The South Caucasus as a Digital-Transport Hub: The Middle Corridor, Data Flows, and Emerging Security Risks

Yunis Gurbanov*

This article discusses the nature of the Middle Corridor, which is changing from a mere transport corridor via a new strategy that integrates connectivity, digitization, cybersecurity and geoeconomics. Specifically, the article discusses how the South Caucasus, and particularly Azerbaijan, is emerging as not only a transit hub connecting Europe and Asia but also potentially as a digital security node that connects Central Asia, the Caspian Sea basin, Türkiye and European markets. The primary focus of this article will be on the evolving connection between two concepts – transport corridors and data corridors – which it will examine through a discussion of digital infrastructure in the Caspian Sea region, digitalized customs and logistics systems, e-commerce sites and cybersecurity cooperation. The key message here is that the future importance of the Middle Corridor will not depend solely on sea ports, railway tracks and roads; it will increasingly rely on securing digital connectivity and establishing cybersecurity strategies along those transit routes. The article considers the changing dynamics of Eurasia by taking note of alternative routes to existing northern ones; the growing relevance of the Organization of Turkic States (OTS); the European Union's (EU) interest in connectivity and digital connections; Chinese Belt and Road logic; and concerns about hybrid threats in the region. In conclusion, the implementation of a safe digital component of the Middle Corridor could help reinforce the South Caucasus' role as a regional centre of geoeconomic initiatives; however, this can only be achieved by overcoming the current fragmentation of infrastructure projects and shifting to an integrated model of digital governance, cybersecurity and international data collaboration.

Keywords: Middle Corridor, Azerbaijan, South Caucasus, digital connectivity, cybersecurity, data corridors, Central Asia.

* **Dr. Yunis Gurbanov** is a Senior Advisor at the Center of Analysis of International Relations (AIR Center), Baku, Azerbaijan, and a Lecturer at the Academy of Public Administration under the President of the Republic of Azerbaijan. He holds a PhD in Political Science from the University of Cologne and an MPA from Columbia University. His research focuses on geopolitics, energy diplomacy, conflict prevention, and regional security in the South Caucasus, Central Asia, and the broader Eurasian region

Introduction

The Middle Corridor has often been considered in terms of railways, ports, roads, maritime connections, customs and east–west cargo shipments. This is quite logical, as the initial priority of the Middle Corridor is to link China and Central Asia with the South Caucasus, Türkiye and Europe via a trans-Caspian multimodal corridor. With the outbreak of conflict in Ukraine, the imposition of economic sanctions against Russia, disruption of supply chains and rising interest in alternative transport corridors connecting Europe and Asia, the Middle Corridor has gained additional geopolitical importance. For Azerbaijan and the South Caucasus region, this offers a unique opportunity to enhance their status as a connecting region and a geoeconomic initiative hub.

However, such an understanding is no longer adequate. A corridor in the 21st century is not just a physical space where transport takes place; it is also a digital space for transporting data, payment transactions, customs information, cargo monitoring, insurance, cargo clearance, security notifications and business intelligence. A corridor that does not have the necessary digital interoperability may be marked on the map, but it will remain slow, costly, vulnerable and strategically deficient. In contrast, a corridor that merges physical infrastructure with secure digital infrastructure could become a regional integration and strategic autonomy platform.

A corridor in the 21st century is not just a physical space where transport takes place; it is also a digital space for transporting data, payment transactions, customs information, cargo monitoring, insurance, cargo clearance, security notifications and business intelligence.

This article, therefore, proposes considering the potential of the Middle Corridor developing into a physical-digital corridor. The competitiveness of the future Middle Corridor would rest on three interconnected layers. The first is the physical infrastructure layer of railways, ports, roads, ships, logistics facilities and energy facilities. The second layer is the digital infrastructure of fibre-optic cables, data centres, customs and other digital clearing houses, e-commerce platforms, tracking systems, cloud computing systems and digital logistics networks. The third is the security-governance layer of cybersecurity measures, data protection, resilience against hybrid attacks, regional coordination mechanisms and trusted political arrangements.

Azerbaijan plays an important part in this process. Azerbaijan is

an essential state within the physical Middle Corridor because of its position between the Caspian and the Black Sea; participation in the implementation of the Baku–Tbilisi–Kars railway project and the construction of Alat Port; energy network infrastructure; ties with Central Asia; and strategic cooperation with Türkiye. However, the potential significance of Azerbaijan could increase through the development of digital corridors within the region, in addition to transport and energy infrastructure. The implementation of fibre-optic connections across the Caspian, and the creation of digital logistics systems and cyber-defence measures, would enable the country to function not only as a bridge for transportation but also as a digital bridge.

The strategic importance of the Middle Corridor has risen considerably in recent years. The World Bank estimates that freight traffic via the Middle Corridor could grow to about 11 million tons by 2030, with travel time decreasing from today's range of 38–53 days to 14–18 days, depending on the implementation of joint reforms by participating nations. New operational statistics show this to be true. According to the Government of Kazakhstan, the volume of goods shipped using the Trans-Caspian International Transport Route (TITR, widely known as the Middle Corridor) grew by 62% in 2024 to touch 4.5 million tons.[1] In remarks delivered at the Central Asia–Italy Summit in May 2025, Kazakhstan's President Kassym-Jomart Tokayev highlighted that the cargo flow along the Middle Corridor had increased by 62% in 2024 and mentioned a target for capacity expansion to 10 million tons per year by 2027. With this goal, Kazakhstan and its allies are seeking to turn the Middle Corridor into a strategic component of Eurasian connectivity.[2]

The central questions of this study are: **how can the Middle Corridor be transformed from an important transport link into a geoeconomically safe digital corridor? And, what is the place of Azerbaijan and the South Caucasus within this process?**

The article offers three core arguments. First, the strategic importance of the Middle Corridor increasingly depends on the synergy of transport, digital and security infrastructure. Second, the role of Azerbaijan in this

1 World Bank, *The Middle Trade and Transport Corridor: Policies and Investments to Triple Freight Volumes and Halve Travel Time by 2030*, November 27, 2023, Available at: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099111723122527465 (Accessed: June 18, 2026).

2 Daly, J.C.K., "Kazakhstan Increases Railway Capacity Along Trans-Caspian International Transport Route", *The Jamestown Foundation*, June 9, 2025, Available at: https://jamestown.org/kazakhstan-increases-railway-capacity-along-trans-caspian-international-transport-route/ (Accessed: June 18, 2026).

infrastructure cannot be solely considered from the perspective of transit geography. Third, the prospects for the corridor will be determined by its ability to avoid isolated national digital infrastructure and develop reliable means of cooperation in matters of security and institution-building.

The structure of the article is as follows. In the methodology section, the qualitative research and policy analysis approach is described. The theoretical background outlines key terms such as geoeconomic connectivity, digital sovereignty and securitization of infrastructure. The following sections analyse the transformation of the Middle Corridor from a transport initiative into a strategic connectivity infrastructure project; the development of data corridors in the Caspian region; Azerbaijan as a digital-transport node; hybrid threats and cybersecurity concerns; external players; and policy measures to ensure a secure and competitive digital corridor.

Methodology

This article employs qualitative and policy-oriented research methods. It relies on information obtained from official statements, regional policy papers, reports issued by international organizations, expert analyses and the latest media reports on such topics as Middle Corridor initiatives, trans-Caspian transportation projects, digital connectivity solutions, cybersecurity concerns and the geopolitical importance of Azerbaijan for Eurasian connectivity. The research is interdisciplinary, covering areas such as international relations, regional studies, geoeconomics and digital security.

The article takes a fundamentally political approach to digital corridors, rather than treating them solely from a technical perspective. Digital networks, logistics platforms, customs databases, cyber-protection systems and big data flows are treated as elements of sovereignty, regional power and economic resilience. This matters because of the possibility that digitalization of transport corridors will either help to decrease dependence and increase regional autonomy or will create additional vulnerabilities if digital networks are managed by foreign powers, have poor cybersecurity or are vulnerable to cyberattacks.

This study adopts a qualitative case study methodology that involves analysing a variety of academic literature and secondary sources. The choice of Azerbaijan as the major case study was made because of

its geographical position, its strategic importance within the Middle Corridor and its increasing involvement in establishing connectivity through digital means from Central Asia to Europe. The article considers Kazakhstan and other Central Asian states as eastern partners of the corridor, while Georgia and Türkiye are seen as the major western connection points. The EU, China, Russia and the Organization of Turkic States (OTS) are the other regional players.

The article uses a policy-oriented approach to analyse the importance of the digital aspect of the Middle Corridor in terms of its strategic value, influence on the security context of the South Caucasus region and possible policy options to enhance the resilience of the Middle Corridor.

Theoretical Framework: From Physical Connectivity to Digital Geoeconomics

The Middle Corridor can be analysed through three different but interconnected perspectives: geoeconomics, digital sovereignty and the securitization of connectivity.

The first perspective is geoeconomics. Traditional geopolitical thinking views territory, military strength and control over key transportation routes as the primary sources of power. Geoeconomics sees nations using trade routes, infrastructure development, financial tools, energy transport, technical standards and supply chains to realize their geopolitical aims. Corridors cannot be seen as purely economic ventures, as they create dependencies, shape bargaining power, influence market entry and establish political leverage. The Middle Corridor is geoeconomic because it enables Central Asian and South Caucasian nations to develop alternative access to world markets and avoid over-reliance on one specific route.[3]

The second lens is digital sovereignty, the ability of states and regions to govern and defend their digital infrastructure, data flows, platforms and dependencies on technologies. In the case of the Middle Corridor, this implies that port facilities, customs procedures, logistics platforms and cargo-tracking technologies should not be regarded purely as commercial instruments. Instead, they are elements of state infrastructure. Consequently, if the digital infrastructure of a corridor

3 Şenol, C. and Erbilen, S.Ü., "Analysis of the Impact of the Middle Corridor on Türkiye in Terms of Geopolitics and Economy in the OBOR Initiative", *Journal of Geography*, No. 45, 2022, pp. 161-180.

is insecure, external and fragmented, then it becomes strategically vulnerable.[4]

Third, there is the securitization of connectivity. Classical security studies have mainly concentrated on threats to statehood by traditional means.[5] However, in a connected world, infrastructure itself becomes an object of security. Pipeline networks, ports, cables, railway systems, orbital satellites, logistics databases and financial transactions are vulnerable to cyberwarfare, sabotage, misinformation, economic sanctions and coercion. Connectivity generates opportunities, but it also generates vulnerabilities. Consequently, the more critical the Middle Corridor becomes, the more likely it will generate strategic rivalry and hybrid threats.[6]

Three perspectives, therefore, can help us understand that the future of the Middle Corridor cannot be predicted simply by measuring the volume of cargo transported or the duration of journeys. The importance of the Middle Corridor will depend on its ability to become faster, safer and more reliable, interoperable and politically resilient.[7]

The Middle Corridor as a New Strategic Connectivity Architecture

The Middle Corridor route has gained prominence as a result of the restructuring of Eurasian connectivity. For several years, the northern corridors through Russia had been some of the most developed routes connecting Europe and China over land. The Russia–Ukraine conflict and resultant geopolitical fallout have changed this reality. While it remains physically feasible to use the northern routes, the increased geopolitical risks, potential sanctions exposure, reputational concerns and the uncertain future make alternative routes attractive.[8]

---

4 Robles-Carrillo, M., "Sovereignty vs. Digital Sovereignty", *Journal of Digital Technologies and Law*, Vol. 1, No. 3, 2023.

5 Abbood, A.A., AL-Shammri, F.K., Alzamili, Z.M. et al., "Investigating Quantum-Resilient Security Mechanisms for Flying Ad-Hoc Networks (FANETs)", *Journal of Robotics and Control (JRC)*, Vol. 6, No. 1, 2025, pp. 456-469.

6 Liu, Z., "The 'Pan-Securitization' of the EU's Connectivity Policy and China–EU Cooperation", in *The Belt and Road Initiative: Past, Present, Future* (Singapore: Springer Nature Singapore, 2025), pp. 259-278.

7 Vasa, L. and Barkanyi, P., "Geopolitical and Geo-Economic Importance of the Middle Corridor: A Comprehensive Overview", *Eurasian Journal of Economic and Business Studies*, Vol. 67, No. 2, 2023, pp. 20-32.

8 *Ibid*.

One alternative for such trade is the Middle Corridor. This route connects China and Central Asia with the Caspian Sea before continuing on to Azerbaijan, Georgia, Türkiye and Europe. It differs from maritime trade by offering a combined land–sea–land route. It differs from northern trade routes by being less reliant on Russia. It is different from the southern trade routes in that it avoids some geopolitical risks posed by Iran and the Persian Gulf. Landlocked Central Asia is provided with an export route into Europe. Azerbaijan and Georgia benefit from enhanced transit significance. Türkiye gains importance as a Eurasian gateway.[9]

The importance of the Middle Corridor in transport operations is also evident from recent statistics. Kazakhstan's Prime Minister Alikhan Bektanov stated that the volume of cargo shipped using the Trans-Caspian International Transport Route grew 62% in 2024 to stand at 4.5 million tons. This growth is much faster than that experienced by container shipments, which grew 170% to 56,500 TEU. By 2027, the capacity of the Middle Corridor is expected to reach 10 million tons.[10]

While corridor building refers to building railway tracks, ports, roads and terminals, corridor governance involves managing all these components through consistent guidelines, safe information exchange and coordination mechanisms.

Nevertheless, the Middle Corridor faces some structural issues. The route crosses several borders, passes through a number of legal regimes and involves multiple customs clearance processes, ports, railway standards, ship and train scheduling processes and national regulatory regimes. A delay in any one part may impact the entire route and, because all parts of the route are interconnected, a weakness in one country's institutional or digital systems can affect the performance of the entire corridor. Thus, although physical infrastructure is essential, it is not sufficient for a functional corridor. It needs to become predictable in administration and secure in terms of information and data flows.[11]

This is where digitalization is important. In the age of the Internet, a state-of-the-art transport corridor should have electronic documents for cargoes, integrated customs clearance systems, tracking systems

9 Reisinezhad, A. and Reisinezhad, A., "The Corridor War in the Middle East", *Middle East Policy*, Vol. 32, No. 3, 2025, pp. 91-108.

10 Caspia Lab, *Cargo Traffic on the "Middle Corridor" Increased by 62% in 2024*, February 6, 2025, Available at: https://caspia-lab.az/article/cargo-traffic-on-the-middle-corridor-increased-by-62-in-2024-1284 (Accessed: June 18, 2026).

11 Gafarli, T., "Unlocking the Potential in the South Caucasus: The Zangezur Corridor's Impact on the Trans-Caspian International Transport Route (Middle Corridor)", *PERCEPTIONS: Journal of International Affairs*, Vol. 29, No. 2, 2025, pp. 148-173.

International organizations have identified and recognized the increasing relevance of digitalization.

for goods, digital payments, harmonized data standardization protocols, automated risk management systems and data exchanges between ports, railway operators, customs services and private logistics firms.[12]

Thus, the development of the Middle Corridor requires a shift from 'corridor building' to 'corridor governance'. While corridor building refers to building railway tracks, ports, roads and terminals, corridor governance involves managing all these components through consistent guidelines, safe information exchange and coordination mechanisms. This is crucial because many regions can build corridors, but few can successfully govern connectivity.[13]

Data Flows as the New Layer of the Middle Corridor

International organizations have identified and recognized the increasing relevance of digitalization. As indicated in the World Bank's analysis of the Middle Corridor project, digitalization, along with improvements in customs practices and interoperability, is crucial to realizing expected growth and decrease transit time. The World Bank estimates that transit time can be decreased from 38–53 days to 14–18 days. Therefore, the above results indicate that digitalization, together with other technological advances such as automated customs processing, logistics platforms and border information systems, will be decisive in determining the future success of the corridor.[14]

This leads to the development of a novel idea known as the 'digital corridor'. This is not an alternative to the transport corridor but, rather, a facilitator of it. It is the invisible architecture that makes the visible one function effectively. In the case of the Middle Corridor, the digital corridor has four dimensions.

---

12 Mammadov, M., Alizada, S., Mammadov, N. et al., "Artificial Intelligence in Transit Corridor Management: Economic Efficiency Prospects of the Zangezur Corridor", *Luminis Applied Science and Engineering*, Vol. 3, No. 1, 2026, pp. 45-52.

13 Rasli, F.N., Juhari, M.L. and Halim, A.H.A., "Green Corridors in Coordinating and Supporting SDG 11: Sustainable Cities and Communities", *International Journal of Research and Innovation in Social Science*, Vol. VIII, 2025, pp. 1053-1071.

14 World Bank, *Middle Trade and Transport Corridor: Policies and Investments to Triple Freight Volumes and Halve Travel Time by 2030*, November 2023, Available at: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099111723122527465 (Accessed: June 18, 2026).

The first component is related to telecommunications infrastructure. Fibre-optic connections across the Caspian Sea have the potential to connect Azerbaijan with Kazakhstan and even Turkmenistan, thereby establishing a direct digital link between the South Caucasus and Central Asia. This is crucial from a strategic point of view, as it may help reduce reliance on alternative routes that can be both longer and riskier.[15]

Azerbaijan's President Ilham Aliyev has repeatedly emphasized his country's ambition to become a major transport, logistics and connectivity hub linking Europe and Asia.

Second, logistics digitalization is required. Ports, railway stations, customs administrations and logistics firms should adopt interoperable technologies. The ideal would be to achieve a state in which data flow much faster than the actual physical products. Indeed, completing the digital process of clearance prior to the arrival of goods at customs points or ports of entry will save substantial transit time.[16]

Third, there is digitalization of commerce. E-commerce, digital trade services, online payment systems and regional business platforms stand to gain from a more coordinated corridor system. The Middle Corridor is not just a passage for physical cargo but also a digital platform connecting Europe, Türkiye, the South Caucasus and Central Asia.[17]

Fourth is cybersecurity. As the Middle Corridor becomes digitized, it requires protection. Hacking of ports, rail networks, customs databases and telecommunications systems can seriously undermine any gains made by the corridor. Without cybersecurity, the digital corridor will become a strategic liability rather than a strategic asset.

Azerbaijan's Role: From Transit State to Digital-Transport Hub

Azerbaijan enjoys the advantages of favourable geography in its efforts

15 Nuriyev, E., "Exploring Future Energy Security in the Black Sea-Caspian Region: Strategic Interests, Political Risks, and Emerging Challenges", in *The Routledge Handbook of Political Risk* (London: Routledge, 2025), pp. 254-276.

16 Zeng, F., Chen, A., Xu, S. et al., "Digitalization in the Maritime Logistics Industry: A Systematic Literature Review of Enablers and Barriers", *Journal of Marine Science and Engineering*, Vol. 13, No. 4, 2025, Article 797.

17 Núñez, Y.G., González, G.R., Ávila, L.R. et al., "Effective Commercial Management: Essential Elements for Its Development in the Current Context", in *Advances in Technical Sciences and Architecture: Selected Contributions of CCIA 2024* (Cham: Springer Nature Switzerland, 2026), pp. 927-934.

to participate in the Middle Corridor, although the geography of a country is not, by itself, sufficient to ensure it a strategic advantage. Strategic advantage is achieved when the geographical advantages of a state are paired with infrastructure, institutions, technologies and international collaborations. Azerbaijan's President Ilham Aliyev has repeatedly emphasized his country's ambition to become a major transport, logistics and connectivity hub linking Europe and Asia.[18]

Azerbaijan has made significant investments in the development of infrastructure for energy and transport in recent decades. Specifically, as stated on the website of Baku International Sea Trade Port, the current capacity of the Port of Baku (Alat Port) is 15 million tons per year and 100,000 TEU in containers. With the planned expansion of the port facilities, this will be increased to 25 million tons and 500,000 TEU. In addition, the Baku–Tbilisi–Kars railway line and the energy facilities of Azerbaijan, along with growing collaboration with Central Asia and Türkiye, add to the country's significance within the Middle Corridor.[19]

Azerbaijan's indispensability for the Middle Corridor is apparent from the following angles

First, Azerbaijan is the Caspian entry point for the South Caucasus. With its Alat Port, railways and connections with Georgia and Türkiye, Azerbaijan becomes a window into Europe as well as an important part of the trans-Caspian bridge. Central Asian states find, in Azerbaijan, an entry point to Türkiye and Europe; Europe sees it as an opportunity to get closer to Central Asia.[20]

Second, Azerbaijan is a connector between transport and energy corridors. The knowledge it has gained from the development and management of large cross-border infrastructure projects, such as the Baku–Tbilisi–Ceyhan (BTC) oil pipeline, South Caucasus Pipeline (SCP) and Southern Gas Corridor (SGC), has helped Azerbaijan become well-versed in handling such infrastructure projects. This knowledge could also be used

18 President.az, *Speech by Ilham Aliyev at the SCO Plus format meeting in Tianjin*, China, September 1, 2025, Available at: https://president.az/en/articles/view/70040 (Accessed: June 18, 2026).

19 Transit.gov.az, *Maritime Transport and Ports*, Available at: https://transit.gov.az/en/transportation-systems/maritime-transport-and-ports (Accessed: June 18, 2026).

20 Gafarli, T., "Unlocking the Potential in the South Caucasus: The Zangezur Corridor's Impact on the Trans-Caspian International Transport Route (Middle Corridor)", *PERCEPTIONS: Journal of International Affairs*, Vol. 29, No. 2, 2025, pp. 148-173.

for transport and digital corridors. The reasoning behind this assumption is that such infrastructure needs to be safe, politically acceptable, economically feasible and internationally recognized.[21]

Third, Azerbaijan is becoming a critical node in terms of digital connectivity between Central Asia, the South Caucasus, Türkiye and Europe. Digital aspects of the Middle Corridor have become more than just a theory. Azerbaijan and Kazakhstan are currently working on the implementation of the Trans-Caspian Fiber Optic Cable project under the Digital Silk Way project. According to information from Azerbaijan's AzerTelecom, the project entails the creation of a 380-km submarine fibre-optic cable, which will connect the cities of Sumgayit (Azerbaijan) and Aktau (Kazakhstan). The planned transmission capacity is up to 400 Tbps. The project is scheduled for completion at the end of 2026 and can be considered one of the most significant digital projects in the Caspian area.[22]

According to NEQSOL Holding, the larger framework of the Digital Silk Way involves investments amounting to more than $250 million with the aim of developing a safe and reliable east–west digital corridor between Europe and Asia. As a result, Azerbaijan is not only seen as a transit country for cargo and natural resources, but may become a transit country for data flows. The project will help in developing telecommunications, cloud computing, digital trade and data-processing services.

As noted by the CEO of AzerTelecom, Emil Masimov, the objective of the Trans-Caspian Fiber-Optic Cable Project is to establish a new east–west information bridge and to make an important contribution to the development of a safer and more diverse system of data exchange between Europe and Asia. In this respect, one can observe how the position of Azerbaijan, in terms of the Middle Corridor, goes beyond transport and energy projects to include the field of digital connectivity and information infrastructure. By opening up new economic prospects for the country, this project also helps to build up digital sovereignty and minimize excessive reliance on the old northern route.[23]

21 Khanayev, A. and Al, A., "Azerbaijan's Renewable Energy Policies and Green Energy Corridors", *Marmara Türkiyat Araştırmaları Dergisi*, Vol. 12, No. 2, 2025, pp. 800-818.

22 AzerTelecom, *Significant Milestone of the Trans-Caspian Cable Line Project*, March 4, 2025, Available at: https://www.azertelecom.az/en/news/significant-milestone (Accessed: June 18, 2026).

23 Digital Silk Way, *Euronews Aired a Special Program on the Trans-Caspian Fiber-Optic Cable Line*, December 18, 2025, Available at: https://www.digitalsilkway.az/news/59/euronews-aired-a-special-program-on-the-trans-caspian-fiber-optic-cable-line (Accessed: June 18, 2026).

As the corridor develops, it will be important for Azerbaijan to maintain a diversified economic model and avoid excessive reliance on transit-related revenues. However, there are much larger benefits to consider than simply earning revenues through charging fees for moving cargo across its land. Some of the additional services that can be offered in relation to the use of the corridor include logistics, data processing, insurance, trade financing and cybersecurity services, among others.

Cybersecurity and Hybrid Risks along the Middle Corridor

The digitalization of the Middle Corridor will introduce a range of vulnerabilities, which should not be considered only from the point of view of technological security but rather within the context of the security environment of the whole region.

The first type of vulnerability refers to the disruption of critical infrastructure. Digitalized systems are ever more frequently employed by ports, railways, customs and telecommunications services, and the energy sector. Disruption of such systems by means of a cyberattack could lead to cargo traffic disruption, economic costs and reputational loss for the route.[24]

The second risk is data manipulation. Data accuracy plays a key role in logistics processes. If the data on cargoes, customs declarations, shipments or tracking are manipulated, then delays, fraud, sanctions violations and security events may occur. Therefore, data integrity is equally important as data availability.[25]

The third risk is related to espionage and the collection of commercial intelligence. Corridors provide a great deal of information on trade volumes, strategic materials, military items, capacity of infrastructure assets and economic partnerships. Third parties may try to gain access to the information and use it, politically and commercially.[26]

---

24 Okika, N., Nwatuzie, G.A., Odozor, L. et al., "Addressing IoT-Driven Cybersecurity Risks in Critical Infrastructure to Safeguard Public Utilities and Prevent Large-Scale Service Disruptions", *International Journal of Innovative Science and Research Technology*, Vol. 10, No. 2, 2025.

25 Mammadov, M., Alizada, S., Mammadov, N. et al., "Artificial Intelligence in Transit Corridor Management: Economic Efficiency Prospects of the Zangezur Corridor", *Luminis Applied Science and Engineering*, Vol. 3, No. 1, 2026, pp. 45-52.

26 Clark, R.M., "The Changing Nature of Intelligence Collection", in *The Oxford Handbook of National Security Intelligence* (Oxford: Oxford University Press, 2025), pp. 258-270.

The fourth potential risk involves dependency on foreign providers of digital services. Without proper safeguards, the corridor could become highly dependent on third-party suppliers of digital platforms, telecommunications, cloud services or cybersecurity infrastructure. Foreign technologies should not be excluded as general policy, but procurement processes and risk assessments should nevertheless be properly conducted.[27]

The OTS is increasingly important for the Middle Corridor, as several key countries along the route share a Turkic identity or participate in Turkic cooperation structures.

The fifth risk relates to disinformation and reputational challenges. With the increasing importance of the corridor, narratives about its reliability, security, cost efficiency and political legitimacy will also become important. Other transit corridors or competing nations can try to challenge the corridor's image through various information warfare techniques. Therefore, cybersecurity is strongly linked to strategic communications.[28]

As shown above, cybersecurity must be incorporated into the overall plan for the development of the Middle Corridor from day one. It cannot simply be added to the existing strategy to address a technical issue. The corridor will need proper cybersecurity standards, joint response to incidents involving several countries, regular cyber-exercises, data sharing practices and more.[29]

The Organization of Turkic States and Digital Connectivity

The OTS is increasingly important for the Middle Corridor, as several key countries along the route share a Turkic identity or participate in Turkic cooperation structures. Azerbaijan, Kazakhstan, Türkiye, Uzbekistan, Kyrgyzstan and other states have a shared stake in ensuring Caspian transit capacity and reducing reliance on conventional transit routes.[30] A series of projects and initiatives concerning digitalization, smart logistics and technology cooperation were initiated during the 11th Summit of the OTS in Bishkek, Kyrgyzstan, on November 6, 2024. First, the Bishkek Declaration, adopted by the Heads of State of the OTS

27 Mammadov et al., *op.cit*., pp. 45-52.

28 Kieffer, E.L. and Carr, K.M., "Disinformation Attacks and Nonprofit Communication Strategies", *Journal of Nonprofit Innovation*, Vol. 5, No. 2, 2025, Article 7.

29 Chatterjee, S., "Multilateral Connectivity Projects and Geopolitical Implications Through Transport Corridors in the Middle East", *Saudi Journal of Humanities and Social Sciences*, Vol. 10, No. 12, 2025, pp. 565-577.

30 *Ibid*.

at the summit, emphasized the need for the development and connection of national digital transport and logistics systems to ensure better connectivity between the countries of the OTS. Also, the introduction of the Trans-Caspian Customs Transit Portal, the e-permit scheme and the increased application of the e-TIR procedure were considered crucial for enhancing the competitiveness of the Middle Corridor. Moreover, cooperation in emerging technologies was acknowledged as another sphere of cooperation between OTS countries.[31]

There are several ways in which the OTS could help advance the digital Middle Corridor initiative. These include facilitating political coordination within member states; promoting customs harmonization and logistics standardization; fostering cooperation on cybersecurity and capacity-building; developing platforms for dialogue between telecommunications providers, logistics companies, ports and digital networks; as well as positioning the idea of digital connectivity as a component of broader Turkic regionalism, but not an ideological one.[32]

Such an approach is crucial. The most productive form of Turkic cooperation is practical, rather than rhetorical. Customs digitalization, cyber-resilience measures, fibre-optic communications, digital marketplaces and unified technical standards will mean more for promoting regional solidarity than would any political declarations. In this way, digital connectivity can lay the groundwork for new forms of regionalism.[33]

From this perspective, Azerbaijan has emerged as one of the key drivers of the Middle Corridor. It has consistently promoted the project as a shared venture that benefits Central Asia, the South Caucasus, Türkiye and Europe alike.

External Actors: The EU, China, Russia, Türkiye and the United States

The digital Middle Corridor will emerge in the context of competition among international actors. Several international players have an interest in the region; however, there are significant differences in their approaches to the topic.

31 Organization of Turkic States, *Bishkek Declaration of the Eleventh Summit of the Organization of Turkic States*, November 6, 2024, Available at: https://turkicstates.org/u/d/temel_belgeler/bishkek-declaration.pdf (Accessed: June 18, 2026).

32 Diriöz, A.O., "The Organization of Turkic States, Contributing to Regional Peace and Cooperation", in *Adaptivity of Science in Reconciliation Conflict Transformation and Peace Studies* (Cham: Springer Nature Switzerland, 2026), pp. 279-292.

33 Abdullaev, A., "The Turkic States Organization's Development Agenda in Logistics", *International Affairs: Politics, Economics, Law*, Vol. 112, No. 2, 2025, pp. 147-156.

The EU considers the Middle Corridor through the prism of diversifying transport connectivity with Central Asia to ensure that there is no heavy reliance on politically unstable transport routes. The EU's interests go beyond transport and include access to vital resources and energy, digital connectivity, regulatory harmonization and supply chain security. These points are reflected in the EU's Global Gateway strategy, which aims at improving sustainable connectivity and infrastructure connections between Europe and other parts of the world. For the South Caucasus region, the approach described above represents a chance to attract investment and increase integration with Europe. Indeed, as part of its Global Gateway strategy, the European Commission plans to enhance cooperation with Azerbaijan in spheres such as transport, energy and digital connectivity. The decision-making procedure within the EU can, however, take a long time because of the bureaucratic nature of the organization. Hence, it is crucial to merge common values with infrastructure and digital investments when dealing with the European community.[34]

For China, connectivity is one element of a larger strategy of expanding infrastructure, economic and trade linkages in Eurasia. It is noteworthy that, contrary to other countries' perception, Beijing does not see the Middle Corridor as a competitive project, but rather as a supplementary project that will add to regional connectivity and help increase trade between Asia and Europe. As China becomes increasingly involved in regional initiatives concerning infrastructure and connectivity, this also creates opportunities for investment and technology sharing. In order to capitalize on these chances, regional states must cooperate with China in a pragmatic way while retaining their strategic independence.[35]

The expansion of other corridors by Russia, including the International North–South Transport Corridor (INSTC) and the Northern Corridor, raises some concerns. However, even if the Middle Corridor is not specifically designed to oppose Russia, it undermines the monopoly of the northward route. As other countries, such as Central Asian and South Caucasus nations, begin diversifying their transportation ways, Russia loses its capacity to exploit geographic advantages for its geopolitical

34 Shahbazov, F., "Azerbaijan's Pragmatism: Navigating Foreign Policy in a Fragmented World", in *Emerging Partners of Central Asia: Engagement of Small and Middle Powers* (Cham: Springer Nature Switzerland, 2026), pp. 165-183.

35 Reisinezhad, A. and Reisinezhad, A., "The Corridor War in the Middle East", *Middle East Policy*, Vol. 32, No. 3, 2025, pp. 91-108.

ends. The development of the Middle Corridor can raise political issues when the region is associated with Western strategic plans.[36]

Türkiye is among the key promoters of the Middle Corridor. The route is of great significance in terms of developing the country's status as an intermediary between Asia and Europe, as well as in expanding cooperation with neighbouring countries. Indeed, the significance of this country lies in the fact that it allows the Middle Corridor to stretch towards Europe.[37]

Resilient supply chains, diversified energy sources, and decreased reliance on Russia and China are strategic interests for the United States. Nevertheless, Washington's involvement has generally not been as infrastructure-driven as that of the EU or China. To sustain its influence in the region, Washington may need to complement political dialogue with greater involvement in cyber-defence, cybersecurity capacity-building and investment initiatives.[38]

For Azerbaijan and the South Caucasus region, the key issue is to take advantage of all these actors while remaining independent of any one in particular. That is the core concept of multi-vector digital geoeconomics: attracting investment, diversifying partners, retaining sovereignty and developing regional ownership.

Digital Sovereignty and the South Caucasus Security Architecture

For a considerable time, the South Caucasus was characterized by conflict, Great Power competition and energy corridors. The emergence of digital corridors has provided another aspect to this characterization. Should the South Caucasus become an important link between Europe and Asia in terms of data connectivity, digital sovereignty will be included in the region's security paradigm.[39] Digital sovereignty does not imply seclusion from international technology players. Rather, it

36 *Ibid*.

37 Schindler, S., Altun, S. and Bayırbağ, M.K., "'There Cannot Be a Corridor Without Türkiye!': Türkiye's Polyalignment Strategy in Pursuit of Strategic Autonomy", *Third World Quarterly*, 2026, pp. 1-19.

38 Arisoy, A. and Gokasar, I., "The Logistics Conjuncture of the Middle Corridor Trade Route and Turkey's Strategic Role", *Journal of Intelligent Decision Making and Granular Computing*, Vol. 1, No. 1, 2025, pp. 143-150.

39 Akıllı, E., "Presence—Sovereign Identity in the Digital Sphere", in *Cognitive Diplomacy and Digital Autonomy: Statecraft in the Age of Artificial Intelligence* (Cham: Springer Nature Switzerland, 2025), pp. 113-135.

implies the capability to take independent decisions in relation to digital infrastructure development, cybersecurity, vendor diversification, data protection and standard setting. For smaller nations, this might prove challenging but inevitable. Vulnerabilities may arise when countries depend solely on an external technology supplier. Insufficient local capacity could limit a country's technological resilience, and inconsistent regulation could undermine integration efforts.[40]

Should the South Caucasus become an important link between Europe and Asia in terms of data connectivity, digital sovereignty will be included in the region's security paradigm.

For Azerbaijan, digital sovereignty must be tied to the corridor strategy. It should consider a few basic questions: who controls digital infrastructure? Where is data stored? What standards safeguard logistics platforms? How is cyber-event management organized? How do private operators participate in the national security framework? Can Azerbaijan engage with Kazakhstan, Georgia, Türkiye and EU countries to strengthen cybersecurity cooperation along the Middle Corridor?

The same questions are valid for the region. If the Middle Corridor is to be digitally secure, states must operate according to common standards. If a container moves from Kazakhstan to Europe via Azerbaijan and Georgia, it must not encounter various digital systems. A cyberattack in one area should automatically activate mechanisms for joint action. It must be feasible to exchange data without disclosing national security data. This necessitates institutional design.[41]

In other words, the South Caucasus could serve as a test bed for safe connectivity. When Azerbaijan, Georgia and their partners establish a reliable digital logistics platform, the strategic importance of the region will increase. Otherwise, the Middle Corridor will look appealing only in theory.

Policy Recommendations

A number of measures could reinforce the digital and cybersecurity aspects of the Middle Corridor.

40 Repetto, E., "Concept 'Stretching' or Concept Innovation? A Review of the Usages of Sovereignty in the Digital Sovereignty Literature", *Policy & Internet*, Vol. 17, No. 3, 2025, Article e70011.

41 Santaniello, M., "Attributes of Digital Sovereignty: A Conceptual Framework", *Geopolitics*, Vol. 31, No. 2, 2026, pp. 788-809.

First, Azerbaijan and other stakeholders should advocate for the idea of a 'Digital Middle Corridor'. This approach will encourage policymakers to think beyond physical transit and move towards connectivity. It should encompass transport digitalization, fibre-optic infrastructure, cybersecurity measures, data governance, digital trade and logistics.

Second, governments of participating countries should establish a cybersecurity policy for the whole corridor. Such an initiative may include minimum cybersecurity standards for ports, rail networks, customs authorities and logistics providers, along with joint cyber-drills, alert systems and collaboration among national CERTs.

Third, digital customs and cargo procedures should be coordinated. In the longer term, efforts should be directed at creating a solution in which cargo information is transferred digitally prior to the arrival of the shipment itself.

Fourth, Azerbaijan could develop digital services related to the corridor. For example, such services might encompass logistics analysis, cargo tracking, digital insurance, trade finance, cybersecurity and data centre capacity. In this way, the country would be able to derive additional value from the corridor.

Fifth, the OTS should be used as a tangible platform for digital connectivity. Instead of making abstract declarations on the political level, countries should focus on technical cooperation in cybersecurity, e-commerce, digital customs clearance, data standards and trusted telecoms infrastructure.

Sixth, the EU and other external actors should not limit their support to the development of hard infrastructure. In addition, external partners should provide assistance for improving digital infrastructure and cybersecurity capacity. Construction of new roads and railroads will have little effect without digital security.

Seventh, regional countries should adopt a multi-vendor approach to the procurement of ICT services. They should avoid reliance on a single external technological environment and should analyse any project from the perspective of national security and resilience.

Lastly, efforts should be made to enhance strategic communications. Instead of framing the Middle Corridor merely as an emergency replacement for Russian transit routes, it is necessary to present it as an alternative that is sustainable and reliable.

Conclusion

The Middle Corridor is entering a new phase of development. The first phase of development involved geography, with the determination of a corridor connecting Central Asia, the Caspian Sea, the South Caucasus, Türkiye and Europe. The second phase was about infrastructure, with improvements to ports, railways, road transportation and logistics capabilities. The third phase of development requires the creation of a digital and secure corridor.

This article proposes an understanding of the Middle Corridor as a physical-digital corridor in which the flow of cargo and the flow of data depend on each other. The future success of the route will be determined not only by the development of infrastructure but also by digital interoperability, cybersecurity, data protection, institutional coordination and strategic trust among the countries participating in the route.

The key country within such a digital-physical corridor is Azerbaijan. Geography, energy know-how, location relative to the Caspian, relations with Central Asia, partnerships with Türkiye and ambitions in digitalization make Azerbaijan a potential digital-transport hub. However, the realization of such an ambition will take more than just being an intermediary state; it requires the delivery of high-value services and the development of the necessary digital platforms.

The South Caucasus is thus not simply located between regions, but is itself becoming a region in which different modes of connectivity intersect. The transport corridor intersects with energy, digital infrastructure, cybersecurity and geopolitical rivalry. This brings opportunities as well as risks. If leveraged properly, the Digital Middle Corridor can be used to increase regional sovereignty, diversify Eurasian connectivity and increase the South Caucasus's importance as a node of geoeconomic initiatives. If left unaddressed, regulatory fragmentation and cybersecurity vulnerabilities could undermine the efficiency and long-term viability of the corridor while increasing the region's exposure to external dependencies.

The most prudent claim, therefore, is not that artificial intelligence, cyberspace and digital infrastructure will replace geopolitics, but that they are increasingly becoming integral parts of geopolitics itself. Hence, in the interconnected world of today, it is not enough for a country to control land routes and seaports; it must also control data, platform governance, digital infrastructure and cross-border cooperation.