova, V., Medzihorsky, J., Natsika, N., Neundorf, A., Paxton, P., Pemstein, D., von Römer, J., Seim, B., Sigman, R., Skaaning, S.-E., Staton, J., Sundström, A., Tannenberg, M., Tzelgov, E., Wang, Y., Wiebrecht, F., Wig, T., Wilson, S., & Ziblatt, D. (2025). *V-Dem [Country-Year/Country-Date] Dataset v15*. Varieties of Democracy (V-Dem) Project. https://doi.org/10.23696/vdemds25

Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.

Feldstein, Steven (2023), *Digital Repression Index 2003-2022*, Mendeley Data, V3, doi: 10.17632/rrnz8p6rvw.3

Freedom House. (2023). Aggregate_Category_and_Subcategory_Scores_FIW_2003-2024.xlsx

Freedom House. (2024). *Freedom of the World*.

Gohdes, A. R. (2024). Repression in the digital age. *Journal of Democracy*, 34(1), 56–70.

Greitens, S. C. (2020). Surveillance, security, and liberal democracy in the post-COVID world. *International Organization*, 74(S1), E169–E190. Surveillance, Security, and Liberal Democracy in the Post-COVID World | International Organization | Cambridge Core

HKTDC Research. (n.d.). *Saudi Arabia country profile – Belt and Road Portal.* https://beltandroad.hktdc.com/en/country-profiles/saudi-arabia

Human Rights Watch. (2023). *Time to ban facial recognition from public spaces and borders.* https://www.hrw.org/news/2023/09/29/time-ban-facial-recognition-public-spaces-and-borders

Jones, M. O. (2022). *Digital authoritarianism in the Middle East*. Princeton University Press.

Liu, H. (2019). *China's surveillance partnerships in the Middle East: A strategic assessment.* Middle East Institute. https://www.mei.edu/publications/chinas-surveillance-partnerships-middle-east-strategic-assessment

Pemstein, D., Marquardt, K. L., Tzelgov, E., Wang, Y., Medzihorsky, J., Krusell, J., Miri, F., & von Römer, J. (2025). The V-Dem Measurement Model: Latent Variable Analysis for Cross-National and Cross-Temporal Expert-Coded Data (10th ed.). V-Dem Working Paper No. 21. University of Gothenburg: Varieties of Democracy Institute.

Rolland, N. (2019). *A concise guide to the Belt and Road Initiative.* National Bureau of Asian Research. https://www.nbr.org/publication/a-guide-to-the-belt-and-road-initiative/

Schlumberger, O. (2023). How authoritarianism transforms: A framework for the study of digital dictatorship. *Journal of Political Power, 16*(2), 1–23.

Snowden, E. (2019). *Permanent record*. Metropolitan Books.

U.S. Department of State. (2023). *U.S. surveillance cooperation reports and funding in Egypt*. U.S. Department of State – Home

Valeriya, M. Pemstein, D. Seim, B. Wilson, S. (2025). *Digital Society Project Dataset v7.*

Feldstein, S. (2019). *The global expansion of AI surveillance.* Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Yayboke, E., & Brannen, S. J. (2020). *The digital authoritarian toolkit: Technology and power in the global South.* Center for Strategic and International Studies.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.