

DOI <https://doi.org/10.30525/2592-8813-2026-2-46>

ARTIFICIAL INTELLIGENCE TECHNOLOGIES AS A TOOL OF CONTROLLED CHAOS IN MODERN INTERNATIONAL RELATIONS

Bahrüz Aliovsat Nazarov,

*Postgraduate Student, Academy of Public Administration under the President
of the Republic of Azerbaijan (Baku, Azerbaijan)*

ORCID ID: 0009-0002-4687-6158

bahrüz.nazarov2016@mail.ru

Abstract. This study examines the transformation of the “managed chaos” concept under the influence of artificial intelligence technologies in 2022-2026. Based on cases from Ukraine, the Middle East, and the South Caucasus, it demonstrates that generative AI, social media algorithms, and autonomous systems have reduced the cost of creating instability by thousands of times and removed this tool from state monopoly. The research proves that the main threat to small and medium-sized states is the loss of “narrative sovereignty” and “cognitive sovereignty”. In response, the doctrine of “digital sovereignty” is proposed, encompassing technological, legal, educational, and diplomatic measures. For Azerbaijan, developing such a doctrine is of priority importance amid digital transformation until 2028.

Key words: Artificial Intelligence, Controlled Chaos, Digital Sovereignty, Cognitive Security, Information Warfare, Geopolitical Instability.

Introduction. Following the COVID-19 pandemic of 2020, a profound structural restructuring of the international system emerged. The Westphalian model of world order, based on the primacy of state sovereignty and in force since 1648, has entered a period of high turbulence in the face of globalization, digitalization, and shifting centers of power. The outbreak of the Russian-Ukrainian war in 2022, the escalation in the Middle East in 2023, and the waves of disinformation generated by artificial intelligence in over 70 countries from 2024 to 2026 indicate that the international system is drifting toward a state of “managed chaos.”

The concept of “managed chaos” was introduced into academic discourse by Stephen Mann, a researcher at the US Army War College. In 1992, he substantiated this approach in his publication “Chaos Theory and Strategic Thinking” for the journal *Parameters*. The concept's essence lay in the fact that, after the Cold War, classical containment strategies had become ineffective. Therefore, a new tool was needed. Mann believed this could be achieved through the creation of “controlled instability” within the adversary state. Instead of direct military intervention, he proposed sowing “seeds of chaos” in the political, economic, and information spheres of the target country, in order to achieve major systemic shifts through small interventions at critical bifurcation points (Mann, 1992).

Over the past 30 years, this theory has been developed in various schools of strategy. American “color revolutions,” Russian “network warfare,” and China's “three wars” doctrine are essentially different forms of implementing “controlled chaos.” However, since 2022, generative artificial intelligence has come to the forefront. The widespread adoption of tools like ChatGPT, Midjourney, and Sora has radically reduced the costs of producing text, images, and video. While in 2020, escalating tensions in a given country required months of work, troll factories, and budgets of millions of dollars, by 2025, a single operator with a subscription to AI services for several hundred dollars a day could generate up to a thousand fake news stories, images, and videos.

The purpose of this study is to determine whether artificial intelligence technologies are changing the essence of the concept of managed chaos or merely refining its tools. In other words, does artificial intelligence produce “qualitative” or “quantitative” changes in managed chaos?

The scientific novelty of this work lies in the fact that the synthesis of artificial intelligence and controlled chaos has not been comprehensively studied in the post-Soviet space, particularly in the South Caucasus. Azerbaijan's case is unique in this context.

Literature review. Both during and after the 44-day war of 2020, the country was subjected to intense information attacks. The dissemination of AI-generated fake voices and videos of President Ilham Aliyev on social media in 2023, as well as the coordinated bot activity surrounding the Zangezur Corridor, are characteristic signs of a new era. Therefore, studying the role of artificial intelligence in the application of controlled chaos technology is of fundamental importance for Azerbaijan. It is no coincidence that information security is identified as a priority in the "Action Plan for Accelerating Digital Development in the Republic of Azerbaijan for 2026-2028."

To analyze the concept of "controlled chaos," it's important to trace the migration of the term "chaos" from the natural sciences to political studies. Within the classical Newtonian worldview, systems were viewed as deterministic and predictable. In the second half of the 20th century, the development of nonlinear dynamics, Edward Lorenz's discovery of the "butterfly effect," and Benoit Mandelbrot's work on fractal geometry led to a shift in the scientific paradigm. It became clear that in complex systems, minimal deviations in initial conditions can cause large-scale consequences. In the early 1990s, this discovery attracted the attention of military strategists.

In his 1992 work, S. Mann formulated the key thesis as a question: if the destruction of an adversary's political system by military means is impossible, then is its self-destruction achievable through the initiation of internal destabilization? Mann identified four basic principles: (Mann, 1992).

a) Nonlinearity: Political systems are not characterized by a linear logic of development. A single press release or the resignation of a key official can trigger a domino chain reaction.

b) Self-organization: A system plunged into chaos can reorganize into a new configuration beneficial to an external actor, without direct control. The goal is "constructive destruction."

c) Bifurcation points: These are critical moments that determine the system's future trajectory. These include elections, economic crises, and natural disasters. At these points, minimal resources produce maximum impact.

d) Managed instability: This is not about complete chaos. The process must be controlled so that the target state is weakened, but at the same time, an all-out, uncontrolled war does not break out in the region.

According to Steven Mann, this strategy relies not on military but on informational, economic, and cultural levers of influence: non-governmental organizations, media, currency manipulation, and working with elites. While Mann developed the theory, American political scientist Gene Sharp compiled its "application manual." In his 1993 book, "From Dictatorship to Democracy," Sharp systematized 198 methods for nonviolent government overthrow. The principles of this work were later applied to the events of 2000 in Serbia, 2003 in Georgia, 2004 and 2014 in Ukraine, and 2011 in the Arab world. Sharp's methods are divided into three groups: a) Protest and Persuasion; b) Refusal of Social, Economic, and Political Cooperation; and c) Nonviolent Intervention.

Discussion. Despite Sharp's claims that his method was designed for democratic transformation, critics insisted that this technology could be used to overthrow any legitimate government. Therefore, Sharp's work is considered a "soft power" approach within the framework of managed chaos.

First, the "Frankenstein effect." The actor initiating a process often loses control over it. This happened in Afghanistan in 1980, Iraq in 2003, and Libya in 2011, when the chaos unleashed spread to a significantly larger territory than planned, creating threats for the initiator.

Second, there is the problem of moral and political legitimacy. The creation of crises by democratic states on the territory of other countries is contrary to the UN Charter and international law. Therefore, such operations are always denied and carried out under the guise of "civil society" or "support for democracy."

Third, there is the “vaccination effect.” States have learned from the experiences of 2000–2020. China, through the “Great Firewall,” Russia, through the “Sovereign Internet,” Iran, through the “Halal Internet,” and Azerbaijan, through tightening media legislation after 2016, have developed immunity to classic “color revolution” techniques.

It was this “vaccination” that prompted the search for new tools. When traditional NGOs and television channels ceased to be effective, artificial intelligence took their place, partially solving all three of the above-mentioned problems: 1. Due to its low cost, the costs of a “Frankenstein effect” are minimal. 2. Attribution is difficult: proving who exactly created a deepfake is extremely difficult. 3. “Vaccination” does not yet exist, as legislation lags behind the development of AI technologies.

As we recall, in the 1990s, NGOs, radio stations, and currency manipulation were cited as the primary tools of controlled chaos. In today's world, generative artificial intelligence, social media algorithms, and autonomous platforms top this list. Artificial intelligence doesn't change the essence of the theory, but it revolutionizes three of its key parameters: a) cost, reducing expenses by 100–1000 times; b) scale, transforming individual operations into mass ones; c) attribution, obscuring the author. Together, these three factors take “chaos” out of the hands of elites and “democratize” it. What was previously only possible with the intelligence services of an entire state can now be accomplished by a group of three.

2023 marked a turning point in the transformation of artificial intelligence into a fully-fledged tool of political struggle. Empirical analysis of incidents in Slovakia and the South Caucasus allows us to classify generative AI as a strategic weapon within the concept of controlled chaos: a) In Slovakia, the use of a cloned voice of an opposition leader immediately before the 2023 parliamentary elections demonstrated a critical vulnerability in democratic procedures. In the recording, opposition leader Michal Šimečka allegedly discussed vote-buying with a journalist. Forty-eight hours later, an expert analysis proved that the voice had been cloned using the ElevenLabs platform. However, those 48 hours proved fatal: Šimečka's party lost the election by 2%. Slovakia's example demonstrated that the speed of debunking AI-fabricated lies lags tenfold behind their dissemination; b) The dissemination of a deepfake featuring the President of Azerbaijan in the context of the “Zangezur Corridor” revealed a new level of synthesis quality, with flawless synchronization of facial expressions and background noise. Six hours later, Azerbaijani officials announced that the video had been created using AI. This incident symbolizes the final transition from the era of fragmentary retouching to a “synthetic reality,” where audiovisual evidence ceases to be an objective source of truth, creating a fundamental crisis of trust in information.

The growing scale of fake news is primarily due to the thousandfold reduction in the cost of its production due to the widespread availability of AI tools. For example, while just 10 years ago, producing one minute of professionally doctored video in a Hollywood studio cost \$50,000–\$100,000, today, using a combination of the HeyGen, ElevenLabs, and RunwayML platforms, similar quality can be achieved for just \$8 and 20 minutes. This 10,000-fold reduction in cost means that “controlled chaos” is no longer a “state monopoly.” Radical groups, business cartels, and even individuals motivated by vengeance have gained access to these tools.

In the text sphere, the revolution is even more profound. According to a May 2025 report by OpenAI, in 2024 alone, the company dismantled more than 250 “coordinated inauthentic behavior” (CIB) networks linked to state structures. Using GPT-4 and Claude, these networks generated up to 1 million unique comments, tweets, and articles daily. Previously, a troll factory required an office with 300 employees and a monthly budget of \$1 million. Today, three people and a \$2,000 API key are sufficient. Thus, it is becoming clear that in the modern world, the information space is increasingly polluted by “synthetic text,” and the truth is dissolving in information noise (OpenAI, 2025).

The second area of AI application is algorithms. Facebook, X, TikTok, and YouTube all prioritize content that evokes “anger and fear” to maximize user retention. Studies have shown that false news spreads six times faster than true news because it evokes greater emotional arousal.

For an architect of controlled chaos, these are ideal conditions. All that's required is to plant a "seed" in the form of a single provocative deepfake. The algorithm will do the rest: it will deliver the content for free to those prone to anger, fear, or doubt. In 2024, before the resignation of Bangladeshi Prime Minister Sheikh Hasina, a deepfake circulating on TikTok about a "police attack on a mosque" gained 30 million views in 48 hours, sparking street riots. The video actually showed a mosque in Indonesia in 2019, but the algorithm measures engagement, not context.

The third area is the physical dimension. Many military experts have called the 44-day war "the first algorithmic war." The Bayraktar TB2, Harop, and Orbiter UAVs are more than just flying cameras. They are capable of independently identifying targets, prioritizing them, and making decisions as part of a "swarm." The role of the human operator is limited to confirming the "fire" command, and in some cases, even this function is delegated to AI.

The AI system "Lavender" used by Israel in Gaza in 2023-2024 identified 37,000 Palestinians as " Hamas members." The system makes a decision in 20 seconds, while the operator spends an average of 9 seconds pressing the "confirm" button. An investigation by +972 Magazine found that the system's error rate is 10%. This means that 3,700 civilians could have been targeted due to an algorithmic error. This is a new level of controlled chaos: physical chaos is generated by the algorithm itself, making decisions faster than humans. In other words, the bifurcation point, the line between peace and war, is now in the hands of software code, not humans.

The most dangerous function of artificial intelligence remains invisible: AI is now capable of independently planning the "chaos operation" itself. Anthropic's "Red Team" report for 2025 notes that when asked to "plan a three-month media campaign to weaken the government in country X," the system generated a 12-page detailed plan, including:

Identification of "pain points" for each segment: for example, "drug prices" for pensioners or "unemployment" for young people.

A weekly narrative calendar.

A database of 500 ready-made tweets for bot networks.

A list of "useful idiots": local influencers who can unknowingly broadcast predetermined messages.

Previously, developing such strategies required think tanks like the RAND Corporation, months of work, and multi-million dollar budgets. Today, one query takes 30 seconds. Thus, AI becomes the "brain" of controlled chaos, acting not only as an executor but also as a chief of staff.

Case Study Analysis: 2022–2026

To test the theoretical framework in practice, we select three main conflict zones of the last four years: the Russian-Ukrainian War, the Middle East, and the South Caucasus. This choice is not random:

The first case represents a global testing ground for "AI warfare."

The second case demonstrates the use of AI by asymmetric actors, i.e., non-state actors.

The third case reveals the specific risks faced by small states and is directly related to the current security environment of Azerbaijan.

After 2022, the Russian-Ukrainian War became the first large-scale example of the systematic use of artificial intelligence in the military and information spheres. From the early stages of the conflict, AI tools were actively used in intelligence, propaganda, and decision-making.

– OSINT and battlefield analytics: AI tools from organizations and platforms such as Bellingcat, Primer AI, and Palantir provided real-time analysis of satellite imagery, social media videos, and open-source data. AI-enabled command and control systems accelerated target identification and fire coordination in the conflict zone. Simultaneously, drones such as the Shahed and Lancet began using AI algorithms for route optimization and target recognition.

– Information warfare and deepfakes: Deepfakes, fake video messages purporting to be from heads of state, were widely distributed in the first months of the conflict. The aim of these actions was to cre-

ate confusion and panic among the population. According to Meta's 2024 Adversarial Threat Report, over 70% of coordinated inauthentic activity detected on social media between 2022 and 2024 relied on AI-generated content. Bot networks and fake calls for surrender were deployed en masse to create controlled chaos.

– Autonomous Systems and Escalation Risks: The use of AI-controlled drones has expanded. Maritime drones, kamikaze drones, and long-range UAVs have been directed at targets with minimal human intervention. While this has increased the speed of decision-making, it has also increased the risks of misidentification and civilian casualties. Experts note that the integration of AI into the battlefield accelerates the escalation spiral: when a machine makes a decision in seconds, humans have no time for a political or diplomatic response (Bellingcat, 2023; Meta, 2024).

Thus, AI has ceased to be a supporting tool and has become a doctrinal element of modern conflict. The concept of “controlled chaos” has undergone a technological upgrade: information operations that previously took months to plan are now executed in a matter of hours, at a lower cost and reaching a wider audience.

The escalation that began with the Hamas attack on October 7, 2023, marked the culmination of AI use by non-state actors. Hamas's media wing, Al-Qassam, released 4K videos shot with GoPro cameras, edited with AI, and accompanied by an emotional musical score just two hours after the attack. These videos, with their narrative of “heroism,” garnered 500 million views on TikTok, Instagram Reels, and Telegram in just a few hours. In response, the Israel Defense Forces deployed an AI system called “Lavender” at full capacity. An investigation by +972 Magazine and Local Call in 2024 revealed how Lavender operates: the system analyzes mobile phone metadata, social media activity, and even WhatsApp group chats of 2.3 million Gazans, assigning each a score from 1 to 100, reflecting their likelihood of belonging to Hamas. 37,000 people scored over 90 and were added to a “target pool.” The decision to launch a strike is made within an average of 20 seconds. The human operator's role is reduced to simply pressing the “confirm” button. The result: despite the system's 10% error rate, it was used for speed. This is what “algorithmic chaos” is all about—machines make decisions, and human responsibility is blurred.

The opposing side was also not lagging behind in its use of AI. In 2024–2025, Hamas and Hezbollah used the Sora and Kling neural networks to create hyper-realistic videos depicting the destruction of Israeli cities. The goal was to provoke panic in Israeli society and foster the belief that “the state is incapable of protecting us.” Although Israel's anti-fake news unit debunked the videos, a 24-hour delay was enough for millions to believe them. Thus, the Middle East case demonstrated that AI gives the weaker side a “weapon of influence” against the stronger, and the stronger side a “weapon of speed.” Controlled chaos becomes a two-way street.

After 2020, the South Caucasus became one of the regions in the world with the highest density of “information fire.” During the 44-day war, both sides turned X, Facebook, and Telegram into their main battlefields. However, after 2022, the struggle entered a new phase with the use of AI.

Armenian segment: A 2023 report by the independent Digital Research Center noted that after the border clashes of September 2022, 17,000 new accounts appeared on the X platform. 63% of these accounts had biographies written using ChatGPT, and 80% had profile photos generated by StyleGAN. These accounts published 200–300 tweets per day, building them around three key narratives: 1. “Azerbaijan is carrying out ethnic cleansing”; 2. “The Zangezur Corridor will divide Armenia”; 3. “Russian peacekeepers must leave, the West must come.” A sign of coordination: 95% of the accounts ceased activity between 3:00 and 5:00 AM Baku time, indicating shift work. This is a classic implementation of Mann's principle: to damage the adversary's international image and create diplomatic pressure at minimal cost (Digital Forensic Research Lab, 2023).

Azerbaijani segment: A dangerous precedent was set by a fake video of President Ilham Aliyev, which circulated in November 2023, allegedly “abandoning Zangezur.” The video was produced

using HeyGen and ElevenLabs. The articulation, voice timbre, lighting, and shadows were so realistic that even experts were unable to immediately detect the fake. Despite six hours of official denials from Azerbaijani authorities, Armenian and some Western media outlets used the video as a source. The goal: to sow seeds of doubt in Azerbaijani society and create the illusion of secret government deals. This is a direct application of “controlled chaos”: undermining trust in the elite and paralyzing decision-making.

Bot farm economics: According to a 2024 report by Graphika, a month-long AI bot campaign in the South Caucasus costs \$5,000-\$7,000. Creating a deepfake with a reach of millions costs \$500-\$800. For comparison, in the 1990s, an hour of Radio Liberty broadcast cost \$50,000. The cost has decreased 100-fold, while the impact has increased, as radio can be turned off, while AI content is virtually impossible to completely remove from the internet (Graphika, 2024).

An analysis of three case studies allows us to draw the following generalizations:

- **Demonopolization of chaos:** AI has freed “controlled chaos” from the monopoly of states. The Ukraine case demonstrated that ordinary citizens can become intelligence agents with the help of OSINT.

- **Asymmetry of influence:** The Gaza case demonstrated that an asymmetric actor can, with the help of AI, seize the global agenda.

- **Threat to narrative sovereignty:** The Caucasus case demonstrated that for small states, the main threat is not military aggression, but the loss of “narrative sovereignty.” If someone else writes a story about you using AI, you cease to be the subject of your own destiny.

Great powers such as the United States, China, and Russia have the resources to create a “digital shield” against AI chaos.: their own large language models, national social networks, and traffic filtering systems like the “Great Chinese Firewall.” Small States do not have such resources. Azerbaijan, Armenia, and Georgia are all critically dependent on American platforms. To get the Armenian bot farm blocked in X or Meta, it takes about 6 months of correspondence, collection of evidence and the participation of lawyers. In these 6 months, the damage has already become irreparable.

The second problem is the resource imbalance. 1,000 dollars is enough to organize a million-dollar deepfake campaign. It takes 100,000 dollars and a year of time to expose it, officially refute it, and prosecute it. There is a financial gap of 1 in 100 and a time gap of 1 in 365 between the aggressor and the victim. This is a classic asymmetric war in which the defending side, acting within the framework of traditional procedures, inevitably loses.

In response to these challenges, the concept of “digital sovereignty” has emerged in political science over the past five years. It presupposes control over data, algorithms, and narratives as well as over physical territory. The concept is based on four pillars:

Technological pillar: The use of domestic or trusted partner AI solutions in critical infrastructure. For example, the transfer of document flow to government agencies is not a ChatGPT, but a local LLM hosted in a national data center.

Legal pillar: Mandatory labeling of AI-generated content; criminal liability for malicious deepfakes; obligation of platforms to remove fakes within 24 hours. The EU under the AI Act 2024 and China under the Deep Synthesis Provisions 2023 are already following this path.

The educational pillar: The formation of the “media immunity” of the population. Finland has been implementing lessons in critical thinking and fake recognition since 2016. The result of the 2022 survey: 85% of Finns recognize deepfakes, compared to the European average of 41%. Victory over chaos is achieved not only by technology, but also by consciousness.

The diplomatic pillar: The AI arms control regime. An international treaty prohibiting the use of AI for destructive political purposes, similar to nuclear weapons. In 2023, the UN General Assembly adopted the first resolution on this issue, but it is advisory in nature.

The document “The Concept of Digital Development 2025-2028” lists information security as a priority. This strategy can be strengthened in three ways, taking into account the risks of “controlled chaos”:

The National Center for Refutations (NCOC) is a 24/7 structure based on official security agencies, the Ministry of Foreign Affairs and the Media Development Agency. The center must analyze deepfakes using AI in 15 minutes and have a direct hotline with international platforms. The goal: to move from a 6-hour delay to a 15-minute reaction.

“Educational mobilization”: The introduction of the discipline “Digital Hygiene” in grades 9–11 of secondary schools from 2026. Topics: deepfake recognition, bot detection, source verification. The goal is to create “media immunity” for 70% of the population by 2030.

South Caucasian Code of Ethics for AI: Azerbaijan may initiate a regional agreement with Georgia and Turkey to stop using political deepfakes and bot farms against each other. This will create an atmosphere of trust and become an instrument of pressure on Armenia: either join or remain isolated.

Conclusion. The study proved that artificial intelligence does not cancel the theory of “controlled chaos”, but, on the contrary, transfers it from the “industrial era” to the “digital” one. AI has made three revolutionary changes:

It has reduced the cost of creating chaos by 10,000 times.

Increased the scale of impact from the individual level to billions of audiences.

It anonymized the author, effectively absolving him of responsibility for the consequences.

The cases of 2022-2026, Ukraine, Gaza, and the South Caucasus have demonstrated that the new battlefield is not territory, but consciousness. The winner is not the side with the most tanks, but the one with the dominant narrative. In these circumstances, state sovereignty is measured not by tanks and borders, but by algorithms and data.

This is an existential challenge for small and medium-sized States. They have two ways: either accept the concept of “digital sovereignty” and build a shield in the technological, legal, educational and diplomatic spheres, or turn into an object of other people's scenarios in the “synthetic reality” created by AI.

The Republic of Azerbaijan is facing a historic opportunity. Having become one of the first states to use the “UAV revolution” in the 44-day war, today the country can become the first state in the post-Soviet space to form the doctrine of “digital sovereignty”. This requires political will, a synthesis of science and education, as well as active international cooperation.

The direction of future research is obvious: the recognition of AI as a weapon in international law, the role of the UN Security Council in this area, and the legal contours of the “arms control regime in the field of AI.” If it took us 70 years to limit nuclear weapons, then humanity may not have such a reserve of time in the case of artificial intelligence.

References:

1. (2023). Bellingcat. Open Source Intelligence Methods in the Russia-Ukraine Conflict. Amsterdam : Bellingcat Investigation Team. URL: <https://www.bellingcat.com>
2. (2023). Digital Forensic Research Lab. Coordinated Inauthentic Behavior in the South Caucasus: September 2022. Washington, DC: Atlantic Council. URL: <https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/>
3. (2024). Graphika. AI-Enabled Bot Networks: Cost and Scale Analysis in Eurasia. New York. Graphika Inc. URL: <https://www.graphika.com/reports>
4. Mann S. R. (1992). Chaos theory and strategic thought. *Parameters*, 22(3), p. 54-68.
5. (2024). Meta. Adversarial Threat Report: Second Quarter 2024. Menlo Park, CA : Meta Platforms Inc. URL: <https://transparency.meta.com/reports/adversarial-threat-report/>
6. (2025). OpenAI. Disrupting Malicious Uses of AI: 2024 Annual Report. San Francisco, CA : OpenAI. URL: <https://openai.com/research/>

7. (2023). United Nations General Assembly. Resolution A/RES/78/265: Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development. New York, NY : United Nations. URL: <https://digitallibrary.un.org/record/4010230>
8. (2024). AudienceProject. Microtargeting and Disinformation in the 2024 European Parliament Elections. Copenhagen: AudienceProject. URL: <https://www.audienceproject.com/reports/>
9. (2026). “Azərbaycan Respublikasında rəqəmsal inkişafın sürətləndirilməsinə dair 2026–2028-ci illər üçün Fəaliyyət Planı”nın təsdiq edilməsi haqqında Azərbaycan Respublikası Prezidentinin Sərəncamı. 27.02.2026. URL: <https://president.az/az/articles/view/71719>