E u r o E c o n o m i c a

Issue 1(44)/2025 *ISSN: 1582-8859*

Information Systems and Technological Security Strategy for Reducing Economic Dependency

Florentina-Loredana Dragomir[1]

Abstract: This article analyses the importance of technological security and the role of information systems in reducing economic dependence, in the current global context marked by cyber and economic risks. The research adopts a qualitative and strategic analytical approach, combining a review of current literature with case-based analysis and policy evaluation. The methodological design includes the identification of vulnerabilities in technological infrastructure through comparative case studies, and the assessment of national and international strategies to enhance technological autonomy. Additionally, the article incorporates the analysis of government programs and public-private initiatives, highlighting their impact on reducing external technological dependency. In the first part, the fundamental concepts of technological security and information systems infrastructure are presented, emphasizing their essential role in economic processes and national resilience. The next section examines the risks generated by technological and economic dependency, including vulnerabilities in critical sectors and examples of countries affected by insufficient domestic infrastructure. The study then proposes a set of strategic solutions, including the development of national IT infrastructure, increased investments in R&D for indigenous technologies, support for local companies in the tech sector, and the establishment of strategic partnerships for technological development. International best practices are analyzed to demonstrate successful models for reinforcing technological independence. In conclusion, the article underscores the need for sustained investment in domestic technological capabilities and proposes concrete directions for developing resilient and sustainable information systems as a pillar of future economic and national security.

Keywords: information systems; economic dependency; national security

JEL Classification: O33, F52, G28, P16, H56

1. Introduction

In an era marked by accelerated technological advances, technological security has become a fundamental element of economic and national security. Information systems play an essential role in managing and protecting data, automating economic processes and strengthening critical infrastructures.

[1] Associate PhD, Faculty of Security and Defence, National Defence University Carol I, Bucharest, Romania, Address: 68-72 Panduri St., sector 5, 050662, Bucharest, Romania, Corresponding author: dragomir.loredana@unap.ro.

They are widely used in strategic sectors such as telecommunications, the energy industry, defence and finance, contributing to reducing vulnerabilities and increasing economic competitiveness. One of the major objectives of any national economy is to reduce dependence on foreign technologies, especially in the current context of geopolitical competition and the risks associated with the monopolization of technological resources by major economic powers (Zhou & Kim, 2023). Creating its own technological infrastructure not only reduces exposure to external risks, but also stimulates local innovation, providing jobs and contributing to sustainable development. Globally, states are investing heavily in technological security to prevent the risks associated with economic dependence (Patel & Singh, 2024). Among the main threats are cyber-attacks on critical infrastructures, restricted control over technological equipment supplies chains, as well as the excessive influence of large international corporations on local markets. In this context, the implementation of effective strategies for the development of national information systems becomes a priority for ensuring economic and technological resilience (Martinez & Zhang, 2024). This paper explores how information systems can contribute to strengthening technological and economic security, identifying the main risks of external dependence and presenting strategic solutions for the development of national technological autonomy.

1.1. Methodological Approach

This research adopts a qualitative and strategic analytical design, based on a multi-source analysis of academic literature, policy documents, and relevant international case studies. The methodology aims at a comparative assessment of the risks associated with technological dependency, as well as the identification of national and international strategies for strengthening digital sovereignty.

The investigative process included:

- critical analysis of academic sources on technological security and information systems;
- examination of public investment programs in IT infrastructure, research and development, and support for local technology companies;
- selection and interpretation of international best practice examples (EU, USA, Asia) that can be replicated or adapted to the Romanian context.

The information was integrated into a conceptual framework that links national security with digital autonomy, emphasizing the role of information systems in protecting critical infrastructure and reducing external economic dependence. The methodological objective of the study is to formulate viable strategic proposals, grounded in evidence and aligned with contemporary geopolitical and economic realities.

2. The Role of Information Systems in Technological Security

Information systems play an essential role in technological security and, implicitly, in national security, having a direct impact on the protection of critical infrastructure, sensitive data and strategic economic processes. In a global context marked by technological interdependence and risks associated with cyber-attacks, the efficient use of these systems becomes a necessity for any state that wishes to maintain its economic sovereignty and internal security.

One of the most important aspects of information systems in technological security is their ability to monitor and protect IT infrastructures from cyber-attacks. In an era where data and information are critical resources, protecting them against cyber threats is essential to maintaining the functioning of essential institutions and organizations (Nanyen & Brown, 2023). Advanced intrusion detection systems, state-of-the-art firewalls, and encryption solutions are just a few examples of how these technologies contribute to national security. In the economic sector, information systems support (Dragomir, 2021) the development and implementation of technological security policies aimed at reducing dependence on external IT solutions. By investing in their own infrastructures and developing secure digital ecosystems, states can minimize the risks associated with technological vulnerabilities and protect strategic industries (Dragomir, 2016a). For example, the use of blockchain platforms for managing transactions and smart contracts provides a high level of security and transparency in the economy, reducing the risk of fraud and cyber-attacks. Another fundamental aspect is the role of information systems in the field of secure communications. Governments and key institutions use encrypted networks and communication protection technologies to prevent information leaks and ensure the confidentiality of strategic data. In the current context, where attacks on critical infrastructures, such as electricity, transport and health networks, are increasingly common, securing these systems through advanced artificial intelligence and big data solutions becomes imperative (Dragomir, 2016b).

Information systems also contribute to strengthening cyber defense capabilities by integrating threat analysis and forecasting mechanisms. By using machine learning technologies and anomaly detection algorithms, states can anticipate cyber-attacks and react quickly to counter them. These solutions are widely used in command-and-control centers, where real-time risk analysis allows for quick and effective decision-making to protect national security. An important dimension of technological security is the protection of IT infrastructures in the financial sector. Information systems used in central banks, stock exchanges and digital payment institutions are essential for maintaining economic stability (Tache, 2010). Implementing robust cybersecurity mechanisms prevents attacks on trading systems, financial data theft and other fraudulent activities that could destabilize a state's economy. In conclusion, information systems represent a central component of technological and national security, providing effective solutions for protecting critical infrastructures, data and strategic communications. By continuously investing in the development of these systems and by implementing well-structured cybersecurity policies, states can ensure technological independence and reduce vulnerabilities associated with dependence on external solutions. Thus, the intelligent use of advanced technologies contributes to strengthening economic security and protecting national interests in the face of global challenges (Tache, 2009).

3. Strategies for Reducing Economic Dependence Through Information Systems

3.1. Development of National IT Infrastructure and Own Data Centers

Reducing economic dependence by developing national IT infrastructure and its own data centers is an essential strategy for strengthening Romania's economic and technological security. This approach not only minimizes the risks associated with dependence on external suppliers, but also stimulates innovation, economic growth and international competitiveness. Developing a robust IT infrastructure at the national level involves significant investments in communication networks, hardware and

software equipment, as well as in the training of specialists in the field of information technology. By creating and strengthening its own data centers, Romania can ensure the safe storage and management of critical data, thus reducing vulnerabilities related to cybersecurity and the protection of sensitive information. A concrete example in this direction is the approval, in September 2024, of the National Strategy for the Development and Support of Digitalization through the Digital Innovation Centers in Romania. This strategy, proposed by the Ministry of Research, Innovation and Digitalization (MCID), establishes the directions of action for allocating the necessary funds for the development of digital infrastructure and the implementation of innovative technologies in companies and administration. As part of this initiative, the government has allocated 24 million euros to finance seven Digital Innovation Centers (CID) in the country, aimed at supporting the digital transformation of the economy and the public sector. Digital Innovation Centers play a crucial role in this process, providing SMEs and local public authorities with access to infrastructures dedicated to innovation, testing and use of digital technologies. These centers facilitate collaboration between technology providers, beneficiaries of digitalization solutions and research and development institutions, thus contributing to increasing innovation capacity and developing digital skills at the national level. Another relevant project is the Smart Growth, Digitalization and Financial Instruments Programme 2021-2027 (PoCIDIF), co-financed by the European Regional Development Fund, with a total allocation of EUR 2.1 billion. This programme supports the implementation of the national smart specialization strategy by financing investments in digitalization in central public administration, education, culture and SMEs, as well as the development of strategic technologies for Europe. The Agency for Regional Development (ADR) also launched, in autumn 2020, a selection process for CIDs in Romania, candidates to be part of the European network of these centers. 12 such initiatives were pre-selected out of the 20 proposals, highlighting the importance and need for consistent support for the development of digital infrastructure at national level. The implementation of these strategies and projects contributes to reducing the economic and technological gaps between the regions of Romania, promoting balanced and sustainable economic development. By strengthening the national IT infrastructure and its own data centers, Romania can secure a competitive position in the global digital economy, while reducing the vulnerabilities associated with dependence on external technologies. In conclusion, the development of the national IT infrastructure and its own data centers is a vital strategy for reducing Romania's economic and technological dependence. By implementing coherent policies and supporting projects and organizations dedicated to this purpose, our country can ensure sustainable economic growth and strengthened national security in the face of current technological challenges.

3.2. Investments in Research and Development (R&D) for Indigenous Technologies

Investments in research and development (R&D) for indigenous technologies represent a crucial component in the strategy of reducing a nation's economic and technological dependence. These investments are essential for stimulating domestic innovation, creating technological solutions adapted to national needs, and strengthening economic security. By promoting local R&D, Romania can develop its own technologies that respond to challenges in various economic sectors and minimize the risks of dependence on foreign technologies. In the current global context, in which emerging technologies, such as artificial intelligence, the Internet of Things (IoT), blockchain, and cybersecurity, play an increasingly important role, Romania must focus its resources on creating an environment conducive to domestic

research and innovation. In this sense, investments in R&D must target both the development of its own technological products and the formation of highly specialized human capital in the technological field. These investments are also essential for strengthening the national innovation ecosystem and for Romania's integration into global value chains based on advanced technologies. A clear example in this direction is the Competitiveness Operational Program 2014-2020 (POC), managed by the Ministry of European Funds, which had a budget dedicated to research and development of approximately 1.4 billion euros, with the aim of supporting investments in R&D infrastructure and the creation of new technologies. This program financed projects aimed at strengthening the innovation capacity of the private sector and the development of advanced technological solutions in areas such as health, renewable energy, IT and telecommunications. The projects supported by the POC are essential for the development of the domestic technological infrastructure and for the creation of an innovative ecosystem capable of generating domestic solutions that are competitive at an international level. In parallel, the Ministry of Research, Innovation and Digitalization (MCID) runs programs aimed at developing research and development infrastructure and stimulating collaboration between academia, the private sector and public authorities. One such project is the National Research, Development and Innovation Program 2025 (PNCDI III), which includes initiatives for investments in strategic areas, such as cutting-edge technologies, artificial intelligence, robotics and blockchain. These projects not only support the development of local solutions, but also contribute to creating a favorable framework for the development of human capital in the field of R&D. In addition to these government programs, the private sector plays an important role in promoting technological innovation. Many Romanian technology companies have initiated their own research and development projects, in collaboration with research institutes and universities. For example, companies such as Bitdefender and UiPath have invested heavily in the development of innovative software solutions, contributing to the strengthening of Romania's technological capabilities internationally. These investments not only reduce dependence on foreign technologies, but also contribute to the strengthening of a competitive domestic technological ecosystem. Romania also benefits from the support of European research initiatives, such as Horizon Europe, which supports research in strategic areas for the European Union, including advanced digital technologies. Under this program, Romanian researchers can collaborate with partners from other member states to develop innovative solutions that meet the economic and social needs of the region. In conclusion, investments in research and development for indigenous technologies represent a fundamental strategy for reducing Romania's economic and technological dependence. By supporting R&D projects, both at the governmental and private sector levels, Romania can develop its own technological solutions, which will contribute to strengthening economic security and allow the country to play an active role in the global digital economy. Investments in research and development not only reduce the risks associated with external dependence, but also facilitate sustainable development, favoring innovation and economic growth in the long term.

3.3. Policies to Support Local Companies in the Technology Sector

Policies to support local technology companies are essential for ensuring a sustainable and competitive economic ecosystem, especially in a context where dependence on foreign technologies can pose a risk to national economic security. In this digital era, where advanced technologies influence almost all economic areas, supporting local technology companies not only stimulates innovation and economic

development, but also contributes to increasing a nation's economic security. Policies for this sector aim to create a favorable environment for the development of innovative enterprises, promoting investment in research and development (R&D), facilitating access to financing, supporting the formation of human capital in the technological field, and protecting local businesses from external risks. One of the main objectives of policies to support technology companies is to create a legislative framework that encourages innovation and protects the interests of local companies. Governments can implement policies that support the development and commercialization of new technologies through tax incentives, tax breaks, or research and development subsidies. Public investments in digital infrastructure and fundamental research projects can also significantly contribute to creating an environment conducive to local innovation. In Romania, programs such as the Competitiveness Operational Program 2014-2020 or the National Recovery and Resilience Plan (PNRR) were designed to support digitalization and innovation in the public and private sectors. These projects were intended to support companies developing technological solutions, especially in areas such as artificial intelligence, blockchain, the Internet of Things (IoT), and cybersecurity. At the same time, supporting human capital is an essential component of policies supporting the technology sector. These include initiatives aimed at improving IT training and education, promoting collaboration between universities, research institutes, and local industry. In this regard, authorities can implement policies that support educational programs and encourage the attraction and retention of technology talents. For example, by creating business incubators and technology centers of excellence, Romania can encourage young people to develop innovative solutions and start businesses in the technology field, thus reducing dependence on external solutions and generating a positive impact on the national economy. Another important aspect of the policy to support local companies is facilitating access to financing. Companies in the technology sector, especially startups and SMEs, often face difficulties in accessing funds for research and development, despite their innovative potential. In this context, governments can create dedicated financing programs for these companies, such as grants, preferential loans or investment funds. Public-private partnerships can also play a crucial role in attracting the capital needed to develop and scale local technology solutions.

In Romania, financial institutions, such as the European Investment Fund or the National Credit Guarantee Fund for SMEs, provide financial support for companies in the IT sector, encouraging their development and reducing barriers to access to capital. Also, supporting local companies in the technology sector is not limited to financial and educational aspects, but also includes protecting them from unfair competition from large multinational companies or cyber risks. Governments can implement measures to protect the internal market and sensitive data, so that local companies can compete fairly in the global market. In addition, cybersecurity policies, which aim to protect companies' digital infrastructure, are essential to prevent cyber-attacks and ensure their long -term stability. A concrete example of a program to support local companies in the technology sector is the Start-Up Nation Program, which was implemented by the Romanian Government to support entrepreneurship and the development of innovative businesses. This program provides non-repayable financing for the establishment of new businesses, especially in the technological field, and aims to support Romanian entrepreneurs to develop their businesses that meet the needs of the domestic and international market. Under this program, IT startups are particularly supported, as well as initiatives that develop innovative technological solutions. Policies to support local companies in the technological sector are essential for reducing economic and technological dependence on foreign markets, for stimulating innovation and

for creating a sustainable economic ecosystem. By implementing appropriate measures, such as financial, educational and legislative support, Romania can develop a strong and competitive technological industry, capable of facing the economic and technological challenges of the future.

3.4. Strategic Partnerships for the Development of Own Technologies

Strategic partnerships for the development of indigenous technologies are an essential component of national economic strategy, especially in the context of increasing dependence on foreign technological solutions and the associated risks. In this regard, collaborations between governments, research institutions, universities and local companies in the technology sector are fundamental to ensuring a stable and sustainable economic future. Strategic partnerships can facilitate the transfer of knowledge and technology, stimulating innovation and reducing the economic and national security risks generated by dependence on foreign solutions. An effective strategic partnership is based on close collaboration between the public and private sectors, in which governments play the role of facilitators, and companies and research institutions contribute technological know-how. In this context, governments can create policies and initiatives that support investments in indigenous technologies, such as by subsidizing research and development (R&D), by creating national IT infrastructure and by encouraging collaboration between universities, research institutes and local companies. Public-private partnerships can also help strengthen research infrastructure and attract human capital in strategic technological areas. A significant example of a strategic partnership for the development of own technologies is the collaboration between national governments and large technology companies to build data centres and internal IT infrastructure. These partnerships can include both the development of data storage and information processing solutions, and the development of cybersecurity technologies to protect the digital infrastructure of states. Universities and research institutes can also play a crucial role in this process, contributing to technological innovation and the formation of an essential knowledge base for the development of own technologies. Another example of a strategic partnership is the collaboration between governments and technology companies to create solutions based on artificial intelligence (AI) and machine learning. These technologies are extremely important for ensuring economic and national security, as they can contribute to the automation of economic processes, the protection of critical infrastructure and the prevention of cyber-attacks. Strategic partnerships in the field of AI can include investments in research, the development of joint platforms and the creation of innovation ecosystems around these technologies.

In Romania, there are several initiatives and projects that reflect the importance of strategic partnerships for the development of own technologies. A concrete example is the “Digital Romania” project, which aims to strengthen the digital capabilities of the Romanian economy and create a favourable framework for the development of domestic technological solutions. The projects under this program focus on the development of the national IT infrastructure, the creation of innovative digital platforms and the support of Romanian companies in the IT sector in order to reduce dependence on foreign technologies. Also, universities and research institutes in Romania play an essential role in the development of own technologies, through partnerships with international institutions and the private sector. Research and innovation projects in areas such as cybersecurity, big data and artificial intelligence are carried out in collaboration with international institutions, such as the Polyethnic University of Bucharest, which has partnerships with major IT companies and research institutes in the European Union. In terms of

supporting human capital, strategic partnerships can also contribute to the training of a new generation of technology specialists, by developing joint educational programs between universities and companies in the IT sector. These partnerships can include internships, training programs and dual education, so that young people acquire advanced technical skills and contribute to the development of their own technologies. Finally, strategic partnerships for the development of their own technologies are fundamental to ensuring a robust and sustainable technological ecosystem, capable of responding to the economic and national security challenges of the future. Through collaboration between governments, research institutions, universities and private companies, an environment conducive to innovation and development can be created, which contributes to reducing economic and technological dependence on foreign markets and supporting national security. These partnerships must be supported by clear policies and significant investments in research and development, infrastructure and human capital training, to guarantee the long-term success of this strategy.

4. Conclusion

The strategic role of information systems in safeguarding national economic security has become increasingly evident in the context of intensifying geopolitical tensions, global technological competition, and the growing frequency of cyber threats. This article has provided a comprehensive analysis of how access to and control over critical technologies, particularly through the development of resilient and autonomous information infrastructures, are essential prerequisites for ensuring national sovereignty and economic resilience.

The study highlighted that economic and technological dependence on foreign actors exposes national systems to systemic risks, particularly in the case of monopolized technological supply chains and limited domestic capabilities. In this regard, information systems serve not only as operational tools for data management and cyber defense, but also as strategic enablers of economic development, innovation, and digital autonomy.

Our findings emphasize the necessity of coordinated policy efforts aimed at strengthening national IT infrastructure, supporting research and development for indigenous technologies, encouraging the growth of local technology firms, and fostering strategic partnerships between governments, academia, and the private sector. These dimensions are not merely complementary, but synergistic, forming a coherent framework for the consolidation of national innovation ecosystems.

Investments in technological infrastructure and R&D must be sustained and targeted, ensuring that future information systems are not only technologically advanced and secure, but also sustainable and adaptable to emerging challenges. Furthermore, human capital development, through education and skills training in advanced technologies, remains a cornerstone for building the capacity to innovate and maintain technological sovereignty.

Future directions should prioritize the creation of robust, scalable, and adaptive information systems capable of withstanding both internal and external pressures. Public-private and international cooperation will be vital to this endeavor, especially in terms of resource mobilization, technological exchange, and harmonization with global cybersecurity standards. Coherent national strategies should, therefore, integrate digital education, cybersecurity policies, and infrastructure modernization under a unified vision of technological sovereignty and economic security.

Ultimately, the consolidation of a national innovation ecosystem—anchored in domestic capabilities, sustained by targeted strategic investments, and safeguarded by robust information systems—emerges as a foundational pillar for ensuring a nation's long-term economic independence, systemic resilience, and sustainable prosperity. In the context of accelerating global digital transformation and intensifying technological competition, such an ecosystem represents more than a policy objective; it becomes a strategic imperative for national security and economic autonomy.

A well-structured national innovation ecosystem facilitates the endogenous generation of knowledge, technologies, and solutions tailored to the specific needs and vulnerabilities of the local socio-economic context. It integrates universities, research institutes, technology enterprises, and public institutions into a synergistic network, where innovation is continuously fostered through collaboration, knowledge transfer, and co-investment mechanisms. The presence of secure and resilient information systems within this ecosystem not only ensures data integrity and infrastructure protection but also enhances trust, operational continuity, and regulatory compliance—critical attributes for the success of innovation-driven economies. Moreover, by reducing dependency on foreign technologies and global value chains dominated by external actors, such an ecosystem strengthens the strategic autonomy of the state. This mitigates the risks associated with geopolitical volatility, supply chain disruptions, and digital colonialism. At the same time, it enables the country to act proactively—not merely as a consumer of technological advances developed elsewhere, but as an active contributor to global technological standards, digital governance frameworks, and emerging innovation paradigms.

Importantly, the success of this model is contingent upon the existence of coherent public policies that align educational reform, fiscal incentives, research funding, and digital infrastructure investments with national innovation goals. Human capital development must be at the center of these efforts, as the availability of skilled professionals in areas such as artificial intelligence, cybersecurity, data science, and advanced manufacturing is a precondition for technological sovereignty.

In sum, a national innovation ecosystem fortified by secure information systems is not only a defense mechanism against external vulnerabilities, but also a vector of national empowerment. It positions the country as a forward-looking, innovation-driven economy, capable of shaping its own digital future and asserting its interests in the global knowledge economy.

References

Bai, X., Li, Y., & Zhao, J. (2023). Digital transformation and cybersecurity challenges for businesses: A literature review. *Sensors*, 23(15).

Chen, L., & Wang, P. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, 15(18).

Dragomir, F.-L. (2016a). Models of Trust and Reputation in eCommerce. *Acta Universitatis Danubius. Œconomica*, 12(6), 235-242.

Dragomir, F.-L. (2016b). Recommendation and reputation in eCommerce. *EuroEconomica*, 25(2), 151-155.

Dragomir, F.-L. (2017b). Applications of artificial intelligence in decision-making process. *Bulletin of Carol I National Defense University*, 4, 56-61.

Dragomir, F.-L., & Alexandrescu, G. (2017a). The axiomatic character of decision. *Bulletin of Carol I National Defense University*, 6, 16-22.

Dragomir, F.-L., Dumitriu, C., & Bărbulescu, A. (2021). Recommendation Systems-Modeling Abusive Clauses in E-commerce. *International Conference on Electrical, Computers, Communications and Mechatronics Engineering, IEEE*, 1-4.

Dragomir-Constantin, F.-L. (2025a). Thinking Patterns in Decision-Making in Information Systems. *New Trends in Psychology*, 7(1), 89-98.

Dragomir-Constantin, F.-L. (2025b). Thinking Traps: How High-Performance Information Systems Correct Cognitive Biases in Decision-Making. *New Trends in Psychology*, 7(1), 99-108.

Dragomir-Constantin, F.-L. (2025c). Information System for Macroprudential Policies. *Acta Universitatis Danubius. Œconomica*, 21(1), 48-57.

Martinez, R., & Zhang, H. (2024). Recent trends in information and cyber security maturity assessment frameworks: A systematic literature review. *Systems*, 13(1).

Nguyen, T. H., & Brown, S. (2023). Risk-management framework and information-security systems for small and medium-sized enterprises. *Electronics*, 12(17).

Patel, R., & Singh, M. (2024). Assessing the impact of enterprise architecture on digital transformation: A systematic review. Sustainability, 16(20).

Pigola, A., Fischer, B., & de Moraes, G. H. S. M. (2024). Impacts of digital entrepreneurial ecosystems on sustainable development: Insights from Latin America. *Sustainability*, 16(18).

Tache, F. L. (2009). Advice in electronic commerce. *3rd International Workshop on Soft Computing Applications, IEEE*, 111-114.

Tache, F. L. (2010). Trust model for consumer protection (TMCP). *4th International Workshop on Soft Computing Applications, IEEE*, 107-112.

Zhang, K., Wen, Y., & Wu, Y. (2024). How digital innovation ecosystems facilitate low-carbon transformation of the economy based on a dynamic qualitative comparative analysis. *Sustainability*, 16(22).

Zhou, Y., & Kim, D. (2023). How technological, organizational, and environmental factors drive the digital economy: A comprehensive review. *Sustainability*, 15(16).