AVİM
AVRASYA İNCELEMELERİ MERKEZİ
CENTER FOR EURASIAN STUDIES

AVİM Commentary • No: 2026 / 17 •

NATO'S DIGITAL EXPOSURES: ARMENIA'S US-BACKED AI MEGAPROJECT IN THE SOUTH CAUCASUS

Teoman Ertuğrul TULUN

Analyst

Introduction

The Armenia □□□□□□ artificial intelligence megaproject has been promoted as a rapidly expanding high □□□□□□□□□□ initiative, supported by significant external financial and political backing and presented as a future regional AI hub.[1] In public discourse, it is largely framed as a flagship of innovation, investment, and digital modernisation, with an emphasis on its transformative economic potential.

This commentary, however, approaches the project primarily as a matter of security and critical digital infrastructure, rather than as a neutral technology park. It therefore asks a central question: how prudent is it for NATO members to place key AI and cloud capacities in non □□□□□□ geopolitically fragile environments, where unresolved conflicts and shifting alignments already challenge the coherence of regional order and cooperative security?[2]

Regional security and cloud disruptions

Against this backdrop, Armenia, situated in the South Caucasus between Turkiye, Azerbaijan, Georgia, Iran, and within Russias extended security perimeter, is not a member of NATO and remains entangled in post □□□□ disputes and unresolved border and status questions. Its security posture has been marked by a gradual reorientation away from exclusive reliance on Russia, without any corresponding integration into collective defence guarantees comparable to those of the Alliance. [3]

At the same time, recent incidents in which major cloud data centers in the Gulf lost power and connectivity after being struck by objects amid intensified US □□□□□□ □□□□ confrontation have shown that ostensibly neutral digital infrastructure can rapidly become exposed to kinetic risk. Viewed together, these developments underline that large AI and cloud facilities in contested regions must be analysed within a broader law □□□□□□□□□□□□□ framework of regional security, rather than through a purely commercial or technological lens.[4]

Critical infrastructure, cooperative security, strategic dependency

The regional picture outlined above makes it necessary to conceptualise large AI and cloud systems as critical digital infrastructure embedded in existing security architectures, rather than as ordinary technology parks primarily evaluated by investment size or innovation discourse. In alliance and partnership settings, the notion of cooperative security presupposes that states sharing such infrastructure also share basic threat perceptions, treaty obligations, and crisis □□□□□□□□□□ norms; where this common basis is lacking, interdependence may turn into an additional channel of vulnerability.

In the context of NATO, whose collective □□□□□□□ logic rests on the assumption that vital capabilities remain reliably available within or under the protection of the Alliance, relocating key digital assets to non □□□□□□ territories risks introducing gaps between formal guarantees and actual operational resilience. Against this backdrop, the concept of strategic dependency becomes central: when indispensable data processing, storage, and AI capabilities are outsourced to non □□□□□□ territories with unresolved security dilemmas, alliance members risk creating asymmetric exposure to political pressure, kinetic disruption, or denial of access at precisely the moment when these capabilities would be most needed.

Armenias AI hub through an alliance-security lens

Within this conceptual setting, the Armenia □□□□□ AI hub is publicly narrated as a story of innovation, investment, and talent attraction, presenting itself as an engine of digital transformation and regional modernisation. This narrative, however, tends to bracket precisely those elements highlighted in the background and conceptual sections: Armenias unresolved conflicts, its location outside any collective □□□□□□□ system comparable to NATO, and the demonstrated vulnerability of major cloud infrastructures in other conflict-adjacent regions.

Emphasis on regulatory compliance and export □□□□□□□ authorisations projects an image of robustness, yet such legal □□□□□□□□□□ filters do not in themselves address the physical and geopolitical risks of escalation, targeting, or coercive leverage over critical facilities. If NATO members or allied institutions were to host sensitive AI workloads and data in such an environment, the distinction between commercial outsourcing and de facto delegation of core security □□□□□□□ functions would become increasingly blurred. From Türkiyes broader regional security perspective □ which increasingly treats cyber, maritime, and conventional domains as an integrated whole □ such inconsistencies between territorial defence principles and the externalisation of critical digital infrastructures appear particularly problematic, as they risk creating vulnerabilities precisely along the South Caucasus □□□□□ Sea arc where strategic stability is already fragile.[5]

Normative assessment and policy angle

Against the background of Armenias unsettled security environment and the demonstrated vulnerability of major cloud infrastructures in other conflict □□□□□□□□ regions, the relocation of mission □□□□□□□□ AI and data capacities to non □□□□ territories appears both normatively and strategically problematic for the Alliance. From a cooperative security perspective, it is difficult to justify an arrangement in which essential digital capabilities underpinning defence, crisis management, or strategic communication are hosted in locations outside collective defence guarantees and exposed to unresolved regional disputes. [6]

For Türkiye, which increasingly conceptualises cyber, digital, and maritime spaces as interlinked dimensions of a single regional security complex stretching from the Black Sea to the South Caucasus, such externalisation risks importing new vulnerabilities into an already fragile arc of stability. A prudential approach would therefore require NATO members and regional partners to prioritise keeping indispensable digital infrastructure within alliance perimeters, or at least to subject any extra □□□□□□□□ hosting to robust, treaty □□□□ multilateral safeguards that clearly regulate access, protection, and crisis □□□□ decision-making.

Conclusion

Taken together, the regional security environment in the South Caucasus, the demonstrated vulnerability of cloud infrastructures in nearby conflict □□□□□□□□ theatres, and the specific alliance □□□□□□□□ logic of NATO all point to the same conclusion: the geography of AI and cloud systems must not be allowed to outrun the geography of collective defence and legal responsibility. The Armenia □□□□□ AI hub illustrates how high □□□□□□□□□□ projects in contested regions can generate new forms of strategic dependency when they host capabilities that are increasingly central to deterrence, crisis management, and defence planning. For Türkiye and other NATO members, this calls for continuous monitoring of similar initiatives through a law □□□□□□□□□□□□ lens that takes both regional disputes and alliance commitments seriously, rather than through a narrow focus on investment or innovation. Conceptual consistency requires that critical digital infrastructures be understood and regulated as integral components of cooperative security and regional order, not as detached technical ventures that can safely be externalised beyond the reach of established collective-security frameworks.

**Picture: DPIndia*

[1] [1] HPC Wire Editorial, Firebird and US Government Move Armenia AI Megaproject into $4B Phase Two, HPC Wire, 10 February 2026, accessed02 March 2026 , https://www.hpcwire.com/off-the-wire/firebird-and-us-government-move-armenia-ai-megaproject-into-4b-phase-two/

[2] Labarre, F., & Niculescu, G. (eds.), New Security Arrangements for the South Caucasus? Regional Stability in the South Caucasus Study Group (RSSC SG), 26th Workshop report, Austrian National Defence Academy, 2024 ; Teoman Ertuğrul Tulun, Integratıng Natos Cybersecurıty And Marıtıme Strategy: Upholdıng The Montreux Conventıon, AVİM Analysis No: 2024/12 (and PDF version Analysis No: 2024/12, 6 August 2024) https://avim.org.tr/en/Analiz/INTEGRATING-NATO-S-CYBERSECURITY-AND-MARITIME-STRATEGY-UPHOLDING-THE-MONTREUX-CONVENTION

[3] Tutku Dilaver, Security Balance In South Caucasus , AVİM Analysis No: 2023/02 (19 January 2023) https://avim.org.tr/en/Analiz/SECURITY-BALANCE-IN-SOUTH-CAUCASUS ; Emil Avdaliani, NATO and the South Caucasus: Lack of Vision or Strategic Withdrawal?, Caucasus Watch, [day month year of publication], accessed 02 March, 2026, https://caucasuswatch.de/en/insights/nato-and-the-south-caucasus-lack-of-vision-or-strategic-withdrawal.html; North Atlantic Treaty Organization (NATO), Relations with Armenia, last updated 29 May 2024, accessed accessed 02 March, 2026, https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-armenia

[4] India Time Editorial, Iran-Israel War: Amazon Cloud Unit Flags Issues at Bahrain, UAE Data Centers amid Iran Strikes, The Economic Times 02 March 2026, accessed 02 March 2026, https://economictimes.indiatimes.com/tech/technology/iran-israel-war-amazon-cloud-unit-flags-issues-at-bahrain-uae-data-centers-amid-iran-strikes/articleshow/128939726.cms

[5] Dr. Frédéric Labarre and Dr. George Niculescu, eds., New Security Arrangements for the South Caucasus: 26th Workshop of the Study Group Regional Stability in the South Caucasus Policy Recommendations (Vienna: Bundesministerium Landesverteidigung December 2023, 1-4, https://www.bmlv.gv.at/wissen-forschung/publikationen/publikation.php?id=1186

[6] North Atlantic Treaty Organization. The Cyber Defence Pledge. Warsaw Summit, 9 July 2016. Accessed 02 March 2026. https://www.nato.int/cps/en/natohq/official_texts_133177.htm

About the Author :

Teoman Ertuğrul Tulun is an analyst at Ankara-based think-tank Center for Eurasian Studies. Dr. Teoman Ertuğrul Tulun received his Ph.D. in Political Science and Public Administration from İhsan Doğramacı Bilkent University in Ankara. His area of research include European Union Studies,

Globalization, Xenophobia, Hate Speech Studies and International Relations.

To cite this article: TULUN, Teoman Ertuğrul. 2026. "NATO'S DIGITAL EXPOSURES: ARMENIA'S US-BACKED AI MEGAPROJECT IN THE SOUTH CAUCASUS." Center For Eurasian Studies (AVİM), Commentary No.2026 / 17. March 03. Accessed November 10, 2026. https://mail.avim.org.tr/en/Yorum/NATO-S-DIGITAL-EXPOSURES-ARMENIA-S-US-BACKED-AI-MEGAPROJECT-IN-THE-SOUTH-CAUCASUS

Süleyman Nazif Sok. No: 12/B Daire 3-4 06550 Çankaya-ANKARA / TÜRKİYE
Tel: +90 (312) 438 50 23-24 • **Fax**: +90 (312) 438 50 26
@avimorgtr
https://www.facebook.com/avrasyaincelemelerimerkezi
E-Mail: info@avim.org.tr
http://avim.org.tr

© 2009-2025 Center for Eurasian Studies (AVİM) All Rights Reserved