Prismatic Horizons
Journal of Social Science and Humanities
www.phjssh.lexarcheus.com
Vol.-03, Issue-02 (Apr-Jun, 2025)



Digital Authoritarianism: How do Authoritarian Regimes use Digital Surveillance and Social Media Manipulation to Maintain Political Legitimacy?

Naim Ahmad Wani
[1] Student of Political Science, University of Kashmir Hazratbal, Srinagar, Kashmir.

*** Corresponding Author:**
Naim Ahmad Wani
naimahmadwani@gmail.com

ARTICLE INFO

Article History

Received	18 Apr, 2025
Revised	16 May, 2025
Accepted	25 Jun, 2025
Available Online	30 Jun, 2025

ARTICLE ID
PHJSSH0302002

KEYWORDS

Digital Authoritarianism, Political Legitimacy, Surveillance, Social Media Manipulation, Censorship

ABSTRACT

This article explores how contemporary authoritarian regimes deploy digital technologies to reinforce their authority and cultivate political legitimacy. By examining mechanisms of surveillance, censorship, disinformation, and social media manipulation, it demonstrates how these tools are employed to suppress dissent, shape public discourse, and manufacture an appearance of public consent. The study highlights how performance-based legitimacy is bolstered by claims of stability, order, and service delivery, while narrative management enables regimes to delegitimize opposition and frame dissent as external interference. Legal frameworks and state–private sector collaboration further institutionalize digital control, presenting repression as lawful governance. Yet, these strategies are not without risks: exposure of surveillance, declining credibility, citizen resistance, and technological countermeasures threaten the durability of such legitimacy. The article concludes that understanding digital authoritarianism is vital for scholars and policymakers seeking to safeguard democratic practices and digital rights in an era of expanding state technological capacity.

© 2025 The Authors, Published by (PHJSSH). This is an Open Access Article under the Creative Commons Attribution 4.0 International (CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/)

Prismatic Horizons: Journal of Social Science and Humanities
ISSN: 2583-9284
Vol. 03, No. 02, Apr-Jun, 2025
www.phjssh.lexarcheus.com

INTRODUCTION

Within the contemporary worldwide order, the upward thrust of virtual technologies has reshaped governance, communique, and energy structures. whilst democratic structures have in large part embraced those tools for transparency and citizen engagement, authoritarian regimes have strategically employed them to consolidate authority and suppress dissent. The emergence of digital authoritarianism" where states installation surveillance, censorship, and social media manipulation" represents a good sized transformation within the way authoritarian rule is continued. The cutting-edge state of affairs suggests that regimes no longer rely entirely on bodily coercion or traditional propaganda; alternatively, they increasingly more exploit superior records and communique technology (ICTs) to display populations, engineer consent, and manufacture legitimacy. by controlling on-line narratives, manipulating algorithms, and attractive in mass virtual surveillance, authoritarian governments craft an image of order, balance, and national safety, while concurrently silencing competition voices. historically, authoritarian states have relied on censorship and propaganda to maintain legitimacy, however the virtual generation has multiplied those techniques into greater state-of-the-art, real-time, and statistics-pushed mechanisms. the integration of surveillance technology, algorithmic censorship, and disinformation campaigns has made it feasible to create a controlled public sphere in which opportunity viewpoints are systematically marginalized. in opposition to this backdrop, this paper seeks to explore how authoritarian regimes make use of virtual surveillance and social media manipulation as tools of political manipulate. It examines the techniques and mechanisms thru which those technologies give a boost to regime legitimacy, highlights variations across extraordinary political and cultural contexts, and discusses the dangers and limitations inherent in such practices. Authoritarian regimes around the world have increasingly turned to digital tools to reinforce their power. Technologies such as mass surveillance, algorithmic content control, disinformation campaigns, and manipulation of social media platforms have given these regimes new means to project legitimacy, shape public opinion, and suppress dissent. This article investigates how these digital strategies are employed and the mechanisms through which they help maintain political legitimacy.

Definitions and Conceptual Background

Digital Authoritarianism: The deployment of information and communication technologies (ICTs) by authoritarian governments to surveil, censor, repress, or manipulate both domestic and foreign populations.

Political Legitimacy: The perception among citizens that a regime has rightful authority, that its rule is proper, just, or acceptable. Legitimacy is often derived from a mixture of coercion, performance (economic, social), tradition, ideology, or procedural fairness.

Surveillance: Collection and monitoring of data about individuals' behaviour, communications, associations, often covertly. This includes state monitoring of social media, mobile phone metadata, location tracking, facial recognition, etc.

Social Media Manipulation: Active shaping of online content and discourse via pro-government propaganda, bot networks, trolls, censorship, algorithm interferences, disinformation, selective promotion or suppression of content.

Tools and Strategies of Digital Authoritarianism

Below are the principal techniques used by authoritarian regimes, together with examples.

© 2025 The Authors, Published by (PHJSSH). This is an Open Access Article under the Creative Commons Attribution 4.0 International (CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/)

1. Surveillance Technology

Mass Monitoring: Collection of large volumes of personal data, communications, metadata. This helps regimes track dissidents, anticipate protests, intimidate critics. China's social credit systems and facial recognition programs are among the most advanced.

Targeted or Predictive Surveillance: Focusing on individuals suspected of dissent, or tracking groups that are potentially critical. Use of mobile phone location data, social media activity to build profiles.

2. Internet Censorship, Shutdowns, and Access Controls

Blocking or Filtering Content: Blocking websites, filtering keywords, censoring publications or posts that criticise the regime. For example, "Great Firewall" in China.

Selective Shutdowns: Shutting down or severely limiting internet and social media access during protests or political crises to prevent mobilisation. Cases from Zimbabwe, Myanmar, Iran, Cuba etc.

3. Social Media Manipulation and Propaganda

Disinformation / Misinformation: Spreading false or misleading narratives to confuse or mislead the public about regime actions, opposition, or external events.

Bots, Trolls, Fake Accounts, Influencers: Using automated or semi-automated agents to amplify regime messages, drown out criticism, generate fake grassroots support ("astroturfing").

Algorithmic Manipulation: Manipulating recommendation algorithms, burying critical content or boosting pro-regime content to shape what people see. Also, throttling internet speeds for certain platforms or types of content.

State Branding and Narrative Control: Promoting narratives that align with government priorities; delegitimizing opposition; framing dissent as foreign interference, chaos, or moral decay.

4. Legal and Regulatory Frameworks

Repressive Legislation: Laws regulating social media platforms, requiring surveillance backdoors, punishing online speech, enforcing strict licensing or registration of online media. These provide legal cover for digital repression.

Private sector collusion or coercion: Forcing telecommunications companies or social media platforms to comply; requiring data sharing; pressuring tech firms.

How These Practices Support Political Legitimacy

Below are mechanisms through which the above tools help regimes sustain legitimacy:

1. Performance Legitimacy via Control and Order

Regimes can appear strong, decisive, protective. By controlling digital narratives, surveillance helps prevent large-scale protests or dissent and maintain public order, which many citizens value. People may tolerate suppression in exchange for stability, security, or absence of social disorder.

© 2025 The Authors, Published by (PHJSSH). This is an Open Access Article under the Creative Commons Attribution 4.0 International (CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/)

Also, by shutting down dissent online, portraying critics as chaotic or foreign agents, regimes can position themselves as guardians of social unity. This enhances legitimacy among those who prioritize stability over liberal freedoms.

2. Manufacturing Consent

Through repeated exposure to pro-government messaging, propaganda, censorship of alternate views, regimes shape public perceptions. Over time, this can create an "information ecosystem" where dissenting voices are marginalised, leading many citizens to accept or internalize regime narratives. Social learning via social media helps here.

Bots, trolls, and algorithmic nudges can simulate broad support, giving the impression of majority consent. Even if real support is weak, the appearance of consensus can discourage opposition, making the regime seem more legitimate.

3. Deterrence, Fear, and Self-Censorship

Surveillance and reprisals (real or symbolic) create a climate of fear. Knowing one's communications or social media activity might be monitored, many people self-censor. Fear of job loss, arrest, social ostracism leads people to avoid criticizing the regime. This diminishes visible dissent, making regime legitimacy look uncontested.

4. Use of Legal and Institutional Cover

Regimes often attempt to blend coercion with law: they pass laws, regulations, or practices that give a veneer of legality. They may hold elections, have courts, or use other institutions to formalise control. These provide legitimacy in the eyes of some citizens and often in the eyes of foreign observers. Digital regulation may be framed as protecting national security, preventing foreign manipulation, or combating "fake news." This provides a rationale that many citizens may accept.

5. Legitimacy through Performance: Public Goods & Social Services

Besides repression and information control, authoritarian regimes often still provide public goods: infrastructure, social welfare, quick responses to disasters, economic growth. Digital tools help them monitor needs (e.g. via data collection), deliver services (smart cities, mobile governance), which can improve state capacity and legitimacy. Even surveillance, when framed as service (e.g. public health tracking, safety), can be accepted by some segments. Some empirical surveys show citizens support digital governance technologies if they believe they help public service and safety.

Variation & Contextual Factors

Digital authoritarian strategies and their effectiveness vary depending on context. Key moderating factors include:

- Level of digital penetration / internet access: In societies with high internet usage, suppression of social media may provoke more backlash; but also more opportunities for manipulation.
- Strength of civil society and media: If independent journalism and civil society are strong, they may resist or expose regime tactics; but if weak, regime narratives may dominate.

© 2025 The Authors, Published by (PHJSSH). This is an Open Access Article under the Creative Commons Attribution 4.0 International (CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/)

- Institutional checks and legal protections: Where courts, constitutions, or international norms impose constraints, regime suppression is more costly and sometimes less severe.
- Public resources & economic conditions: Legitimacy is harder to sustain purely through repression if economic performance is poor or inequality high.
- Culture, historical legitimacy: Some regimes have traditional legitimacy, ideological bases, or nationalist credentials that help them retain legitimacy even while suppressing dissent.

Risks, Limitations, and Backlashes

While the above strategies can help preserve regime legitimacy, they are not without pitfalls.

Backlash via protest: Overuse of repression or exposure of surveillance abuses may incite protests or resistance. For example, when information about mass surveillance or manipulation leaks, people may lose trust.

Information leakage and external exposure: Whistleblowers, independent media, global connectivity can expose regime's tactics.

Digital resistance / circumvention: Citizens may use VPNs, encrypted messaging, mirror sites, alternative platforms to bypass censorship.

Legitimacy crisis when control fails: If repression or manipulation is insufficient to prevent crises (economic crisis, public health failures, social unrest), legitimacy may erode more rapidly because people observe mismatch between regime narrative and lived reality.

Credibility loss: Deliberate manipulation and propaganda risk being detected; once people believe regime is lying or covering up, credibility falls, possibly undermining legitimacy further.

Technological arms race: As regimes develop more sophisticated tools, so do activists, journalists, and opposition groups; also, international pressure or sanctions may limit some surveillance technology access.

Empirical Evidence / Case Examples

Below are illustrative cases showing these mechanisms in action.

Saudi Arabia & UAE: In these Gulf monarchies, authoritarian control is maintained not only through direct repression, but also via state efforts to shape online civil society — promoting loyal narratives, discrediting critics, crowding them out, discouraging open political debate. Regime branding is used to project stability, progress, and modernisation.

Middle East & North Africa (MENA): After the Arab Spring, many regimes increased investment in digital repression (surveillance, content filtering), propaganda, disinformation, and shutdowns when protests threaten regime stability.

China & Russia: China's model of extensive surveillance, algorithmic censorship, social credit, and Russia's skilled disinformation and foreign influence campaigns serve as influential templates. These regimes also export surveillance tools or collaborate with other authoritarian regimes.

Survey-based evidence: Recent experimental and survey research across different countries shows that informing citizens about potential misuse of digital governance technologies

© 2025 The Authors, Published by (PHJSSH). This is an Open Access Article under the Creative Commons Attribution 4.0 International (CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/)

reduces their support for those tools. But in many contexts people still support digital governance when framed around safety, stability, or national security.

Implications for Legitimacy: Theoretical Analysis

From political theory and legitimacy literature, we can see that authoritarian regimes using digital tools are trying to manage both output legitimacy (performance, order, service delivery) and input legitimacy (consent, recognition from the public), though the latter is often superficial.

Output legitimacy: By maintaining social order, preventing chaos, delivering basic services (or at least the appearance of doing so), regimes strengthen the belief that they are capable and necessary.

Managed input legitimacy: Even where elections or institutions exist, they are often tightly controlled. Digital manipulation helps shape "input"— what voters see, the information environment, who can speak, and what narratives dominate.

Legitimacy as perception: Legitimacy is fragile; it depends on what people believe is real. Controlling what people believe to be true is central. Hence regimes invest heavily in information control. The more they can make their narrative seem unanimous, the more legitimacy they project.

Directions for Future Research & Ethical Considerations

More empirical work across less studied regions (Africa, Latin America, Southeast Asia) to compare how different regimes use digital tools in local context.

Longitudinal research to track how manipulation affects legitimacy over time, including potential erosion of trust.

Ethical dimensions: privacy, autonomy, mental health, freedom of expression; issues of digital inequality.

Analysis of international norms/regulation: how global institutions, technology firms, civil society can act to limit abusive practices.

CONCLUSION

Authoritarian regimes increasingly rely on digital surveillance, internet control, and social media manipulation to cultivate and sustain legitimacy. Through performance (order, security), narrative control, suppression of dissent, and legal institutions, they shape citizens' perceptions in ways that reduce visible opposition and foster an appearance of consensus or necessity. However, these strategies carry risks: loss of trust when people perceive manipulation, exposure of abuses, inability to meet performance expectations, or resistance both online and offline. Understanding these strategies is crucial both for scholars and for policymakers, especially as digital tools become more powerful and pervasive. Strengthening oversight, transparency, digital rights, and alternative information ecosystems can be key in pushing back or providing counterweights to digital authoritarianism.

REFERENCES

Edwin Yingi and Everisto Benyera, *"The Future of Democracy in the Digital Era: Internet Shutdowns, Cyber Laws and Online Surveillance in Zimbabwe,"* 2024.

© 2025 The Authors, Published by (PHJSSH). This is an Open Access Article under the Creative Commons Attribution 4.0 International (CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/)

Claudia Aradau and Emma McCluskey, *"Making Digital Surveillance Unacceptable? Security, Democracy, and the Political Sociology of Disputes."*

Chatham House, *"The Rise of Digital Authoritarianism in MENA."*

Robert Uniacke, *"Authoritarianism in the Information Age: State Branding, Depoliticizing and 'De-civilizing' of Online Civil Society in Saudi Arabia and the United Arab Emirates,"* 2020.

Yilmaz, Akbarzadeh, Abbasov, and Bashirov, *"The Double-Edged Sword: Political Engagement on Social Media and Its Impact on Democracy Support in Authoritarian Regimes,"* 2024.

Karpa and Rochlitz, *"Authoritarian Surveillance and Public Support for Digital Governance Solutions,"* 2024.

"Digital Authoritarianism: A Systematic Literature Review," Journal of Communication/Development.

Eda Keremoğlu and Nils B. Weidmann, *"How Dictators Control the Internet: A Review Essay,"* 2020.

© 2025 The Authors, Published by (PHJSSH). This is an Open Access Article under the Creative Commons Attribution 4.0 International (CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/)