Artofficial Intelligence

Artificial intelligence (AI) has become one of the most powerful tools in the modern state's toolkit for governance, surveillance, and social control. It is among the most transformative developments in human history. Like the printing press, electricity, and the internet, AI is reshaping how societies communicate, govern, wage war, create wealth, and distribute power. Unlike earlier technological revolutions, however, AI has a distinctly political character: it can observe, predict, persuade, manipulate, and make decisions at an unprecedented scale. Governments and political leaders around the world are rapidly integrating AI into statecraft, administration, security, and political messaging. Although AI promises greater efficiency in public services, predictive analytics, and resource allocation, its use by governments often blurs the boundary between legitimate administration and authoritarian oversight. Examples from Asia, the Middle East, North America, Europe, and elsewhere reveal patterns of "digital authoritarianism," in which technology expands state power, often at the expense of privacy, civil liberties, and democratic processes.

Some doomsday scenarios predict the collapse of individual freedom, economic competitiveness, liberalism, and even democracy itself, culminating in the singularity - a hypothetical moment when artificial intelligence surpasses human intelligence and triggers uncontrollable technological growth that irreversibly transforms civilization.

> ***While the AI revolution is undeniably real and already pervasive, governments and politicians are still pursuing an old objective with a new tool: preserving power and control.***

Yet while the AI revolution is undeniably real and already pervasive, governments and politicians are still pursuing an old objective with a new tool: preserving power and control.

TEMURI YAKOBASHVILI
Contributor

Ambassador Temuri Yakobashvili distinguishes himself as an accomplished leader in government, crisis management, and diplomacy. As the founder of TY Strategies LLC, he extends advisory services globally. A pivotal figure in co-founding the Revival Foundation, aiding Ukraine, and leading the New International Leadership Institute, Yakobashvili held key roles, including Georgia's Ambassador to the U.S. and Deputy Prime Minister. With the rank of Ambassador Extraordinary and Plenipotentiary, he is a Yale World Fellow, trained at Oxford and Harvard. As a co-founder and chair of the Governing Board of the Georgian Foundation for Strategic and International Studies, he actively contributes to global media discussions on regional security. His significant contributions have merited the Presidential Medal of Excellence.


© GEOPOLITICS

Out of the Box (and Control) Toolbox

The struggle to gain and retain power is as old as human history, but the tools enabled by AI are unprecedented. For that reason, they deserve closer examination.

Mass Surveillance: AI-powered monitoring systems that combine CCTV footage, facial recognition, and Wi-Fi sniffers can restrict free speech and assembly. These systems allow authorities to monitor large gatherings, track political opponents, and deepen the fear of a constant "watchful eye." As a result, AI surveillance speeds up the identification, deterrence, suppression, and punishment of dissent while reinforcing loyalty and preempting opposition.

Monitoring and manipulating social media: Governments collect vast amounts of social media data for intelligence, law enforcement, immigration control, and "situational awareness." Agencies often rely on third-party vendors for keyword searches, sentiment analysis, geolocation, network mapping, and predictive analytics. These tools scan public posts, hashtags, and social connections at scale. Instead of simply observing, the governments now shape online narratives through influence operations, disinformation campaigns, and information warfare. State-sponsored propaganda and troll farms are common. Russia's Internet Research Agency, China's "50 Cent Army" and United Front operations, Iran, and others use networks of accounts, bots, and state media to amplify messages, sow division, and support regime interests. Typical tactics include fake news, conspiracy theories, coordinated posting, and impersonation.

Disinformation and Information Control: Generative AI makes it easy to produce deepfakes, personalized propaganda, and synthetic media at scale, flooding elections, damaging candidates, and creating confusion. Deepfakes can spread false narratives, erode trust in institutions, deepen divisions, and weaken adversaries.

Internationally, Russia has circulated deepfakes of U.S. officials making false statements about Ukraine policy. Iran has produced waves of AI-generated videos during conflicts, showing fabricated strikes or events. China has integrated AI into broader influence campaigns.

Domestically, political actors also create fake content aimed at voters. Examples include audio deepfakes that mimic politicians and videos designed to smear candidates. In several elections, deepfakes have portrayed leaders rigging votes or making inflammatory statements. State-linked networks use such content to intensify polarization or promote preferred outcomes, weakening informed consent and electoral integrity.

> ***AI-driven repression has become a growing trend in which governments use technology to punish dissent and prevent collective political action before it gains momentum.***

Data Integration: Governments can combine vast datasets, including social media, surveillance feeds, public records, commercial data, and biometrics, with AI to enable sophisticated political manipulation, from predictive profiling and targeted influence to preemptive repression and narrative control. This merges surveillance with actionable insights and automated operations, amplifying both legitimate security uses and the risks of overreach or authoritarian control. AI-driven repression has become a growing trend in which governments use technology to punish dissent and prevent collective political action before it gains momentum. In this model, data integration becomes predictive and preventive: it identifies networks, maps activists, monitors communication patterns, and discourages mobilization through fear of exposure. Such measures leave opponents with little chance of replacing those in power through peaceful means such as free and fair elections.

The effects of these practices are already visible worldwide. They erode trust, chill speech, deepen inequalities, especially through bias against minorities, and consolidate power. Autocracies become more efficient at repression, while democracies risk drifting toward authoritarianism. Without transparency, accountability, and human oversight, algorithms can become unaccountable rulers. Although AI can improve safety and efficiency, the risks of abuse, suppressed dissent, manipulated elections, and stratified societies are clear and rather imminent.

What Can I Buy with AI?

Even a brief look at several major powers shows how strongly AI is enhancing the ability of governments and political elites to exercise control over their populations.

China is the most advanced and widely cited example of AI-enabled population control. The Chinese Communist Party (CCP) has integrated AI into a vast surveillance system that includes facial recognition, predictive analytics, and the Social Credit System (SCS). With more than 200 million surveillance cameras across the country, AI processes real-time data for identification, behavior scoring, and preemptive intervention. Actions such as traffic violations, financial defaults, or online criticism can lower a person's score, leading to restrictions on travel, loans, or employment. Political offenses, including petitioning officials, are heavily penalized. In regions such as Xinjiang, AI is used with particular intensity against Uyghur Muslims, flagging "suspicious" behavior, such as religious practice or certain contacts, for detention in re-education camps. AI analyzes phone data, social media activity, and camera feeds to predict and prevent unrest. It also automates censorship on platforms like WeChat, monitors inmates in prison, and forecasts demonstrations. Combined with the Great Firewall, AI helps create an information environment in which dissent is detected and suppressed algorithmically. This system not only controls the population but also shapes political loyalty by making surveillance constant and punishment predictable.

As the world's largest democracy, India presents a hybrid case in which AI supports both welfare delivery and state control. Aadhaar, the world's largest biometric database, assigns each person a unique 12-digit ID linked to fingerprints, iris scans, and facial data. Although designed to promote inclusion and improve service delivery, it also enables extensive tracking when connected to other databases. Critics warn of "Aadhaar creep," in which biometric authentication spreads into welfare, banking, hotels, and other areas, expanding surveillance risks. Data breaches and private-sector access have further raised concerns about profiling and the exclusion of vulnerable groups.

Police have also deployed AI-powered facial recognition technology (FRT) and Automated Facial Recognition Systems (AFRS). During the 2020 anti-CAA protests, Delhi Police used FRT to identify and track demonstrators, raising constitutional concerns under Articles 19 and 21, which protect freedom of expression and privacy. Predictive policing tools analyze data to identify hotspots, sometimes disproportionately targeting minorities. Internet shutdowns in places such as Kashmir further reinforce digital control by limiting political mobilization.

Singapore's Smart Nation initiative uses AI, Internet of Things sensors, and predictive analytics to manage the city-state more efficiently and responsively. Cameras, lamppost sensors, and integrated data platforms track traffic, crowds, littering, and public behavior, while AI analyzes this information in real time to guide adjustments.

Although often praised for improving safety and convenience, this system also raises concerns about self-censorship in a highly monitored environment. Facial recognition and behavioral monitoring, combined with strict laws on speech and assembly, reinforce social control. Singapore has also exported

this "smart" authoritarian-lite model, pairing strong public trust in government with pervasive surveillance.

Authoritarian regimes across the Middle East are also rapidly adopting AI for preemptive control. In Egypt, AI is used to monitor social media for dissent-related keywords to head off protests following the Arab Spring. Iran uses AI to monitor internet traffic, enforce moral policing, and target activists, including those abroad, through hacking. Saudi Arabia and the UAE are investing heavily in facial recognition, predictive policing, and "Safe City" initiatives, integrating AI into broader security strategies and development agendas such as Vision 2030.

Bahrain and other states deploy spyware and AI-driven monitoring against opposition groups. Gulf countries also export these technologies, sometimes with indirect support from EU-funded programs, intensifying repression in Palestine and elsewhere through checkpoints and migration control. In the future, AI-based conflict forecasting could help regimes predict and suppress unrest before it begins, further entrenching their power.

Russia uses AI for both domestic surveillance and foreign influence. Facial recognition helps track anti-Putin protesters in Moscow, while AI monitors social media for criticism of the war in Ukraine or support for the opposition, often labeling such content "extremist."

Internationally, Russia is a leading user of AI-driven disinformation, employing generative tools for deepfakes, bots, and tailored propaganda to influence elections. These tactics sow division, intensify polarization, and undermine trust in democratic institutions without the use of direct military force.

Internationally, Russia is a leading user of AI-driven disinformation, employing generative tools for deepfakes, bots, and tailored propaganda to influence elections. These tactics sow division, intensify polarization, and undermine trust in democratic institutions without the use of direct military force.

Even liberal democracies show troubling trends. In the United States, AI surveillance has expanded through contractors such as Palantir, which supports ICE by aggregating location and social media data for profiling, including that of protesters. Social media screening in visa decisions and programs like "Catch and Revoke" have also targeted political expression. Predictive policing systems such as PredPol in Los Angeles and the Strategic Subject List in Chicago have faced criticism for bias and disproportionate policing of minority communities, though some have since been discontinued.

AI and the New Architecture of Control in Georgia

The Georgian government's growing use of digital technologies against political dissent has become one of the most troubling indicators of the country's democratic deterioration. While surveillance and political monitoring are not new phenomena in Georgia, recent developments suggest a transition from traditional forms of observation toward more sophisticated systems that increasingly incorporate automated data processing and facial recognition technologies.

Georgian civil society organizations, journalists, and international watchdogs have documented growing concerns over the use of surveillance technologies during anti-government and pro-European demonstrations.

Over the past two years, Georgian civil society organizations, journalists, and international watchdogs have documented growing concerns over the use of surveillance technologies during anti-government and pro-European demonstrations. Human Rights Watch, in its assessments of democratic backsliding and state responses to protests in Georgia, has noted a broader deterioration of civic freedoms and an increase in pressure on protesters and critics of the government.

One of the clearest examples concerns the increasing use of AI-assisted surveillance cameras during mass demonstrations in Tbilisi. Civic watchdog organizations and independent media investigations have reported substantial expansion of surveillance infrastructure around key protest locations and public gathering areas. According to the Georgian Young Lawyers' Association (GYLA), authorities have increasingly relied on facial recognition technologies and surveillance footage in cases against demonstrators, raising serious concerns about legality, privacy protections, and due process.

The concern extends beyond the existence of cameras themselves. Modern surveillance systems no longer merely record events, but also analyze them. Artificial intelligence allows authorities to automate identification processes, connect individuals across multiple data sources, and create behavioral profiles at a scale previously impossible. Such systems can identify patterns, social relationships, and repeated participation in political activities. The result is a shift from reactive policing to predictive and preventive monitoring.

International experience demonstrates where such developments can lead. In Russia, facial recognition systems have reportedly been used to identify opposition activists and anti-war demonstrators after protests ended. Human Rights Watch warned that such technologies create serious risks for freedom of assembly and privacy rights because individuals may avoid participating in protests if they know they can later be identified and punished. Similar concerns increasingly apply to Georgia, which seems to be on the Russian track of governance.

> ***In Russia, facial recognition systems have reportedly been used to identify opposition activists and anti-war demonstrators after protests ended. Human Rights Watch warned that such technologies create serious risks for freedom of assembly and privacy rights because individuals may avoid participating in protests if they know they can later be identified and punished.***

The lawyers representing protesters have argued that the use of facial recognition risks creating an environment where participation in political activity itself becomes associated with personal legal exposure. Individuals may face fines, administrative sanctions, detention, or criminal investigations not because of unlawful conduct but because of their identifiable presence in politically sensitive spaces. The psychological effect of such systems may be as important as their technical capability. Citizens who believe they are permanently watched may begin to self-censor before any formal action is taken against them.

A future and potentially even more troubling risk concerns the expanding relationship between governments and major artificial intelligence providers. Although there is no evidence, except for rumors, that the Georgian government has sought access to private conversations or prompts from platforms such as ChatGPT or Claude, the possibility raises significant concerns for democratic societies. AI companies maintain policies under which they may respond to legally binding requests from law enforcement authorities under certain conditions.

In an increasingly authoritarian political environment, one can imagine a scenario in which

governments attempt to broaden the scope of lawful information requests. Opposition activists, journalists, researchers, and political organizers increasingly use AI systems to organize their work, prepare legal arguments, plan campaigns, brainstorm political strategies, or simply explore controversial ideas privately. If governments were to gain legal access to such conversations through court orders or expanded legal authorities, AI interactions could become a new source of political intelligence.

The broader concern, therefore, extends beyond cameras in the streets or surveillance at protests. The deeper issue involves the emergence of an ecosystem of digital governance in which surveillance systems, biometric technologies, social media monitoring, and artificial intelligence become interconnected. In such a system, repression no longer begins when citizens take political action. It begins earlier - when they search, communicate, organize, or simply think.

Beginning of the End or End of the Beginning?

The apparent success of authoritarian and semi-authoritarian regimes in integrating AI into political life raises a legitimate question about the future of democracy and the liberal order. The answer is neither automatically optimistic nor inevitably dystopian. AI can strengthen liberal democracy by improving governance, expanding access to information, and increasing institutional efficiency. Yet it also magnifies existing vulnerabilities such as disinformation, polarization, and surveillance while creating new risks through automated manipulation and the concentration of power.

> ***The apparent success of authoritarian and semi-authoritarian regimes in integrating AI into political life raises a legitimate question about the future of democracy and the liberal order. The answer is neither automatically optimistic nor inevitably dystopian.***

The future will be shaped less by technology itself than by the institutions, laws, and political cultures that govern its use. AI significantly expands the state's ability to process information, monitor populations, automate decisions, and shape public discourse. Such concentration of informational power can undermine democratic checks and balances and challenge assumptions on which liberal systems were built.

> ***For decades, many believed that economic modernization would naturally lead to political liberalization. AI complicates that assumption.***

For decades, many believed that economic modernization would naturally lead to political liberalization. AI complicates that assumption. Technologically advanced states may now sustain economic growth while simultaneously strengthening authoritarian control. If authoritarian systems become more stable and efficient through AI, democratic governance may no longer appear universally superior.

Democracy also depends on citizens sharing a common understanding of reality. If political actors flood the information environment with convincing fabrications and synthetic content, trust in institutions and facts may erode. Some scholars describe this as "epistemic instability" — a breakdown of shared standards of truth necessary for democratic debate. When citizens increasingly inhabit separate informational worlds, political compromise becomes far more difficult.

Yet democratic societies retain one critical advantage: openness. Innovation thrives where there is academic freedom, free exchange of ideas, and tolerance for criticism and dissent. Authoritarian systems may deploy AI more aggressively in the short term,

but excessive censorship and conformity can eventually weaken the creativity needed for long-term technological leadership.

Ultimately, the survival of democracy in the AI era depends less on technological capability than on political philosophy. Liberal democracy was never designed to maximize efficiency alone; it rests on limiting concentrated power and preserving human autonomy. AI does not weaken the importance of these principles—it makes them even more essential. The future liberal order will undoubtedly evolve, but its survival will depend on whether democratic societies can adapt without abandoning the values that define them.

> ***The challenge for Georgia and others is not whether AI will enter political life (it already has!) but whether democratic institutions can establish sufficient safeguards before technological capabilities outpace political accountability.***

Georgia increasingly illustrates many of these broader dilemmas in practice. The country's recent democratic backsliding demonstrates how technologies intended for legitimate state functions can become politically sensitive in polarized environments with weak institutional safeguards. The expanding use of surveillance infrastructure during protests, concerns surrounding facial recognition systems, pressure on independent media and civil society, and broader attempts to control political narratives all raise questions about how emerging technologies may be used in the future. In a context where judicial independence and institutional trust are increasingly contested, AI-powered tools could further widen the imbalance between state authorities and political opponents. Georgia, like other increasingly authoritarian states, therefore, risks becoming a testing ground for how digital tools can strengthen political control in transitional democracies. The challenge for Georgia and others is not whether AI will enter political life (it already has!) but whether democratic institutions can establish sufficient safeguards before technological capabilities outpace political accountability ■