BAKU DIALOGUES

POLICY PERSPECTIVES ON THE SILK ROAD REGION

Vol. 7 | No. 4 | Summer 2024

Exclusive *Baku Dialogues* Interview

The Significance of COP29 and the Role of Azerbaijan
Baroness Patricia Scotland KC

Perspectives on Climate Finance and Technological Sovereignty Preparing for COP29

Azerbaijan's Green Finance Capacity
Shamil Muzaffarli & Sheyda Karimova

Sovereign Cloud Platforms
Miloš Jovanović & Stefan Jančić

Living with Russian Grand Strategy

Moscow's Evolution Towards a G-Zero/Silk Road Paradigm
Nikolas K. Gvosdev

Armenia's Challenges

Pashinyan Under Pressure: Less Inconsistent, But Still Unpredictable
Onnik James Krikorian

A Transforming Silk Road Region Two Views

Hedging Foreign Policies
Murad Nasibov

Regional Order-Making Mechanisms
Nargiz Azizova

bakudialogues.ada.edu.az

UNIVERSITET • UNIVERSITY ADA

INSTITUTE for DEVELOPMENT and DIPLOMACY

ISSN Print: 2709-1848
ISSN Online: 2709-1856

Empowering Nations through COP29

Sovereign Cloud Platforms and Technological Sovereignty for Critical Industries

Miloš Jovanović and Stefan Jančić

One of COP29's thematic days, as chosen by Azerbaijan's Presidency, is titled "Science, Technology and Innovation / Digitalization." Like all other parts of the Conference's thematic program, this one is designed to advance the Presidency's overarching vision, which consists of two mutually-reinforcing, parallel pillars—"enhance ambition" and "enable action"—at the heart of which stands climate finance. To quote from the COP29 President-Designate's 17 July 2024 Letter to Parties and Constituencies:

> The COP29 Presidency's top negotiating priority is to agree [on] a fair and ambitious NCQG [New Collective Quantified Goal], taking into account the needs and priorities of developing country Parties. […] But this is not just our priority. The COP29 Presidency has heard the voices of so many Parties and communities that are counting on all of us to take this step at COP29. We must all go the extra mile together to deliver this historic milestone. […] Both adaptation and mitigation financing require a substantial increase. […] Our work on climate finance should represent progression beyond previous efforts, delivering multiples, adequate to the scale and urgency of the problem. Transparency and accessibility will also be key facilitating conditions that will require effort from multiple stakeholders.

Milos Jovanović *is President of OpenLink Holding in the UK and CEO of OpenLink Group in Serbia. He is also Professor of Information Security at both the Faculty of Information Technology at Belgrade Metropolitan University and the Faculty of Mechanical and Civil Engineering in Kraljevo at the University of Kragujevac, having been the youngest PhD recipient in the field of advanced security systems in the history of Serbia.* ***Stefan Jančić*** *is a Researcher at the Ministry of Defense of Serbia in the field of electronics and information technologies. He is a master's student at the School of Electrical Engineering of the University of Belgrade and holds a BSc degree in Electrical Engineering and Computer Sciences (EECS) from the Military Academy of the University of Defense of Serbia. The views expressed in this essay are their own.*

We intend this essay to serve as a contribution to the ongoing conversation on this theme, but also to the broader global debate about the utility of sovereign cloud platforms and technological sovereignty for critical industries. Enhanced cooperation at the inter-state level to save the planet is one thing; ensuring it does not infringe on the prerogatives of national sovereignty, including security considerations, is quite another.

This essay can contribute to COP29's thematic day on Science, Technology and Innovation / Digitalization, but also to the broader global debate about the utility of sovereign cloud platforms and technological sovereignty for critical industries.

Our objective is to describe the role of sovereign cloud platforms in different core sectors and to stress the necessity of having strong technology infrastructure, data management, and AI regulation. We believe that each nation has a responsibility to work out for itself a proper balance between these and related concerns, which requires having a proper unbiased grasp of the issues involved. Azerbaijan is no different. We thus conclude this essay with a brief consideration of how our findings can be applied to the technological independence and economic development of the Alat Free Economic Zone (AFEZ).

Technological sovereignty is a term that has emerged in today's world, characterized by a high rate of development of information technologies, as a vital factor for countries that want to keep their data and key industries under their own control and preserve their own security. The concept of sovereign cloud platforms should be seen as a game-changing opportunity for such countries to upgrade their data processing capacities, improve cooperation between ministries and other state entities,

and optimize governmental and private sector activity.

Through the establishment and management of a nation's digital architecture, it is possible to protect its information, establish an environment for innovation, and spur sustainable economic growth. Sovereign cloud platforms not only contribute to improving business processes and their security, but can also create a lot of additional economic value. When data is centralized in a secure cloud system, along with the help of AI and IoT, nations can both use resources and manage data costs efficiently, as well as enhance their decisionmaking processes.

This economic benefit spans different areas such as healthcare, energy, and manufacturing, where data optimization and the improvement of security leads to improved services, reduced costs, and, therefore, greater competitiveness.

New Cloud Platforms Needed

Worldwide experience with the application of cloud platforms demonstrates their high potential for engendering changes in data processing and inter-ministerial cooperation, especially in such sensitive spheres as medicine and energy. Hence, through sovereign cloud platforms, nations can address bureaucratic inefficiencies, as important information will henceforth be stored in a central place, easily retrievable by other end-users in the administrative apparatus.

Take healthcare. Having all of a patient's records safely stored in a single, cloud-based system means that these can be accessed by any healthcare provider. This, in turn, can reduce errors in treatment processes. We know, for instance, that patients rarely provide doctors with a fully accurate history, which can have a negative impact on treatment, including drug prescriptions. Not only does single-system storage enhance the accuracy and efficiency of medical measures, but it also helps to shape the entire healthcare system. Centralized, cloud-based recordkeeping in the medical field ensures convenient access to all patient information and reduces the chances of errors in treatments.

In the energy sector, a centralized cloud platform can contain every single aspect of the consumption cycle. More and more accurate data results in better analysis, which in turn can optimize distribution (particularly in the context of electricity sector liberalization and the introduction of two-way communication and power transmission through the building of smart grids and micro-grids), detect all sorts of grid and distribution inefficiencies (e.g., leakages), modernize billing procedures (e.g., dynamic pricing in real-time), and enhance overall efficiency. It can also ensure problems are detected swiftly, including corruption and payment clearance issues. Lastly, a centralized cloud-based energy platform can enable the detection of network attacks and other forms of security breaches, thus making energy infrastructure safer and more secure.

Cloud platforms can also be extremely useful in other contexts. Using cloud-based management platforms, for instance, can be beneficial in industrial parks in various ways. Thus, any organization can easily utilize the flexible technologies that are part of the cloud computing universe.

In the same manner, a cloud-based smart gateway platform may also be able to ensure that all smart home devices are aware of each other and collect data to alter the device's connectivity and functionality.

To improve the sovereign cloud platform, cloud platforms should be connected to other modern technologies such as artificial intelligence (AI) and the Internet of Things (IoT). Thus, cloud data centers should be smarter and more efficient with the help of AI solutions and should be a part of the green cloud data center concept, characterized by optimized energy intake and effectiveness. Also, the integration of IoT cloud systems can be useful in identifying performance parameters as well as in the monitoring and controlling of attached devices in real time for enhancing productivity in various sectors.

Moreover, cloud platforms can be helpful for energy management since the consumption of energy is very important. For example, in active distribution grids, cloud platforms for service restoration can involve an optimization algorithm to improve the response time in emergencies and thereby reduce the grid's reliability. Similarly, the cloud platforms to supervise the battery conditions in the energy storage systems can also enhance the efficiency and reliability of large-scale energy storage systems and solutions in energy management.

In addition, cloud platforms enable fast assessments and confirmations of energy efficiency, as has

been shown in studies on the energy consumption of washing machines and other similar appliances. If these platforms are developed based on cloud computing techniques, combined with measurement and verification methodologies, it is valuable to assess the energy-saving performance and to make decisions in energy management.

Overall, sovereign cloud platforms may benefit countries by enhancing the operations of governments, industries, and end-users because of the advantages of giant data analytics, communication, and the elimination of bureaucratic inefficiencies.

Regarding the purpose of cloud platforms, it is possible to mention the following: combining the centralization of information, developing advanced technologies, and optimizing the usage of energy in different fields ultimately increases the transparency and effectiveness of industries and sectors for the sustainable development of states.

All such platforms, employed in a strategic context, can also enhance a country's capacity to manage and leverage resources to strengthen the governmental apparatus for closer cooperation.

Technological Sovereignty and Critical Industries

Organizations want to maintain control over cloud platforms that are deployed in sensitive sectors like health, power, and other ministries. Control over platforms ensures that data is secure and shielded from various intrusions—especially so where the data is sensitive (e.g., patient or energy records).

Thus, countries possessing cloud infrastructure can design secure protection systems that correspond to the needed level of protection and legal requirements to prevent hacking or stealing of vital information. Such and similar threats indicate that full sovereignty must be achieved over the technology domain. Only in such a case can a state ensure that no outside influence can penetrate into the sanctity of a country's critical systems.

Full sovereignty must be achieved over the technology domain. Only in such a case can a state ensure that no outside influence can penetrate into the sanctity of a country's critical systems.

Technological sovereignty also enables nations to modify cloud platforms to suit the requirements of their main economic sectors. For example, in the healthcare industry, tailored solutions powered by 5G networks, AI, and cloud computing can be customized to meet the unique health requirements of a given country's population, thereby raising the standard of care provided and the condition of the patient.

Customization is also essential for developing tools tailored to the energy ministries to improve energy management in individual countries and also assess energy usage, billing procedures, and so on.

Furthermore, maintaining control over cloud platforms can spur national technological innovation and development. Thus, by guiding cloud infrastructure, states can support research and development projects, enhance talent development, and foster the implementation of innovative technologies such as AI, IoT, and big data analytics in the fields related to a country's strategic interests. This not only helps to build up a competitive edge for domestic industries, but it also fosters economic development and national capability in the context of disruptive technologies.

Promoting technological development at the domestic level is thus critical to minimizing technological importation and fostering the eventual development of sustainable national technologies and non-off-the-self technological solutions.

Moreover, sovereign cloud platforms allow countries to design their rules, regulations, and governance systems in ways that are fully compatible with their interests and cultures. This way, states can keep control over cloud infrastructure and impose data localization policies, ensure compliance regarding industry-specific requirements, and minimize the risks of unauthorized data transfers across borders.

It is crucial to establish indigenous technological capabilities to minimize reliance on foreign technologies, which is always dangerous for a country's security and technological independence.

Such a level of control is crucial for maintaining a country's digital sovereignty, safeguarding its critical infrastructure, and ensuring the confidentiality of sensitive data. It is crucial to establish

indigenous technological capabilities to minimize reliance on foreign technologies, which is always dangerous for a country's security and technological independence. This point of view is in line with the general aim of retaining sovereignty over cloud platforms to keep vital national information and processes within a country's jurisdiction.

With technological sovereignty, countries would be in a position to have maximum benefits from cloud computing while at the same time reducing risks and increasing the full potential that a country has to go through this digital transformation in key sectors. This represents an integrated approach to controlling technological infrastructure and underscores the importance of sovereignty in safeguarding national interests whilst driving both climate action and sustainable development in an increasingly connected digital world.

Efficiency in Manufacturing

Cloud platforms of a centralized nature enhance the efficiency of bureaucracies and do away with critical errors in manufacturing. They make workflow and decisionmaking processes smooth and efficient by consolidating data and streamlining communications.

In manufacturing industries, the cloud platform plays the role of automating production lines, inventories, and supply chains. The integration of cloud solutions with IoT devices and data analytics tools enables one to get a deeper understanding of the operation, proper utilization of resources, and enhanced productivity.

Cloud-based industrial automation systems are used in the management of industrial processes from remote areas, and thus the efficiency of the processes is improved, with minimal interruptions. These systems allow changes to be made conveniently on production lines and prevent the formation of complications in the process.

In the interest of ensuring that centralized cloud platforms enhance bureaucratic efficiency, adequate measures must be taken to secure the data. Measures include the use of blockchain, encryption of data, and control of access—all these provide data and ensure its privacy in cloud-based systems.

Moreover, the implementation of edge and fog computing also helps in reducing delay and enhancing the processing of data, especially in applications that require real-time decisionmaking. Therefore, these advanced security and computing mechanisms, when implemented together, can assure the nations regarding the security and efficiency of cloud structures.

Technological Ecosystems and Internet Sovereignty

If a country wants to be independent on the internet and control the data generated within its borders, then it needs to ensure that technologies, governments, and innovations support each other. Therefore, through policy and regulation, cooperation and partnership, technology and invention, a state could put in place a solid foundation for data protection, sovereignty, and control of its digital assets.

If a country wants to be independent on the internet and control the data generated within its borders, then it needs to ensure that technologies, governments, and innovations support each other.

Among the necessary conditions for a country to establish technological conditions that would enable it to establish internet sovereignty, a proper legislative framework—one that guarantees adequate protection of data and its conformity to international standards—is foremost. Data protection, cybersecurity, and possession and ownership of data constitute the context of the invention of sovereignty and self-rule of digital property. Such frameworks have to be robust enough to address the constantly growing threat landscape and cyber events that seek to penetrate digital systems.

The formation of public-private and academic partnerships must become the foundation for the establishment of long-lasting technological solutions in governmental organizations. By establishing and encouraging a culture of innovation, knowledge transfer, and interdisciplinary cooperation, a state can get the best skills and financial support to improve its domestic technological process and maintain its digital sovereignty.

Thus, there is a requirement for continuous support of present and future research initiatives relating to the IoT, AI, and cloud computing technologies to improve technological systems. This implies

that support from stakeholders including innovation hubs, incubators, and parks can go a long way in shaping the right environment for inventions that support the industries and economy of the regions.

This also contributes to the development of new technologies and establishes the basis for a country's technological independence and therefore minimizes the risks and threats associated with the use of foreign technologies.

Internet sovereignty and data control technological ecosystems can be described as an environment that is made up of the following four components: regulation, collaboration, technology, and talent.

It becomes crucial to develop indigenization of technological capabilities because this represents real independence on the technological side. Therefore, it becomes easier to focus more on the domestic processes and avoid dependencies and domination by foreign actors in the sphere of digitalization.

This involves supporting domestic IT firms, investing in domestic research and development, and creating the right conditions for technology development. Indigenous innovation refers to the attempt to make technological improvements and to persuade people to change from learning and imitation into actual creation: Indigenous, sovereign technological advancement should fit into the country's goals and principles.

Thus, enhancing awareness and skills application among the working population is essential for the continuation and effectiveness of technological settings. Education and training to increase people's knowledge of digital technology increase the potential that a skilled workforce can bring into reality such ideas and cope with change. This refers not only to the formal academic qualifications of staff, but also to the retraining of knowledge and skills, as the rate of technological development is rather high.

Good governance to support internet sovereignty and data control is very important in the functioning of a state's internet governance mechanisms. When there is policy coordination with all relevant stakeholders (e.g., government, industry, academia, and civil society), policy diversification and optimization results. These

structures have to be future-proof and yet keep the core elements of data protection (from both outside and inside threats) and data protection sovereignty.

Internet sovereignty and data control technological ecosystems can be described as an environment that is made up of the following four components: regulation, collaboration, technology, and talent. Thus, it is possible to provide the development of stable technological environments that are built on sovereignty and independence in the context of the digital world, protect data, encourage innovations, and give people the possibility to manage the technologies. Such an approach, properly executed, can enable a country to get the best out of the digital age without undermining its national interests and, at the same time enhance its international position.

As will be discussed in greater detail below, the experience of the Alat Free Economic Zone AFEZ) can be a useful example to illustrate how geographical advantages, optimal legislative arrangements, and the use of proper tech solutions can be used to stimulate economic growth and the development of high technologies whilst enhancing Azerbaijan's technological sovereignty.

Data Control and Security

In modern cloud platform development, governments need to establish rules, laws, and regulations with technical support in data control and security enhancement. Among these is the introduction of appropriately tight data protection laws that force cloud service providers to guarantee data security through the use of cryptography, limit access to data, and conduct regular data checks to ensure that data meets the laid down security standards.

Such laws and policies also assist governments in ensuring that people adhere to data management and storage systems laws so that it becomes mandatory to protect the data from hackers and other nefarious factors.

It is critical to have many laws that guard data owing to the frailty of cloud platforms. All these laws should ensure that serious encryption solutions, like the Advanced Encryption Standard (AES), are used—especially when data is both stored and when it is in motion.

In layman's terms, encryption can be illustrated as follows: even if someone tries to take this data, they

will not understand it since a code is used to encrypt the data. Hence, through the adoption of encryption technologies in storage systems in the cloud, the state can protect its data from hackers and any other persons who may wish to gain access to it.

The relevant laws should also include regular and spot security audits and vulnerability assessments, which can be performed according to what are called Content Security Policies (CSPs). To enhance the security of identity management in cloud environments, governments can influence user identification and authorization to adhere to enhanced authentication mechanisms like the Multi-Factor Authentication (MFA) solution. MFA requires passwords, biometrics, or tokens and thus enhances the security of the cloud environments and reduces the chances of important data being accessed without authorization.

To reduce the risks of what is called "digital leakage" in cloud computing platforms, governments can use Data Loss Prevention (DLP) solutions that consist of monitoring, detection, and prevention. DLP tools function by analyzing all the data traffic and isolating risks and breaches that contain sensitive data, thus preventing data leakage.

Through the implementation of such solutions, governments will be in an optimal position to observe the activities of data both in and outside the cloud to prevent the leakage of sensitive data. Thus, the goal of enhancing the quality of protection should be pursued by enhancing the activity of cloud service providers—that is, by ensuring that they increase their level of responsibility and transparency.

Technological sovereignty, particularly in the context of AI, cannot be maintained without reference to societal values.

In addition to ensuring that security checks and scans occur more often and that cloud platforms meet certain standards set by the relevant security regulator or overseer, other preventive measures can be developed by policymakers to enhance the security of cloud environments from various security threats. This incorporates the formulation of national cybersecurity policies that determine the responsibilities of the different players in protecting cyber assets.

All told, a state can prevent data leaks and cyber-crimes emanating from new cloud platforms by applying regulatory, technological, and preventive standards. Thus, by improving measures such as data protection, encryption, secure authentication, and transparency, a state may strengthen its control and security over a cloud environment and protect valuable information and negating threats in the cybersecurity sphere. Such an all-inclusive, strategic approach should ensure that a country's national digital framework is well-safeguarded and sustainable enough to undertake the important responsibilities of today's government and business operations.

AI Governance in Cloud Platforms

A state will also need to establish an effective governance structure for the use of AI-based solutions in cloud platforms, particularly for critical industries. AI governance frameworks are beneficial for government agencies as they reduce risks, increase transparency, and encourage accountability in the use of AI in sensitive domains.

There are several ways for AI governance to be applied in cloud platforms. One is to define the rules for the ethical usage of AI following whatever principles and requirements are set by the state. There is no good reason why any country should simply, blindly, enable an AI company—usually based outside its jurisdiction—to operate freely within its borders: the stakes are simply too high and potentially too dangerous. Thus, issues of bias, interpretation, and data privacy also need to be addressed. Technological sovereignty, particularly in the context of AI, cannot be maintained without reference to societal values.

A state should thus develop AI governance by empowering its regulatory authorities to oversee AI and the way it functions. This will help build confidence in the use of AI systems and prevent potential negative effects associated with implementing AI integration. It will also ensure that other technologies that could be used in conjunction with AI governance in cloud platforms are fully interoperable.

There are several approaches to defining AI in ways that increase interpretability,and thus make the decision process easier to understand and less mysterious. Preventive models, for example, can be used to establish and counter the biases that are built-in to a given AI system by its creators cannot

affect its decisionmaking processes. Such technical tools are useful in making an AI system more accurate and credible, particularly for applications associated with vital assets or services: the ramifications of an improper or prejudiced AI determination can be costly.

Positive AI governing guidelines contribute to ensuring that a given AI system is secure, effective, and morally and ethically compatible with a state's interests. Such guidelines, properly written and enforced, increase the likelihood that AI will be adopted by a state's user community. AI governance is also a great help when it comes to the proper usage of AI in cloud platforms, especially for sensitive industries.

To be clear: technological sovereignty in the case of AI means that a state should be able to control the processes of AI technologies' development and use according to its priorities—not those of the AI creator. By implementing the best available AI governance practices, a state can ensure that this revolutionary technology—which is here to stay—substantially benefits the major sectors of the economy without sacrificing its development and stability. Proper AI governance can thus contribute to a state's technological sovereignty.

Hardware and Software Sovereignty

The final element we explore in this essay on securing a state's technological sovereignty involves regulating the backbone of its technological infrastructure, namely the hardware (HW) and software (SW) that is used in its various systems, including the cloud. This is especially relevant for states that are, or aspire to be, leaders in critical industries. We are talking about microchips, here.

The need to secure and maintain technological independence and drive innovation is now spurring a growing number of states to seek ways to ensure the local manufacturing of microchips. It is also advantageous that some major industrial areas such as healthcare, energy, and defense receive the particular technological requirements that they need while at the same time protecting themselves from oscillations and disturbances driven by outside and foreign action.

Measures a state can take to address such and similar concerns and thereby improve control over microchips include developing domestic capacity in semiconductors, engaging key stakeholders in the industry, and developing policies on secure and reliable supply chains. Investment in domestic research and development (R&D) can result in the design and manufacturing of microchips that are unique to a state's specific needs and, in addition, go a long way towards eliminating the various types of disparities impeding technological development.

All in all, a state's continuing dependence on foreign-made and foreign-supplied critical technologies, including microchips, is incompatible with the pursuit of a strategy of total technological sovereignty. The emphasis here is on "total." It is not necessarily geopolitically and geoeconomically realistic for most states to pursue such a strategy, but the more control they can gain over the various technologies discussed in this essay, including on the microchip issue, the closer they will come to assuring a reasonable level of technological sovereignty. The point, however, is that a state should work to ensure that it does not allow foreign interests to impose their own preferences and standards of what constitutes this "reasonable level."

A state's continuing dependence on foreign-made and foreign-supplied critical technologies, including microchips, is incompatible with the pursuit of a strategy of total technological sovereignty.

AFEZ as the Key to the Silk Road Region's Technological Sovereignty

In some ways, Azerbaijan is uniquely well-placed to attempt technological sovereignty—what skeptics would claim is effectually a "moonshot" endeavor. This applies particularly to the Alat Free Economic Zone (AFEZ).

AFEZ provides the gold standard in investment incentives, including exemptions on all relevant taxes and customs duties. In addition, it also has at least three strategic advantages. *One*, its legal basis, which could be described as "more than autonomy, less than independence"—effectually, a state within a state (we are overstating here, but conceptually, this makes sense); *two*, its ready-to-use industrial land plots pre-equipped with direct connections to infrastructure and utilities, including plentiful and cheap power sources; and *three*, its strategic geographical location. AFEZ is located at the literal intersection of the Silk Road region's two most

important strategic road and rail corridors (i.e., the Middle Corridor and the International North-South Transport Corridor) and right next to first-in-its-class Baku International Sea Trade Port, the region's Òkeystone five-star transport hub,Ó as its director put it in the Fall 2020 edition of *Baku Dialogues*. AFEZ is even building its own cargo airport.

Businesses engaged in high value-added and export-oriented manufacturing and internationally traded services that use innovative technologies and approaches, including the latest environmental standards, are welcome to set up shop on the territory of AFEZ. It is, therefore, perfectly suited to serve as the location for the establishment of not only Azerbaijan's but the entire Silk Road region's center for achieving digital technological sovereignty.

Azerbaijan's independent foreign policy posture and ideal geographic location, coupled with its membership in the Organization of Turkic States, interest in joining BRICS, and growing engagement with the Shanghai Cooperation Organization, illustrate AFEZ's underlying geopolitical and geoeconomic advantages. To put it directly, AFEZ can and should become the home of big data centers providing cloud-based platforms and solutions, host AI systems, provide space for the production of HW and SW, including microchips and other vital components, and so on.

For the countries that make up the core of the Silk Road region—which in all cases that matter, also belong to the Turkic world—making AFEZ the strategic center of a drive to acquire and maintain technological sovereignty should become an imperative. Without such a concerted venture, the quest to successfully transform this part of the globe into a "worldwide power center"—as Azerbaijani President Ilham Aliyev put it at the Shusha Global Media Forum on 20 July 2024—would be much harder to accomplish. BD

bakudialogues.ada.edu.az