Philosophy, Economics and Law Review

Vol. 4. No. 2. 2024
Received: 18.07.2024
Revised: 22.11.2024
Accepted: 25.12.2024

Journal homepage: https://phelr.com.ua/en

UDC 330.34:004.9

DOI: 10.63341/2786-491X-2024-2-16

Technological sovereignty of the state: Practical experience of Ukraine and the European Union

Yevhen Novikov*

PhD in Law, Doctoral Student
The Research Institute of State Building and Local Self-Government
of the National Academy of Legal Sciences of Ukraine
61024, 80 Chernyshevska Str., Kharkiv, Ukraine
https://orcid.org/0000-0002-6085-8258

Abstract. The purpose of the study was to comprehensively examine the impact of technological sovereignty on economic and national security. The paper considered key aspects of technological sovereignty. The results of the study showed that technological sovereignty has a substantial and multifaceted impact on national security, including economic, energy stability, and military security of the country. This ensures the sustainability of national economies and reduces dependence on global markets and critical technologies, which is especially important in the context of growing competition with major technology players. Ensuring economic independence also allows the country to control strategically important resources, contributing to more sustainable development in the face of international turbulence. The impact on energy security is manifested through the introduction of innovations in the field of renewable energy sources, the development of own energy efficiency technologies, and the creation of national networks for energy management, which helps to reduce dependence on imported energy resources and increases resistance to external influences, such as energy crises and economic sanctions. Military security, as an important component of national security, is also substantially strengthened through technological sovereignty. In particular, the development of its own cyber technologies, defence systems, artificial intelligence systems, and data analysis technologies minimises the risks of external interference in defence processes and ensures the country's independence in the field of national defence. Technological sovereignty allows for a more effective protection of critical infrastructure from cyber attacks and a reduction of dependence on foreign developments. The experience of Ukraine and the EU showed different approaches to achieving technological independence, including support for national research, development of their own semiconductors and digital technologies, cybersecurity programs and initiatives to reduce technological dependence. These factors highlighted the need to integrate public strategies to build technological sovereignty as a key component of national and economic security

Keywords: technological sovereignty; economic independence; digital infrastructure; data protection; innovation; cybersecurity; energy efficiency

Introduction

Ensuring technological sovereignty in the face of fierce competition and dependence on foreign technologies is one of the priorities of national governments, as it becomes critical for ensuring national security in general and its sectors such as military, economic, and energy security. States feel an urgent need to develop and implement their own technologies, strengthen control over critical infrastructure, and minimise dependence on imported technology solutions. Ensuring technological sovereignty is crucial to reducing the risks of economic vulnerability, especially in the face of global economic competition and the possibility of applying technological sanctions.

Previous research confirms that technological sovereignty and the ability to implement and develop its own technologies is one of the critical factors for ensuring the national security and economic sustainability of the state. In the paper of Y.T. Zang & F. Xiong (2020),

Suggested Citation:
Novikov, Ye. (2024). Technological sovereignty of the state: Practical experience of Ukraine and the European Union. *Philosophy, Economics and Law Review*, 4(2), 16-35. doi: 10.63341/2786-491X-2024-2-16.

*Corresponding author

it is argued that the development of innovation infrastructure and the support for local technology companies are fundamental aspects of achieving technological independence of the state. The researchers argue that building a solid foundation for long-term economic growth requires actively attracting public investment in research and development projects.

M. Robles-Carrillo (2023) and O. Omar *et al*. (2022), in turn, emphasise that technological sovereignty is closely linked to the problems of ensuring cybersecurity and controlling critical information. Their study proves that the availability of national technologies for data protection and control over digital infrastructure provides a high level of protection against external threats. In particular, these researchers point out that digital control is a strategic component of a country's national security, especially in the face of increasing cyber threats. Issues of ensuring technological and digital sovereignty at the academic level are raised in the studies by D. Eckert (2024), H. Roberts (2024), and Ye. Novikov (2024), who considered digital sovereignty as an independent measurement of technological sovereignty. These authors argue that effective management of national digital platforms, the development of their own cyber defence technologies and the implementation of data control contribute to strengthening national security. Countries that create and actively develop their own technology platforms can reduce the economic and political risks associated with external influence.

F. Crespi *et al*. (2021) and R. Csernatoni (2022) draws attention to the importance of adapting foreign technologies to national needs. This is due to the fact that dependence on imported technologies limits the opportunities for implementing own strategic initiatives. As these authors emphasise, the development and implementation of national technological solutions is a necessary condition for achieving full technological sovereignty, which avoids potential threats associated with foreign influence.

J. Hackenbroich *et al*. (2020) and M. Prathap *et al*. (2024) in their studies, focus on the economic aspect of technological sovereignty. They believe that the development of own technologies contributes to creating new jobs and increasing the competitiveness of the national economy. Therefore, national governments must support local companies through public investment and promote startup development to ensure sustainable economic growth in the long term. This, in turn, will help reduce dependence on imported technologies and strengthen national economic sovereignty.

O. Ivanytska & O. Voznenko (2024), and P. Foley *et al*. (2024) draw attention to such an important aspect of the problem as strengthening control over critical infrastructure. Having own technologies is a prerequisite for ensuring the sustainability of life support systems, in particular, in the fields of energy, health, and transport. The researchers argue that controlling infrastructure is key to achieving full sovereignty, as it avoids threats associated with external interference. Studies by D. Badea & D. Ranf (2021), and D. Boga (2024), which highlight the impact of technological sovereignty on military security also deserve attention. The authors argue that the development of national defence technologies is a necessary condition for ensuring protection against potential threats. They emphasise that dependence on foreign technologies in the military sphere can create risks that endanger national security.

The problem of international cooperation in the development of technological standards is raised in the publication of U. Cantner (2024). The author notes that the establishment of international legal norms and standards will help to increase the level of technological independence of each country, reducing the risks associated with unilateral dependence on leading technology players. Previous research confirms that technological sovereignty is critical to national security and economic sustainability. Important aspects are the development of innovative infrastructure and support for local technologies, which reduces dependence on imports and economic risks.

The purpose of this study was to identify the theoretical aspects of technological sovereignty and examine its impact on the economic, energy, and military security of the state. The main objectives of the study were:

- investigate strategies for ensuring technological sovereignty on the example of the EU and Ukraine, covering support for innovation, research, and local technology companies;
- analysis of the relationship between technological and digital sovereignty through the prism of data control, cybersecurity, infrastructure;
- examine the role of technological sovereignty in ensuring economic, energy, and military security on the example of practices used in the EU and Ukraine.

Materials and methods

This study applied a comprehensive approach to the analysis of technological sovereignty and determining its importance for ensuring national security. The approach involves a step-by-step examination of the relationship between controlling critical infrastructure, developing proprietary technologies, and strategies to reduce import dependence. The EU and Ukraine were chosen for the study, as they are actively working to strengthen their technological independence, which makes them illustrative examples for analysis. The study was conducted in stages, with the aim of providing in-depth analysis and systematisation of information related to technological sovereignty. At the first stage, a thorough preparatory work was conducted, which included the collection and analysis of a wide range of political and legal documents, that highlighted in Table 1:

Table 1. Analysed policy and legal documents

Document	Title	Year
Law of Ukraine No. 2297-VI	"On the Protection of Personal Data"	2010
Directive of the European Parliament and of the Council No. 2016/1148	"Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union"	2016
Directive of the European Parliament and of the Council No. 2016/943	"On the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure"	2016
Law of Ukraine No. 2163-VIII	"On the Basic Principles of Cybersecurity in Ukraine"	2017
Order of the Cabinet of Ministers No. 605-r	"On Approval of the Energy Strategy of Ukraine for the Period up to 2035 'Security, Energy Efficiency, Competitiveness'"	2023
Law of Ukraine No. 2657-XII	"On Information"	2023
Law of Ukraine No. 1116-IX	"On State Support of Investment Projects with substantial Investments in Ukraine"	2023
Law of Ukraine No. 3687-XII	On Protection of Rights to Inventions and Utility Models	2023
Law of Ukraine No. 3792-XII	"On Copyright and Related Rights"	2023
Law of Ukraine No. 1089-IX	"On Electronic Communications"	2024
European Commission Documents	Various data and reports	2020-2024
Reports of International Organisations	"United States Agency for International Development"	2022

Source: developed by the author

Special attention was paid to sources covering issues of technological sovereignty in the context of modern challenges of globalisation, the development of digital technologies, and information security. The collection of information allowed forming a general picture of current trends that determine countries' policies in the field of technological independence. Key strategies aimed at strengthening control over critical technologies, in particular, data protection, cybersecurity, creating a national digital infrastructure and developing own technology solutions, were examined.

The second stage of the study consisted of a detailed analysis of the strategy for ensuring technological sovereignty in the EU and Ukraine, in particular, the development of innovation potential, mechanisms for supporting local technology companies and creating a modern research infrastructure. Specific initiatives aimed at promoting the growth of Ukrainian companies in strategic industries were analysed. The third stage explored the relationship between technological and digital sovereignty, where data control, cybersecurity, and the development of reliable infrastructure played an important role. In this context, special attention was paid to data exchange, protection, and storage policies, as data is a key resource in the digital economy. The method of content analysis of EU and Ukrainian documents revealed the main points that demonstrate the interdependence between technological achievements and the need to protect the digital sphere.

The fourth stage was devoted to the assessment of the role of technological sovereignty in ensuring national security, with a special focus on the economic, energy, and military spheres. The mechanisms by which technological independence contributes to the strengthening of security in various industries, such as reducing dependence on foreign suppliers in the energy sector or strengthening military capabilities through the development of their own technologies, were examined. A comparative analysis of examples from the EU and Ukraine's practice in the fields of cybersecurity, state support for information technology (IT) and telecommunications, and the development of technological products exports was conducted, which helped to identify specific mechanisms and solutions through which technological sovereignty increases the country's resilience to external threats and ensures stability in strategically important sectors.

Results

Theoretical foundations of technological and economic sovereignty

Technological sovereignty, as the ability of a state to maintain independence in the field of critical technologies, is an important element of national security and economic stability. The concept of technological sovereignty includes the ability of a country not only to meet critical technology needs but also to actively develop its own resources and technological solutions. Technological sovereignty ensures the control of the national government over key industries and processes, in particular, over critical infrastructure, which is the basis for the functioning of the economy and the social system in general.

In modern globalised world, where the technological sphere is rapidly developing, the issue of sovereignty goes beyond domestic politics and becomes of strategic importance for any state. The country's ability to ensure relative autonomy in information and

communication technologies, cybersecurity, and the development of its own scientific research are fundamental factors for its independence in the technological field. This reduces the risks associated with possible external dependence and provides resilience to crisis situations, such as supply chain disruptions, which were clearly demonstrated during the COVID-19 pandemic. Reducing dependence on imports of strategically important technologies and components is also an important aspect of technological sovereignty. This is especially important in the area of critical infrastructure, where reliable control over resources and technologies can be a crucial factor in national security. In addition, the ability to develop its own technologies and innovative solutions contributes to economic growth and increases the country's competitiveness in the global market. Technological sovereignty not only has a positive impact on the internal stability of the state but also strengthens its position in international relations. Such relative autonomy gives the national population the opportunity to independently choose the vector of its development and maintain stability in the unstable conditions of the global economy.

Control over critical infrastructure is the basis for ensuring national security and sovereignty, especially in the present time, where information and energy systems are important for the functioning of the state and society. Critical infrastructure includes energy networks, telecommunications systems, transport networks, water supply, as well as medical and financial institutions, the continuous operation of which is necessary for the stable functioning of the economy and the well-being of the population. Dependence on foreign suppliers or weaknesses in the cyber defence systems of such infrastructures can create serious risks, including increasing vulnerability to cyber attacks, espionage, and economic pressure from other states or corporations. For states seeking to secure their technological sovereignty, it is important to create their own solutions related to the development of hardware and software for critical infrastructure and organise a high level of cybersecurity. This approach minimises risks and prevents potential threats from unfriendly states that may use technological dependence as a tool of influence. For example, in the energy sector, this may include the development of national energy grid management systems that are independent of software and technologies supplied by foreign companies.

The EU pays special attention to ensuring the security of critical infrastructures, as evidenced by the adoption of the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) (European Commission, 2023a), which obliges member states to provide a reliable level of protection in cyberspace and strengthen the security of national infrastructures. This directive defines common standards for protecting networks and information systems, including monitoring cyber threats, responding quickly to incidents, and ensuring data security in the event of cyber attacks. Thus, NIS2 not only enhances cybersecurity but also supports the EU's technological independence, reducing reliance on external suppliers, which minimises the potential risks associated with foreign interference.

In the context of global digital transformation, ensuring control over critical infrastructure is becoming a strategic priority for many countries, including Ukraine, which is also actively developing its own cybersecurity infrastructure. In view of geopolitical instability and constant cyber threats from Russia, the Ukrainian government pays special attention to strengthening national cybersecurity since the country's critical infrastructure, in particular, the energy, financial, transport and telecommunications sectors, are potential targets for cyber attacks. Ukraine is implementing initiatives to improve cyber defence, in particular, the project "Cybersecurity for critical infrastructure", funded by the EU and the United States of America (United States Agency for International Development, 2022). This project provides for strengthening cyber defence in strategic sectors of the economy through the introduction of modern technologies for monitoring and responding to incidents, as well as the creation of educational programmes for training specialists in the field of cybersecurity. An important step in this area was the adoption of The Law of Ukraine No. 2163-VIII (2017), which regulates the activities of public and private institutions in the field of cybersecurity, defines the rights and obligations of critical infrastructure operators, and provides for mandatory information about cyber incidents. Ukraine is also focusing its efforts on modernising its digital infrastructure and improving its protection systems against cyber attacks in the face of Russian aggression, which has substantially worsened cybersecurity issues.

The main goal of Ukrainian cybersecurity legislation is to protect critical infrastructure, national information resources, and the confidentiality and security of citizens' data. Therewith, Ukrainian legislation still has some gaps compared to the EU, where cybersecurity is regulated by the standards defined by the NIS2 directive. Directive of the European Parliament and of the Council No. 2016/1148 (2016) and its updated version NIS2 (European Commission, 2023a), are the main regulations defining cybersecurity policies in EU member states. The directive obliges the governments of EU member states to develop national cybersecurity strategies, establish focal points and cooperate at the EU level to ensure cybersecurity. NIS2 expands the range of organisations that are required to comply with cybersecurity requirements, including more critical infrastructure sectors such as finance, energy, transportation, and the healthcare sector. NIS2 strengthens the requirements for Risk Management, which includes

mandatory measures for managing data privacy, monitoring cyber threats, and preventing and responding to incidents. An important element is also the introduction of sanctions for violation of requirements, which encourages entities to ensure a high quality of cybersecurity.

Ukrainian legislation in the field of cybersecurity and NIS2 have a lot in common, but there are also substantial differences in the details and binding requirements. For example, Ukrainian legislation focuses less on sanctions and risk management than NIS2. Although the Law of Ukraine No. 2163-VIII (2017) defines the basic principles of cyber defence, it does not regulate in sufficient detail the requirements for risk management, monitoring of cyber threats and data privacy protection, especially in critical infrastructure industries. The EU has stricter data privacy requirements, which include mandatory regular security audits, mandatory reporting on cyber incidents, and critical data access control systems. In Ukraine, such requirements are partially provided for and the legislation does not require regular inspections or audits in certain sectors. This creates potential risks for the sustainability of Ukrainian networks and the confidentiality of critical data.

Ukrainian cybersecurity legislation needs comprehensive improvement to ensure the effective protection of national interests in the digital sphere. The first important issue is cyber risk management. Ukraine needs to introduce mandatory procedures for monitoring and evaluating cyber risks, which are the standard in the EU thanks to the NIS2 directive. The directive obliges EU member states to ensure systematic monitoring of cyber risks in the public and private sectors and impose sanctions on organisations that neglect established standards. This will help strengthen companies' responsibility for data security and increase their readiness for cyber threats.

The second key issue is the protection of the privacy and personal data of citizens. The introduction of mandatory protocols for the protection of personal information is extremely important, especially in the face of increased cyber threats. In this area, it is necessary to establish clearer rules for access to confidential data and tighten the requirements for the entities that process them. For example, EU law provides for strict sanctions for data privacy violations, which helps reduce the risk of leaks and unauthorised access. The third area that needs substantial improvement concerns the protection of critical infrastructure. The law should provide for mandatory certification of equipment used in critical networks to ensure its resistance to cyber attacks. The EU has special certification requirements for equipment manufacturers that guarantee that products comply with cybersecurity standards (European Green Deal, 2019). In Ukraine, such certification is just beginning to be implemented, and additional steps at the legislative level are needed to fully protect such critical sectors as energy, transport, and communications.

Since 2022, the government has been actively implementing initiatives aimed at strengthening national cybersecurity, relying on the support of international partners, including the United Nations and various international foundations. This collaboration includes the development and implementation of comprehensive measures covering a wide range of tasks to reduce cyber threats. In particular, the government has initiated programmes such as the Tallinn Mechanism (Ministry of Foreign..., 2023) and Cybersecurity (United States Agency for International Development, 2022) aimed at protecting critical infrastructure, such as energy, transport, and financial networks, from potential cyber attacks that can disrupt the work of government agencies and affect the daily lives of citizens. These programmes include several key components. Firstly, the government, together with international partners, constantly monitors cyber threats, analysing threats from various sources to respond in a timely manner to any attempts of unauthorised access to critical systems. For this purpose, modern technologies are used, such as artificial intelligence and machine learning, which allows automatically identifying suspicious activity and preventing potential attacks. In addition, one of the priority areas is the creation of educational programmes to raise awareness about cybersecurity among citizens and civil servants (European Commission, 2022b). Under the auspices of the United Nations and other international foundations, a series of training seminars and trainings was organised for employees of government agencies, during which cybersecurity specialists transfer their knowledge and skills. These measures are aimed at ensuring that employees have threat recognition skills and know how to act correctly in the face of a cyber incident, which substantially increases the overall level of data security. Considerable attention is also paid to the development of the national cyber defence system, which provides for the modernisation of equipment and expansion of the network of data centres, and the introduction of new information security standards. Due to the cooperation with international organisations, Ukraine receives technical support that allows it to introduce the latest technologies in the field of cybersecurity. For example, some applications include the use of advanced encryption tools to protect citizens' sensitive data and the development of tools to detect phishing attacks and other cybercrimes.

Reducing dependence on imports in strategically important areas is one of the priorities of economic policy, as it helps to avoid risks that arise during global crises, such as the COVID-19 pandemic, which clearly demonstrated the vulnerability of international supply chains. With borders closed and global commodity flows severely restricted, the economies of many countries heavily dependent on imports were threatened by shortages of essential goods, medical supplies, food, and other critical resources. This situation has prompted

states to rethink their policy of supporting their own production. The import substitution policy, which has become a response to these challenges, focuses on creating conditions for the development of national production of goods and services that were previously imported from abroad.

In addition, such policies create new jobs and stimulate employment growth, which has a positive impact on the economic stability of the state. Support for national manufacturers of critical goods, such as medicines, medical equipment, food, and personal protective equipment, allows creating a reliable internal reserves for rapid response to emergencies. The EU also actively invests in research aimed at creating innovative products and technologies that can replace imported analogues, increasing the competitiveness of local producers in the domestic and foreign markets (European Commission, 2021a). Such policies contribute to strengthening the economic sustainability and independence of both member states and the entire united Europe. In the event of new crises associated with restrictions on the international market, a state that has a developed internal production base will be able to provide the population with the necessary resources and goods, reducing the impact of external factors on the domestic economy. Thus, import substitution becomes a critical element on the path to economic autonomy, contributing to the long-term stability and sustainability of the economy.

In the field of cybersecurity, protection from cyber threats and the development of intellectual property are equally important. Ukrainian legislation in the field of intellectual property is important for protecting the development of companies and scientists working on innovative technologies. In the context of rapid technology development and globalisation, intellectual property protection is a critical factor for stimulating innovation and attracting investment. The protection of intellectual property in Ukraine is conducted through such legal instruments as patents, copyrights, and trade secrets but the effectiveness of each of these tools depends on how much they meet European standards and how much their application contributes to innovation.

In Ukraine, relations in the field of patent law are regulated by The Law of Ukraine No. 3687-XII (2023). According to this law, a patent grants its owner the exclusive right to an invention or utility model, allowing third parties to prohibit the use of this object without the permission of the patent owner. In Ukraine, as in the EU countries, a patent can be issued for new, useful, and industrially applicable inventions. The law also allows the transfer of patents and licenses to others, which is important for the commercialisation of innovations. Thereby, unlike many EU member states, Ukraine's patent system has some gaps. For example, in Ukraine, there are difficulties with effective patent protection in court since patent cases are often considered for a long time and legal costs can be high. In the EU, according to the European Patent Convention (2020), there is a single patenting system for all member states, which simplifies the process of protecting intellectual property at the European level. The introduction of such practices in Ukraine could improve the legal protection of inventions of Ukrainian developers and researchers.

The Law of Ukraine No. 3792-XII "On Copyright and Related Rights" (2023) regulates the protection of creative works, such as literary and artistic works, software, music, photographs, and other forms of creative activity. In Ukraine, copyright protects works during the author's lifetime and 70 years after their death, which meets European standards. Copyright provides authors with the right to control the use of their works and receive remuneration for their commercial use. Despite the existence of such legislation, copyright protection in Ukraine faces certain challenges. The main problem is the high level of piracy, in particular, in the digital sphere, and insufficient law enforcement practice to protect copyright in court. In the EU, considerable attention is paid to the protection of copyright on the internet, in particular, under the Digital Single Market Copyright Directive, which obliges platforms to remove content that violates copyright (European Commission, 2021b). Ukraine has not yet fully adapted this legislation, which is a challenge for Ukrainian developers and authors who suffer losses due to the illegal use of their works. It is advisable to improve the mechanisms for protecting copyright on the internet and increase responsibility for violations of these rights to strengthen legal protection in Ukraine.

Trade secrets in Ukraine are protected by The Law of Ukraine No. 236/96-VR (2020) and are also partially regulated by the Civil Code. Trade secrets protect information that is valuable to businesses but not patented, such as production processes, formulas, marketing strategies, and other confidential information. Owners of trade secrets have the right to prohibit access to this information by third parties, which helps prevent its illegal use. However, in Ukraine, the protection of trade secrets has limitations compared to European standards. The Directive of the European Parliament and of the Council No. 2016/943 (2016), which provides broader protection of confidential information and introduces specific requirements for evidence and sanctions in the event of its illegal disclosure. Ukrainian legislation does not provide for clear procedures and sanctions, which makes the protection of trade secrets less effective. The introduction of European standards in Ukraine could strengthen the protection of confidential information and help protect innovations, in particular, in high-tech industries where such assets are extremely valuable.

Ukrainian legislation in the field of intellectual property is important for protecting innovations and stimulating the development of technologies but

it needs to be improved to ensure better compliance with European standards. It is necessary to improve the protection mechanisms in the judicial system, adapt the regulations on copyright protection on the internet, and strengthen the protection of trade secrets to improve the protection of intellectual property in Ukraine. The introduction of European standards will help create favourable conditions for Ukrainian innovators, reduce the risks associated with unfair use of their developments, and ensure better integration of Ukraine into the international system of intellectual property protection.

Ukraine needs to strengthen legal mechanisms and improve relevant legislation to strengthen national sovereignty in the digital sphere and ensure the protection of public and private interests. This is particularly important in light of the growing influence of large international corporations such as Google, Microsoft, and Amazon, which play a critical role in the development of digital infrastructure in Ukraine, the EU, and the world in general. Their activities cover the provision of cloud services, the development of artificial intelligence, internet services, and other technological solutions that are becoming critical for the modern economy and society. However, along with these advantages, their influence poses a threat to the digital sovereignty of states because such companies control a substantial part of digital infrastructure, data, and communication channels. The EU and Ukraine are gradually implementing various legal mechanisms and expanding regulation in the field of cybersecurity and data management to minimise these risks and maintain control over strategic digital resources.

The EU adopted the Digital Markets Act (DMA) in 2022, which has become an important tool for limiting the dominance of large technology companies (European Commission, 2022c). The DMA Law defines the so-called "watchmen" of digital markets – companies that have a large market share and control major platforms such as search engines, online markets, and cloud services. These companies include Google, Amazon, Apple, Microsoft, and Meta. The DMA Law sets out a number of responsibilities and prohibitions for these companies, in particular, prohibits abuse of a dominant position, such as restricting access to competitors, requires ensuring the interoperability of their services with other platforms, and prohibits the preferential promotion of their own products in search results or other services. This law is designed to reduce barriers to entry for new companies and ensure competition, promoting balanced digital sovereignty in the EU. With DMA, EU member states can have greater control over data generated and processed on their territory, limiting the ability of large corporations to monopolise digital infrastructure and services.

For Ukraine, which seeks integration with the EU, adapting such initiatives is an important task. Although the Ukrainian legislation, in particular, The Law of Ukraine No. 1089-IX (2024), regulates certain aspects of the digital sphere, it does not cover all the issues that the DMA solves, in particular, the control of the dominance of large corporations. The use of DMA experience in Ukraine leads to several important changes, for example, the establishment of criteria for determining companies that have a dominant position in the market and restrictions on monopolisation of markets to support local players and ensure equal conditions for all market participants. Another important initiative could be the development of mechanisms for monitoring the storage and processing of data on the territory of Ukraine. Large technology corporations store substantial amounts of data from citizens and businesses in foreign data centres, which poses a potential threat to national security. A legal restriction on the storage of certain categories of data outside the country and the requirement for transparency in data processing could strengthen Ukraine's digital sovereignty. However, Ukraine faces certain challenges in implementing such initiatives. The dominance of international corporations is often the result of their technological and resource superiority, which is difficult to quickly compensate for by the local market since Ukrainian companies often do not have enough resources to compete with technology giants such as Microsoft or Google. In addition, the adaptation of the DMA requires substantial institutional and resource changes, including the creation of an independent body to monitor the activities of technology giants in a market that requires funding, specialised knowledge, and technical resources that can be difficult to find in an economic crisis.

Ensuring independence in critical technology areas allows states to reduce dependence on external suppliers, increase economic sustainability, and protect national interests. Strategies of technological sovereignty are aimed at developing their own scientific and technological competencies, supporting internal innovations, and creating conditions for the production of strategically important technologies at the national level. The development of the IT sector and telecommunications industry has substantial potential to stimulate employment. According to the state statistics service of Ukraine, in 2023, about 300 thousand people were employed in the IT sector, and this number is growing by 6-7% annually (IT Research Ukraine, 2023). With additional investment, especially in national startups and telecommunications equipment, it can expected that the number of new jobs may increase. For comparison, in EU countries that have implemented government programmes to support the digital economy, employment growth in IT industries increased from 3.5% to 4.6% from 2015-2023. For example, in Poland, job creation in technology industries increased from 2.6% in 2015 to 4.6% in 2023, due to government support in innovation programmes (Eurostat, 2023).

The increase in exports is an important indicator of economic growth and the country's ability to compete in the international market. In 2023, Ukraine's exports brought the Ukrainian economy USD 6.7 billion in revenue, which is usually 8.5% less than in 2022, but still a record number. The IT sector has reduced its share in total service exports to 42% but the sector still retains its status as the first largest among Ukrainian export industries (IT Ukraine Association, 2024). Investments in the telecommunications sector, especially in national producers, could substantially increase this indicator, creating new export directions, contributing to the growth of gross domestic product (GDP), and strengthening the country's economic independence. In addition to stimulating domestic production, such investments have the potential to strengthen the innovation base and attract highly qualified personnel to the sector, which in the future can increase Ukraine's competitiveness on the world stage. For comparison, the export volume of IT and telecommunications equipment in Poland in 2023 amounted to about USD 25.5 billion (Statista, 2023), which was made possible by the expansion of the domestic manufacturers' market, the implementation of national grants programmes, such as SMART path (National Centre for..., 2023) and FENG (National Centre for..., 2021), and support for research projects in the field of telecommunications technologies. Poland has successfully integrated its manufacturers into European supply chains, focusing on high-tech solutions and cooperation with international partners.

Similar programmes in Ukraine could become an impetus for the development of national producers, contributing to their entry into foreign markets, in particular, to the EU and the United States. Measures such as government grants for research and development, tax breaks for exporters, and the creation of industrial parks focused on the production of telecommunications equipment can substantially strengthen the country's economic potential. The success of such initiatives depends on their focus on supporting both large companies and small innovative enterprises that form the ecosystem for sustainable development of the sector.

The development of technological sovereignty is a complex multi-component process that involves the constant introduction of the latest technologies and innovative solutions. Without active investment in innovation, this process is impossible since it is the innovation that contributes to the creation of technological products that can compete in the global market. The EU, aware of the importance of technological independence, has developed a number of programmes to drive innovation, such as Horizon Europe, an initiative aimed at supporting research and development in key areas, including digital technologies, environmental stability, and cybersecurity (European Commission, 2021b). This programme provides funding for research projects that contribute to the development of the European scientific and technological base, strengthening its competitiveness and reducing dependence on third-country technologies.

The EU experience can be particularly useful for Ukraine, which also strives to achieve technological sovereignty and actively develops the innovation sector. In Ukraine, more and more attention is paid to supporting startups and technology companies, such as the "State in a smartphone". Such initiatives are aimed at promoting the development of high-tech enterprises, providing them with access to investment, tax incentives, and modern infrastructure for implementing innovative projects. It is also worth noting that EU programmes, such as Horizon Europe, place special emphasis on the sustainability and safety of technologies being developed. This is extremely relevant for Ukraine, as creating a stable ecosystem for technology startups will help strengthen the country's cybersecurity and ensure the smooth functioning of critical infrastructure in the face of external threats. Such efforts will help Ukraine strengthen its national economy and create its own technological products that meet international quality and safety standards.

Research funding is a critical factor in achieving technological sovereignty, as it provides the necessary resources to develop innovations and technologies that can reduce the country's dependence on foreign markets. The experience of the EU, where about 2% of GDP is spent on research and development, is substantial: substantial funds are invested in strategic areas such as green energy, artificial intelligence, cybersecurity, and advanced manufacturing technologies (Table 1). This allows EU countries not only to develop their domestic technological potential but also to consolidate their positions in highly competitive global markets.

Table 2. Comparison of research and development costs in Ukraine and the EU

Year	Spending in Ukraine (% of GDP)	Spending in the EU (% of GDP)	Ukraine's GDP (in current US dollars), billion	EU GDP (in current US dollars), trillion
2018	0.47	2.19	130	15.9
2019	0.43	2.22	153	15.6
2020	0.4	2.3	156	15.3
2021	0.38	2.28	199	17.3
2022	0.33	2.27	161	16.7

Source: compiled on the basis of World Bank (2024a; 2024b)

For Ukraine, increasing investment in research and innovation projects is an important step towards creating a strong technological infrastructure that will contribute to ensuring national security and economic sustainability. Investing in developing technology solutions and supporting innovative startups can help a country avoid dependence on imported technologies, which can be critical in the face of global crises or sanctions restrictions. Successful implementation of these plans requires attracting not only public but also private investment and active cooperation with universities, scientific institutes, and international organisations. Co-financing programmes and incubators for innovative projects can create an effective ecosystem for the development of research activities.

National companies and startups are the basis for the development of technological sovereignty, as they are able to generate innovative solutions adapted to the needs of the domestic market. The support of such companies helps to create the country's own high-tech products, reducing dependence on foreign technologies and licenses. For example, the EU has a specialised programme, the European Innovation Council (2024), which provides grants and investments to promising startups and small businesses, contributing to their growth and competitiveness in the global market. This allows the EU to encourage the creation of unique technologies and maintain control over critical technological processes. Ukraine is also implementing mechanisms for financing and supporting national innovative enterprises. The Ukrainian Startup Foundation provides grant support to young companies operating in high-tech industries such as IT, medical technologies, green energy, and artificial intelligence. This fund helps not only financially but also provides access to mentoring programmes that promote business development and increase its innovative potential. Due to such initiatives, Ukrainian technology companies are able to implement their own ideas, while maintaining control over intellectual property and reducing the need for imported technologies.

Additionally, special economic zones and tax incentives for startups are often created at the national level, which encourages their development and allows them to attract investment. Such measures are aimed at ensuring that young companies can get the necessary resources and technological infrastructure to develop products that meet national needs. The support of local technology companies not only contributes to the development of the national innovation ecosystem but also helps to strengthen the country's position in the global technology market, gradually building economic independence and technological sovereignty.

In the context of technological sovereignty, it is important to consider separately the issue of digital sovereignty, which reflects the ability of a state or organisation not only to own and control digital information, technologies, and infrastructure within its jurisdiction but also to create conditions for their effective protection from external threats and influences. Digital sovereignty provides states with the ability to control data flows, regulate access to them, and set their own rules for processing them, which is especially important in an era of globalisation and the growing importance of data as a strategic resource. This aspect of sovereignty is critical in a globalised economy, where data volumes are growing exponentially and their uncontrolled use can pose a potential threat to national security. In an environment where most of the data is stored in cloud services controlled by large technology companies based abroad, there is a risk of transmitting confidential information to foreign governments or unfriendly structures. Digital sovereignty involves not only technical measures to protect data but also the creation of a legislative framework that controls the use of information by foreign companies. This includes the adoption of national data protection standards and the introduction of legislation restricting the ability of foreign organisations to access citizens' personal data without appropriate government permits. One of the most influential examples is the General Data Protection Regulation (2018) (GDPR) in the EU, which sets strict rules for the processing of personal data of EU citizens. It includes the requirement to obtain consent to data processing, restrictions on their transfer outside the EU, and sanctions for violations. The GDPR applies to all companies that work with the data of EU citizens, in particular, foreign ones, which allows the EU to strengthen digital sovereignty. Notably, Germany introduced the Information Technology Security Act 2.0, which expands cybersecurity measures to protect critical infrastructure from possible threats and restricts the use of foreign technologies in strategically important sectors (Federal Office for..., 2021). This allows the government to conduct national security checks against suppliers, helping to strengthen digital sovereignty.

In Ukraine, The Law of Ukraine No. 2297-VI (2010) operates, which was supplemented in accordance with the GDPR standards. It ensures the protection of the personal data of citizens, defines the requirements for the processing and storage of data, and restricts their transfer abroad without the consent of the data subjects or the government. In the face of a full-scale war with Russia, Ukraine is actively working on additional standards to protect data of national importance. Unlike the broader concept of technological sovereignty, which encompasses the ability of a state or organisation to control the entire technological cycle – from hardware manufacturing to software development and scientific development – digital sovereignty focuses on protecting data and ensuring the reliability of information systems. This includes the ability of a country to use its own resources to protect its information assets, build a national infrastructure for data processing and

store strategically important information on the territory of the country, which ensures independence from external sources and prevents possible cyber attacks. Ensuring digital sovereignty also requires states to have special institutions and regulators that are able to control the information technology market and monitor its participants. In addition, within the framework of digital sovereignty, many countries are developing strategies to support national IT companies and create conditions for the development of their own technological solutions, which reduces dependence on foreign software and services. This policy allows increasing the level of data security, stimulating the development of the domestic market, and maintaining economic stability in the event of external threats, such as sanctions or geopolitical tensions.

Data control is a key aspect of both technological and digital sovereignty. This means ensuring a full cycle of storage, processing, and protection of information on the territory of the state, which minimises the risks of interference by foreign players, ensuring control over critical information, including personal data of citizens, commercial information, and government data. The EU has adopted a number of initiatives to ensure such conditions, in particular, the GDPR (2018), which sets high standards for data protection and requirements for companies that process personal data of EU citizens, regardless of where they are located. The GDPR regulates, in particular, the mandatory obtaining of consent to data processing, grants users the right to delete personal data (the "right to be forgotten") and requires notification of data leaks.

Ukraine is also working to improve the level of data protection and bring it closer to European standards as part of the state's overall digitalisation strategy. This includes the adoption of laws that bring Ukraine's legal framework closer to EU standards and the introduction of modern technologies to strengthen cybersecurity. Ukrainian enterprises, especially those working with European markets, are adapting their practices to meet the requirements of the GDPR (2018), which allows them to remain competitive and reduce risks to the personal data of citizens. Data control is strategically important for maintaining information sovereignty and increasing citizens' trust in digital services, providing them with security and confidentiality guarantees. In Ukraine, this role is performed by a number of legal acts aimed at ensuring the protection of personal information and compliance with national and international standards. The fundamental document in this area is the Law of Ukraine No. 2297-VI (2010). It regulates the processing and protection of personal data, ensuring the rights of subjects to privacy and control over personal information. The law obliges data processing entities to ensure the confidentiality and security of information, which creates a basis for protecting citizens' rights and increases trust in digital services. The Law of Ukraine No. 2657-XII (2023) is also important as it plays a critical role in ensuring information sovereignty, as it determines the procedure for storing, processing, and distributing information, including personal data. This law protects the rights of citizens to the confidentiality of personal data and restricts the possibility of their illegal access without the permission of the relevant person. This contributes to the creation of a secure digital environment for personal and commercial transactions and contributes to the economic development of the state in the face of globalisation and constant cyber threats.

Another important component is ensuring cybersecurity, as cyberspace in 2024 is critical for the economic, social, and national security of each country. With the proliferation of digital technologies and the growing dependence of government institutions, businesses, and citizens on network technologies and systems, protecting against cyber threats is becoming a top priority to ensure digital sovereignty. A security breach in cyberspace can lead to the loss of sensitive data, economic losses, and in some cases even undermine the stability of the state. The EU sees cybersecurity as one of the fundamental elements of its digital sovereignty strategy. In 2020, the Cybersecurity Act (European Commission, 2020a) was adopted, which established the basis for strengthening common security standards in EU member states. One of the key institutions responsible for implementing this strategy is the European Union Agency for Network and Information Security (ENISA), which develops and implements a pan-European Cybersecurity Policy. ENISA supports member states in improving their cyberattack protection systems by providing expert advice, research, and recommendations on protecting critical infrastructures. ENISA is also engaged in raising awareness of cyber threats among the public, which is an important aspect of ensuring a collective level of cybersecurity in the EU.

Ukraine, in turn, also pays considerable attention to cybersecurity, especially given the growing cyber attacks by states and groups that pose a threat to national security. One of the main documents in this area is the national cybersecurity strategy of Ukraine, which defines the main tasks and priorities in ensuring the protection of public and private sectors from cyber threats (Decree of the..., 2021b). The strategy includes measures to strengthen the protection of critical infrastructures, such as the energy sector, transport, communications, and the banking system. Ukraine is also working to create and strengthen specialised institutions responsible for protection in cyberspace. In particular, the Government Computer Emergency Response Team of Ukraine was created – a cyber incident response team that provides monitoring and rapid response to cyber attacks. In addition, Ukraine is developing partnerships with other countries and international organisations, in particular, the EU and NATO, to exchange

experience and information on cyber threats and receive expert support. Due to the aggression from Russia, Ukraine is forced to quickly increase the level of cyber defence, paying attention not only to the protection of state institutions but also to the private sector. It is important that cybersecurity in Ukraine includes measures to raise citizens' awareness of the basics of digital hygiene, which helps reduce the risk of cyber threats.

Infrastructure is another aspect that ensures the interaction of technological and digital sovereignty. The EU invests in the development of its own data centres and data networks, in particular, through GAIA-X projects to ensure the sustainability and independence of digital infrastructure. Infrastructure is one of the key aspects that unite technological and digital sovereignty, as it provides the physical basis for the functioning of all digital systems. Infrastructure refers to hardware and software resources and data transmission networks that ensure the smooth operation of digital services, cloud technologies, and data processing. In a globalised environment, this includes not only national networks, but also cross-border communications, data centres, and information storage platforms, which in turn requires substantial investment and appropriate policies. Infrastructure plays an important role in ensuring technological and digital sovereignty both in the EU and in Ukraine. Investing in national networks and data centres and ensuring high cybersecurity standards is essential to reduce dependence on foreign suppliers and maintain control over critical digital resources.

Digital and technological sovereignty are interrelated but relatively autonomous phenomena, the provision of which is crucial for the national security, and political and economic independence of the state. Technological sovereignty implies the ability of a country to develop, control, and implement its own technological solutions, minimising dependence on foreign suppliers and ensuring the autonomy of critical systems. Digital sovereignty, in turn, focuses on controlling information resources, including the protection of personal data, cybersecurity, and the ability of the state to maintain the functioning of information infrastructure regardless of external threats or pressure. The relationship between technological and digital sovereignty is manifested due to the fact that the achievement of one is impossible without the other. For example, effective control over data, in particular, its processing and storage, depends on the availability of a sovereign technical infrastructure that a country owns and manages. Countries that do not have a sufficiently developed internal infrastructure are often forced to turn to foreign cloud storage service providers, which can lead to loss of control over critical data.

In the current conditions of global instability and increased international competition, the issue of technological sovereignty is becoming of key importance for ensuring the economic, energy, and military security of countries. Technological sovereignty implies the ability of the state to control the development, production, and implementation of strategically important technologies without critical dependence on foreign suppliers. The lack of such capabilities poses risks to national security, limits the ability to quickly adapt to changes in the global political and economic environment, and increases vulnerability to external pressure. The concept of technological sovereignty is becoming particularly important in the context of growing technological competition at the global level. A country's economic security depends on its ability to meet its own technological needs and avoid critical dependence on external suppliers, which is especially important for strategically important industries such as energy, defence, and information technology. The economic stability of the state directly depends on the development of its technologies, which are the foundation for ensuring competitiveness in the world market and protecting national interests (Table 2).

Table 3. High-tech exports (in current US dollars) to Ukraine and the EU

Year	Exports in Ukraine (billion)	Exports in the EU (billion)
2018	1.2	571.5
2019	1.1	580.2
2020	1.1	528
2021	1.2	633.8
2022	0.8	693.6

Source: compiled on the basis of World Bank (2024c)

Continuous access to advanced technologies is one of the key factors of economic sustainability, as it allows states to reduce production costs, improve the quality of goods and services, and expand employment through the development of high-tech industries. In addition, the presence of own technologies substantially reduces the risk of a technological embargo that may be imposed in the context of worsening international relations. In this context, economic independence is an important factor in national security, because a country dependent on the import of strategic technologies can suffer substantial losses if access to them is restricted.

The EU, considering the challenges of the global economy, is actively developing its own technological base to reduce dependence on foreign suppliers in strategic sectors. Industries such as semiconductor manufacturing, pharmaceuticals, advanced materials manufacturing, and energy equipment are a priority

for the EU. In 2020, the European Commission adopted the "European Industrial Strategy", which provides for the creation of production facilities in high-tech sectors (European Commission, 2020b). According to this document, the EU aims to meet domestic demand for strategic technologies, in particular, in the field of semiconductors used in all sectors of the economy – from the automotive to the information-communications industry. This approach allows the EU to minimise the risks associated with potential dependence on external suppliers and ensure stability in the event of economic or political upheaval.

In Ukraine, similar goals are laid down in the concept of "digital sovereignty", which includes the development of national technology products and the strengthening of local IT infrastructure. This concept provides for the creation of our own data centres, cloud services, and the development of advanced technologies such as artificial intelligence, blockchain, and cybersecurity. These measures are aimed at strengthening Ukraine's digital independence and reducing dependence on foreign IT solutions and technologies, which is especially important in the context of global instability and hybrid threats. Ukraine is also taking steps to attract investment in national technology startups that will be able to provide the country with innovative solutions in the future and strengthen its position in the global market.

Ensuring technological sovereignty is vital to reducing a country's economic vulnerability, as it reduces dependence on foreign suppliers and protects the economy from external threats such as economic sanctions, trade barriers, and political conflicts. Developing our own technologies and manufacturing capabilities helps strengthen the national economy, ensuring continuous access to critical resources, products, and services, even in the face of global crises or political instability. The EU example clearly illustrates how the introduction of resource-based technology solutions increases economic sustainability in a world where geopolitical and economic challenges are becoming increasingly unpredictable. The EU has launched an active policy of supporting strategic autonomy, in particular, through initiatives related to the semiconductor industry, renewable energy, and digital technologies. The COVID-19 pandemic has demonstrated the dangers of dependence on global supply chains: production shutdowns in one region have led to shortages of vital resources such as medical equipment, medicines, and materials for their production. This experience has forced the EU to reconsider its strategies and increase investment in the domestic technology base, which has reduced the risks of economic disruptions and increased the ability to respond quickly to emergencies.

For Ukraine, reducing economic vulnerability is an extremely important task, given the systematic challenges caused by Russia's military aggression and the unstable political situation in the region. Economic vulnerability increases a country's dependence on external economic conditions, which may limit its ability to withstand economic shocks such as export blockages, energy crises, or financial sanctions. In the context of prolonged military aggression, economic independence becomes a strategic priority, as it allows strengthening the financial stability of the state, preserving the viability of the national economy, and reducing the influence of external forces on internal processes. A number of legislative acts were introduced to increase economic stability. In Ukraine, one of the key documents is The Law of Ukraine No. 2163-VIII (2017), which is aimed at protecting critical infrastructure from cyber attacks, which is especially relevant in the context of modern hybrid threats. Another example is The Law of Ukraine No. 1116-IX (2023a) which aims to create favourable conditions for attracting domestic and foreign investment, which strengthens the economy and reduces dependence on external loans.

The development of technological sovereignty is not only a matter of national prestige but also a strategic necessity for improving economic security. It allows maintaining control over critical industries, reducing dependence on imported technologies and resources, and strengthening the country's position in the international arena. Considering the current economic and political challenges, creating conditions for the development of technologies becomes a necessary element of a long-term economic development strategy. Technological sovereignty in the energy sector means the ability of the state not only to use but also to develop and implement own technological solutions to ensure a stable and safe energy supply, minimising dependence on external suppliers. This approach includes the development of national energy technologies that allow the state to be more independent of global fluctuations in energy markets and increase resilience to risks associated with the political and economic instability of energy suppliers. The development of own technological potential in the energy sector helps to reduce the vulnerability of the economy to external threats, such as sharp fluctuations in the prices of oil, natural gas, and other energy carriers, which can affect the cost of production and the standard of living of the population. In addition, the availability of national energy technologies allows the state to move faster and more efficiently to renewable energy sources, such as solar, wind, and hydropower, which is an important factor in the context of current global challenges related to climate change and the need to reduce greenhouse gas emissions. Countries invest in the development of innovation, research, and implementation of advanced solutions in such areas as smartgrids, energy-efficient technologies, energy storage, and demand management systems to achieve technological sovereignty in the energy sector. These technologies allow ensuring reliable energy supply and optimising its consumption,

thus reducing dependence on energy imports and increasing energy security.

In addition, energy technological sovereignty helps the state avoid foreign policy pressure associated with the need to import energy resources. As the EU experience shows, countries that invest in the development of their own renewable energy sources and energy infrastructure can achieve greater autonomy and sustainability. This approach is particularly important for countries facing geopolitical risks, in particular, in the case of Ukraine, which, due to its dependence on fossil fuel imports, is at constant risk of energy vulnerability. The EU in its strategic documents, such as The European Green Deal (2019), focuses on the need to reduce dependence on energy imports and directs substantial efforts to develop an independent energy system. This strategy provides for achieving climate neutrality by 2050 and creating a new model of economic growth based on the use of renewable energy sources, energy conservation, and the gradual abandonment of fossil fuels. One of the key goals of the European Green Course is to develop technologies that can not only reduce greenhouse gas emissions but also increase the energy independence of EU member states. This approach aims to reduce vulnerability to external energy crises that may arise due to geopolitical conflicts or fluctuations in oil and gas prices. The development of renewable sources such as solar, wind, and hydropower allows the EU to reduce its dependence on imported energy resources and ensure a sustainable energy balance. In particular, the EU aims to achieve the goal of 45% of the share of renewable energy in total energy consumption by 2030 (European Commission, 2023b).

In Ukraine, similar goals are laid down in the energy strategy until 2035, which provides for reducing dependence on energy imports by developing its own energy sector and gradually switching to renewable energy sources (Order of the era, 2023). The strategy aims to increase the country's energy independence, in particular, by stimulating the production of energy from renewable sources such as solar, wind, hydro, and bioenergy, which will reduce the volume of purchases of fossil fuels on international markets. The energy strategy until 2035 also provides for measures to modernise the energy infrastructure and improve energy-saving technologies and energy efficiency in industry and utilities. This includes the reconstruction of old power plants, reducing energy losses during transportation and optimising energy systems, which will increase the stability of energy supply and reduce dependence on energy imports. The transition to renewable sources is an important strategic step not only for energy independence but also for the environmental security of Ukraine. The introduction of green energy reduces greenhouse gas emissions and contributes to the achievement of EU environmental standards, which Ukraine strives for in the framework of cooperation with the EU. The energy strategy also focuses on the need to integrate the Ukrainian energy system with the European one, which will contribute not only to the stability of the domestic market but also create opportunities for exporting Ukrainian green energy to the European market.

Smart energy and renewable energy sources are also important elements of energy sovereignty, which allow efficient management of energy resources and minimise energy losses. Smart networks integrate technologies that provide monitoring, control, and optimisation of energy flows, increasing the stability and flexibility of the power grid. Through the introduction of smart technologies, the EU seeks to reduce dependence on external suppliers and make the energy system more adaptive to market fluctuations. Renewable energy sources – wind, solar, hydro, and bioenergy – are the basis of modern energy strategies aimed at ensuring energy security. The use of renewable energy sources reduces dependence on imported energy resources and contributes to the stability of energy supply, especially in the face of fluctuations in prices for traditional energy carriers.

One of the advantages of technological sovereignty in the energy sector is the ability to reduce the country's energy vulnerability, which is critical for the stable functioning of the national economy and ensuring the well-being of the population. Dependence on imports of energy resources and equipment makes states vulnerable to price fluctuations, geopolitical conflicts, and external sanctions and limits their ability to respond independently to emergencies in the energy sector. Maintaining technological sovereignty through the development of our own energy technologies, including renewable energy sources, helps reduce these risks. The EU has been working for many years to reduce energy dependence, especially on oil and natural gas imports from unstable or potentially unfriendly countries. The EU strategy provides for the active development of renewable energy sources and local technological capacities, including energy storage technologies and the development of smart networks, which ensures the sustainability of the energy system and the stability of supplies. The European Green Deal (2019) initiative, as well as the REPowerEU (European Commission, 2022a) plan, are aimed at reducing Russian energy imports, improving the efficiency of the energy sector, and expanding the share of renewable energy sources in the EU's energy balance (European Commission, 2021a). This not only helps to reduce the risk of an energy crisis but also creates additional opportunities for innovation and job creation in the green sector of the economy.

For Ukraine, reducing energy vulnerability is a priority in the context of constant threats to energy security, in particular, in the context of military aggression and possible restrictions on energy supplies from abroad. In the face of these challenges, technological sovereignty in the energy sector becomes the key to economic and national security. The introduction of

national technologies for energy production and support for the development of renewable energy sources, in particular, solar, wind, and bioenergy, contribute to reducing dependence on imported energy carriers, which ensures stability in crisis conditions. Ukraine is actively implementing such initiatives, in particular, in the development of solar and wind power plants, which reduces dependence on energy imports. Technological sovereignty in the military field is a strategic advantage that allows a state to effectively protect its national interests and ensure security without having to rely on foreign technology, equipment, or spare parts. This means that the state is able to independently develop, produce, and modernise weapons and military equipment, which ensures independence from external suppliers and substantially reduces the risks of loss of defence capability in the event of restrictions or sanctions. In today's environment, where conflicts are often hybrid in nature and use high-tech means of warfare, the ability to respond quickly and adapt to new threats is crucial.

Dependence on foreign military-technical supplies creates a number of risks. Firstly, it increases vulnerability to the policy decisions of supplier countries, which may restrict access to critical technologies or even completely cut off supplies in the event of an escalation of conflicts. Secondly, limited access to advanced technologies makes it impossible to effectively modernise the armed forces and creates a technological gap between the state and potential opponents. For example, states that have limited access to modern communications systems, cyber defence, or intelligence tools risk losing their edge in a modern war where information and technology play a vital role.

EU countries are aware of the importance of technological sovereignty in the military field and are taking measures to strengthen their autonomy. For example, the European Defence Fund programme aims to support research and development in the field of defence technologies, including artificial intelligence systems, cyber defence tools, robotics, and the latest weapons systems (European Commission, 2020c). This allows EU countries to jointly develop technologies, reducing their dependence on third countries and simultaneously increasing their collective security. For Ukraine, the issue of military technological sovereignty has become particularly important in the context of a full-scale war with Russia, which substantially affects the country's security strategy. The ability to independently produce and maintain critical elements of military equipment is key to ensuring the operational independence of the Armed Forces of Ukraine and reducing dependence on foreign supplies, which may be limited or even blocked in crisis situations. The ability of Ukraine to independently produce armoured vehicles, air defence systems, unmanned aerial vehicles, electronic warfare systems, and other high-tech means helps to strengthen the combat capability and mobility of the Ukrainian army and provides a faster response to operational needs. The National defence-industrial strategy of Ukraine, approved by the government, provides for the development of advanced technologies in the field of defence and incentives for local producers of defence products (Decree of the..., 2021a). It is aimed at creating an independent and competitive defence industry that can meet both domestic needs and ensure the export of defence products. This allows saving financial resources within the country, investing them in the local research and development sector, which contributes to the creation of new jobs, the development of the high-tech sector, and the improvement of the economic situation in general.

In addition, technological sovereignty provides Ukraine with the ability to adapt its weapons systems to specific combat conditions, which is important given the specific challenges and threats that the country faces. In the context of modern hybrid warfare, Ukraine is actively developing cyber defence technologies, electronic warfare tools, and systems for collecting intelligence information, which allows effectively counteracting modern methods of aggression. The development of the country's own technologies ensures not only defence capability but also contributes to the formation of national technological potential, which is an important aspect for long-term economic and political stability.

The development of our own military technologies is an important factor for improving military capabilities, operational independence, and ensuring national security in the face of modern threats. The EU is aware of the importance of technological sovereignty in the military sphere, and therefore actively works to develop its defence capabilities. Within the framework of the EU defence policy, projects are being implemented aimed at introducing the latest technologies into command and control systems, which allows member states to better coordinate actions, improve information exchange, and respond to threats faster and more effectively. In particular, the development of European unmanned aerial vehicles and intelligence systems is aimed at ensuring autonomy in the field of defence and reducing dependence on third-country technologies. Programmes such as the European Defence Fund support innovative research and development of the latest military technologies, including work on artificial intelligence, cyber defence, and robotic systems (European Commission, 2020c).

Ukraine is also implementing programmes aimed at developing and implementing modern military technologies to improve national security. Among the most successful examples is the development and use of unmanned aircraft systems, such as the Bayraktar complex, which is used to monitor borders and protect against potential threats. Although Bayraktar is of Turkish origin, Ukraine is actively involved in its modernisation and adaptation to local conditions (Ministry

of Defence..., 2024). The use of such systems gives Ukraine a substantial advantage in intelligence and rapid response to threats. In addition, Ukraine is actively developing its own air defence and radar systems to protect against air threats. Modernisation and local production of radar systems can substantially strengthen the country's ability to resist air attacks, in particular, from unmanned aerial vehicles and missiles.

Technological sovereignty is a key condition for ensuring the country's economic, energy, and military security, especially in the current context of global challenges and threats. The development of technologies allows states to reduce dependence on foreign suppliers, strengthen economic sustainability, and increase the level of independence in strategically important sectors. Ensuring economic sustainability directly depends on the ability of the state to develop and use its own technologies because external dependence on suppliers increases the risks of economic vulnerability. In the energy sector, technological sovereignty ensures energy independence, especially through the development of renewable energy sources and the introduction of smart energy solutions. Military security also depends substantially on technological sovereignty, because the development of national defence technologies, such as unmanned systems, air defence systems, and cyber defence tools, allows strengthening defence capabilities and independence in the field of security. Technological sovereignty is the basis for the stability and independence of the state. Providing their own technological capabilities in the economic, energy, and military spheres is an important strategic direction for countries seeking to minimise external dependence and protect their interests in the face of global instability.

Discussion

The results of the study emphasise the importance of technological and economic sovereignty for national security and stability of the state's economy. Technological sovereignty allows a country to control critical infrastructure, protect data, and develop its own innovative capabilities, which reduces dependence on foreign technologies and minimises the risks associated with cyber threats or economic pressure from other countries. This helps strengthen the state's resilience to global challenges, such as geopolitical conflicts, sanctions, or disruptions in the supply of key technologies.

The studies by I. Yakoviyk & Ye. Novikov (2023), and K. Lingfu *et al*. (2024) emphasise that technological independence is not only a sign of a country's economic maturity but also a critical factor in its sustainability in the face of global challenges. The authors state that reducing dependence on foreign technologies allows countries to avoid the negative impact of fluctuations in world markets, especially in cases of political instability or trade sanctions. Such measures reduce the vulnerability of the economy and provide an opportunity for the continuous development of key industries. The country's ability to produce and develop its own technologies provides control over critical infrastructures, increases competitiveness in the international arena, and contributes to the creation of new jobs in the technology sector. The results of this study also confirm this trend: countries that invest in the development of domestic technological potential show a more stable economy, less susceptible to external economic shocks and risks associated with dependence on imports. Technological independence contributes to increasing innovation potential, which in the long term allows states to develop high-tech industries and maintain economic growth at a more stable level.

The study shows the importance of digital sovereignty as a separate aspect of technological sovereignty. Digital sovereignty provides states with the ability to control key elements of their digital infrastructures and effectively protect critical data from external influences. An analysis of cyber threats in the EU confirms that the ability to protect digital resources and information flows is critical for national security. Implementing digital sovereignty strategies aimed at strengthening internal control over data allows countries to ensure stability and reduce the risks of influence from foreign companies and governments. A. Shoker (2023) and B. Park (2024) emphasise that this approach contributes to the formation of a sustainable digital ecosystem that makes states less vulnerable to cyber attacks and threats to the information space. This area is particularly important in the context of the current growth of cyber attacks and the growing influence of foreign companies on data management.

Based on the conclusions of J. Edler *et al*. (2023), strategic support for innovation can increase the level of technological independence and create favourable conditions for the active development of the national technology market. This includes financial support for research and development, the creation of incubators for startups, and assistance in creating a favourable legislative environment that encourages innovation. The study further emphasises that strategic support for innovation helps attract talented specialists and create high-tech clusters that can become the basis for long-term economic growth. Investment in innovation also helps to increase the competitiveness of national companies in international markets, allowing them to implement the latest technologies and optimise production processes. Countries that actively support innovative startups and promote technology development achieve the highest level of technological sovereignty and economic stability. Such countries can respond more effectively to global challenges, reduce dependence on imported technologies, and develop their own scientific developments. In addition, the development of the domestic technology market creates new jobs, promotes economic diversification, and

reduces the risks associated with economic fluctuations at the global level.

Energy independence is another important aspect of technological sovereignty that was analysed in this study. The conclusions are consistent with those of B. Andriienko (2024) and M. Ade (2024), noting that the development of smart energy and renewable energy sources is key to the energy security of states. The experience of the EU and Ukraine, examined in the framework of this paper, demonstrates that the use of renewable energy sources allows states to reduce dependence on energy imports and increase energy stability. Thus, the results confirm that the development of energy resources contributes to strengthening national sovereignty and protecting the economy from global fluctuations in energy prices.

Special attention is paid to the relationship between technological and military sovereignty since both of these aspects play a key role in ensuring national security and strategic independence. The study confirms that the development of national technologies in the defence sector, including cybersecurity, can substantially increase the level of state protection from external threats. According to the findings of F. Sauer (2021) and J. Reis *et al*. (2021), investments in the development of defence technologies contribute to reducing dependence on foreign weapons and control systems, which provides greater control over critical military resources and reduces the level of military risks.

The study confirms that ensuring technological independence in the field of defence plays a critical role in maintaining national security and stability of the state. This not only allows the country to protect its interests more effectively but also forms a strategic basis for state sovereignty. States that develop their own defence technologies are becoming less dependent on external suppliers of weapons and equipment, which, in turn, reduces the risks associated with possible sanctions or embargoes from other countries. In addition, it provides an opportunity to adapt weapons and systems to the specific defence needs of the country, making the national security system more flexible and independent. This is confirmed by the studies conducted by S. Kılıç (2024), and F. Attinà & M. Karammia (2024), which stress that such states also occupy a more stable position in international relations since the ability to provide their own protection increases their autonomy on the world stage. Investing in defence technologies, including the development of air defence systems, radars, drones, and cybersecurity systems, allows effectively responding to new threats such as hybrid wars, cyber attacks, and new types of weapons used by potential aggressors. For example, the active introduction of high-tech defence solutions contributes to the country's ability to quickly restore its defence potential and take countermeasures in response to any threats.

An important component of the study was the assessment of EU policies, which largely determine the content and direction of economic, political, administrative, and legal reforms in candidate countries and neighbouring states. This is evident both in the requirements for compliance with EU standards and in the mechanisms of economic and legal cooperation that regulate the EU's relations with these states. This is confirmed by the papers of I. Yakoviyk *et al*. (2018) and N. Helwig & V. Sinkkonen (2022), noting that it is the EU, as a supranational entity, that sets the framework for the political identity and administrative reforms of these countries. National governments, despite the influence of the EU, choose the direction and pace of integration themselves, coordinating them with their own national interests. The study confirms the importance of technological sovereignty for state security and economic independence. The development of the state's own technologies in the fields of energy, cybersecurity, and defence helps to reduce the risks of dependence on imports and ensures the stability and sustainability of the country in the face of global challenges.

Conclusions

The results of the study confirm that technological sovereignty contributes to sustainable economic development by reducing import dependence and ensuring the integration of national innovations in important industries such as information technology, energy, telecommunications and defence. Thanks to the development of its own technological potential, the state increases its competitiveness in the world market, as well as protects its economy from possible fluctuations in international markets and economic crises. This is particularly relevant in the current context of growing global instability. Technological sovereignty also contributes to improving energy security, in particular, through the introduction of renewable energy sources, the development of energy-efficient technologies and the creation of National Energy Management Systems. This not only reduces their dependence on imported energy but also makes them less vulnerable to external influences, such as energy crises or economic sanctions. The introduction of domestic production of energy technologies allows maintaining the stability of the economy and protecting it from global risks. In addition to economic and energy security, technological sovereignty plays an important role in ensuring military security. The development of its own defence technologies and cyber defence systems substantially reduces the risk of interference in military processes, as well as increases the level of state autonomy in providing national defence.

The experience of Ukraine and the EU clearly illustrates different approaches to achieving technological independence. In Ukraine, technological sovereignty is seen as an important component of national security, including the development of cybersecurity,

national research, and semiconductor development. The EU pays considerable attention to digital technologies and cybersecurity, developing programmes to support research and initiatives to reduce technological dependence on partner countries. Key challenges to technological sovereignty are the lack of political will in individual countries, especially due to internal political conflicts or short-term economic interests, as well as limited access to resources in developing countries to implement their own technologies. Corruption, especially in countries with low levels of transparency, can undermine the implementation of technology strategies through the interests of certain economic groups that are interested in maintaining the status quo. The combination of these factors slows down the process of achieving technological independence and requires more detailed analysis. The limitation of the study was also the limited available data, since the concept of technological sovereignty is relatively new in economic and political science, which makes it difficult to analyse its long-term impact. Further research may focus on analysing specific strategies to support national technologies and develop innovative institutions to strengthen economic stability.

Acknowledgements
None.

Conflict of interest
None.

References
[1] Ade, M. (2024). *The role of smart grids in modernizing power distribution and energy efficiency*. Retrieved from https://www.researchgate.net/publication/384445107_The_Role_of_Smart_Grids_in_Modernizing_Power_Distribution_and_Energy_Efficiency.
[2] Andriienko, B. (2024). The theoretical meaning of the concept of "smart energy system". *Economic Herald of the Donbas*, 75-76(1-2), 14-19. doi: 10.12958/1817-3772-2024-1-2(75-76)-14-19.
[3] Attinà, F., & Carammia, M. (2024). EU, world order transition and strategic autonomy. *European Foreign Affairs Review*, 29(3), 275-294. doi: 10.54648/EERR2024013.
[4] Badea, D., & Ranf, D. (2021). The impact of technological development on managerial resilience in the military organisation. *Romanian Military Thinking*, 2021(4), 260-271. doi: 10.55535/RMT.2021.4.15.
[5] Boga, D. (2024). Military leadership and resilience. In A. Sookermany (Ed.), *Handbook of military sciences* (pp. 1-20). Cham: Springer. doi: 10.1007/978-3-030-02866-4_101-2.
[6] Cantner, U. (2024). Technological sovereignty in a time of radical technological change. In Y. Ouyang, R.R. Nelson & H. Hanusch (Eds.), *Technological revolution and new driving forces for global sustainable development* (pp. 59-64). Singapore: Springer. doi: 10.1007/978-981-97-7332-9_8.
[7] Crespi, F., Caravella, S., Menghini, M., & Salvatori, C. (2021). European technological sovereignty: An emerging framework for policy strategy. *Intereconomics*, 56(6), 348-354. doi: 10.1007/s10272-021-1013-6.
[8] Csernatoni, R. (2022). The EU's hegemonic imaginaries: From European strategic autonomy in defence to technological sovereignty. *European Security*, 31(3), 395-414. doi: 10.1080/09662839.2022.2103370.
[9] Directive of the European Parliament and of the Council No. 2016/1148 "Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union". (2016, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.
[10] Directive of the European Parliament and of the Council No. 2016/943 "On the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure". (2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.
[11] Eckert, D. (2024). Seeking digital sovereignty. In D. Eckert (Eds.), *40 Years of European digital policies* (pp. 147-168). Cham: Springer. doi: 10.1007/978-3-031-61641-9_9.
[12] Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy*, 52(6), article number 104765. doi: 10.1016/j.respol.2023.104765.
[13] European Commission. (2020a). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.
[14] European Commission. (2020b). *European industrial strategy*. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en.
[15] European Commission. (2020c). *The European Defence Fund at a glance*. Retrieved from https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en.
[16] European Commission. (2021a). *Horizon Europe*. Retrieved from https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

[17] European Commission. (2021b). *New EU copyright rules that will benefit creators, businesses and consumers start to apply*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1807.
[18] European Commission. (2022a). *REPowerEU: A plan to rapidly reduce dependence on Russian fossil fuels and fast forward the green transition*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3131.
[19] European Commission. (2022b). *Advancing Europe's digital decade The EU: Pioneering the way to a safe and trusted digital world*. Retrieved from https://state-of-the-union.ec.europa.eu/state-union-2022/state-union-achievements/advancing-europes-digital-decade_en.
[20] European Commission. (2022c). *What is the DMA about?*. Retrieved from https://digital-markets-act.ec.europa.eu/about-dma_en.
[21] European Commission. (2023a). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.
[22] European Commission. (2023b). *State of the Energy Union 2023: EU responds effectively to crisis, looks to the future, and accelerates the green transition*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5188.
[23] European Commission. (2024). *New rules to boost cybersecurity of EU's critical entities and networks*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342.
[24] European Green Deal. (2019). Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en.
[25] European Innovation Council. (2024). Retrieved from https://eic.ec.europa.eu/eic-2025-work-programme_en.
[26] European Patent Convention. (2020). Retrieved from https://www.epo.org/en/legal/epc.
[27] Eurostat. (2023). *Employed ICT specialists*. Retrieved from https://ec.europa.eu/eurostat/databrowser/view/ISOC_SKS_ITSPT__custom_13663996/default/table?lang=en.
[28] Federal Office for Information Security of Germany. (2021). *Second act on increasing the security of IT systems* (*German IT Security Act 2.0*). Retrieved from https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig-2-0_node.html.
[29] Foley, P., Moro, L., Neis, B., Stephenson, R., Mellin, R., Singh, G., Hall, P., Kelly, R., & Kulsum, U. (2024). Expanding infrastructure ontologies: Integrative and critical insights for coastal studies and governance. *Coastal Studies & Society*, 3(4), 203-226. doi: 10.1177/26349817241282440.
[30] General Data Protection Regulation. (2018). Retrieved from https://gdpr-info.eu/.
[31] Hackenbroich, J., Oertel, J., Sandner, P., & Zerka, P. (2020). *Defending Europe's economic sovereignty: New ways to resist economic coercion*. Retrieved from http://www.jstor.org/stable/resrep26434.
[32] Helwig, N., & Sinkkonen, V. (2022). Strategic autonomy and the EU as a global actor: The evolution, debate and theory of a contested term. European *Foreign Affairs Review*, 27, 1-20. doi: 10.54648/eerr2022009.
[33] IT Research Ukraine. (2023). Retrieved from https://itcluster.lviv.ua/wp-content/uploads/2023/12/it-research-ukraine-2023-public-eng.pdf.
[34] IT Ukraine Association. (2024). *In 2023, Ukrainian IT services export faced its first decline in years*. Retrieved from https://itukraine.org.ua/en/in-2023-ukrainian-it-services-export-faced-its-first-decline-in-years/.
[35] Ivanytska, O., & Voznenko, O. (2024). Risk management of critical infrastructure. *Finance of Ukraine*, 6, 93-107. doi: 10.33763/finukr2024.06.093.
[36] Kılıç, S. (2024). Half-hearted or pragmatic? Explaining EU strategic autonomy and the European defence fund through institutional dynamics. *Central European Journal of International and Security Studies*, 18(1), 43-72. doi: 10.51870/FSLG6223.
[37] Law of Ukraine No. 1089-IX "On Electronic Communications". (2024, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1089-20?lang=en#Text.
[38] Law of Ukraine No. 1116-IX "On State Support of Investment Projects with Significant Investments in Ukraine". (2023, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1116-20?lang=en#Text.
[39] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19?lang=en#Text.
[40] Law of Ukraine No. 2297-VI "On the Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.
[41] Law of Ukraine No. 236/96-VR "On Protection Against Unfair Competition". (2020, June). Retrieved from https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80?lang=en#Text.
[42] Law of Ukraine No. 2657-XII "On Information". (2023, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12?lang=en#Text.
[43] Law of Ukraine No. 3687-XII "On Protection of Rights to Inventions and Utility Models". (2023, December). Retrieved from https://zakon.rada.gov.ua/laws/show/3687-12?lang=en#Text.

[44] Law of Ukraine No. 3792-XII "On Copyright and Related Rights". (2023, December). Retrieved from https://zakon.rada.gov.ua/laws/show/3792-12?lang=en#Text.
[45] Lingfu, K., Bano, S., Saraih, U.N., Shah, N., & Soomro, B. (2024). Digital technology and entrepreneurship: Unveiling the bridging role of digital innovation. *European Journal of Innovation Management*. doi: 10.1108/EJIM-02-2024-0132.
[46] Ministry of Defence of Ukraine. (2024). *The MoD has already commissioned more than 40 samples of drones and more than 20 ground robots since the start of 2024*. Retrieved from https://www.mil.gov.ua/en/news/2024/06/01/the-mod-has-already-commissioned/.
[47] Ministry of Foreign Affairs of Ukraine. (2023). *Tallinn Mechanism: Ukraine and international partners launch new tool for cyber cooperation*. Retrieved from https://www.kmu.gov.ua/en/news/tallinnskyi-mekhanizm-ukraina-ta-mizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori.
[48] National Centre for Research and Development. (2021). *European Funds for a Modern Economy programme*. Retrieved from https://surl.li/gxcgfe.
[49] National Centre for Research and Development. (2023). *SMART path – phased projects*. Retrieved from https://www.gov.pl/web/ncbr/sciezka-smart-projekty-fazowane.
[50] Novikov, Ye. (2024). Digital sovereignty: Conceptual challenges and constitutional implications. *Constitutional and Legal Academic Studies*, 1, 61-69. doi: 10.24144/2663-5399.2024.1.08.
[51] Omar, O., Aldajani, I., Juwaihan, M., & Leiner, M. (2022). Cybersecurity in sovereignty reform. In I.M. AlDajani & M. Leiner (Eds.), *Reconciliation, heritage and social inclusion in the Middle East and North Africa* (pp. 109-128). Cham: Springer. doi: 10.1007/978-3-031-08713-4_8.
[52] Order of the Cabinet of Ministers No. 605-r "On Approval of the Energy Strategy of Ukraine for the Period up to 2035 "Security, Energy Efficiency, Competitiveness"". (2023, August). Retrieved from https://zakon.rada.gov.ua/laws/show/605-2017-%D1%80#Text.
[53] Park, B. (2024). *Digital sovereignty*. doi: 10.13140/RG.2.2.27759.24488.
[54] Prathap, M., Suresh, A., Seth, B., & Behera, S. (2024). Economic uncertainty and impact of governments' spending on economic growth: An empirical study of emerging market economies. *Global Journal of Emerging Market Economies*, 17(2), 180-198. doi: 10.1177/09749101241287863.
[55] Reis, J., Cohen, Y., Melão, N., Costa, J., & Jorge, D. (2021). High-tech defense industries: Developing autonomous intelligent systems. *Applied Sciences*, 11(11), article number 4920. doi: 10.3390/app11114920.
[56] Roberts, H. (2024). Digital sovereignty and artificial intelligence: A normative approach. *Ethics and Information Technology*, 26, article number 09810. doi: 10.1007/s10676-024-09810-5.
[57] Robles-Carrillo, M. (2023). The European Union strategy for cybersecurity. In D.M. Vicente, S. de Vasconcelos Casimiro & C. Chen (Eds.), *The legal challenges of the fourth industrial revolution* (pp. 173-192). Cham: Springer. doi: 10.1007/978-3-031-40516-7_10.
[58] Sauer, F. (2021). Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible. *International Review of the Red Cross*, 102(913), 235-259. doi: 10.1017/S1816383120000466.
[59] Shoker, A. (2023). Digital sovereignty strategies for every nation. *Applied Cybersecurity & Internet Governance*. doi: 10.48550/arXiv.2307.01791.
[60] Statista. (2023). *Value of the information and communications technology (ICT) market in Poland from 2020 to 2023*. Retrieved from https://www.statista.com/statistics/1258937/poland-value-of-the-ict-market/.
[61] United States Agency for International Development. (2022). *Cybersecurity of Ukraine*. Retrieved from https://www.usaid.gov/uk/ukraine/fact-sheets/aug-05-2022-cybersecurity.
[62] World Bank. (2024a). *Research and development expenditure (% of GDP) – Ukraine, European Union.* Retrieved from https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=UA-EU.
[63] World Bank. (2024b). *GDP (current US$) – Ukraine, European Union*. Retrieved from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2023&locations=UA-EU&start=2018.
[64] World Bank. (2024c). *High-technology exports (current US$) – Ukraine, European Union*. Retrieved from https://data.worldbank.org/indicator/TX.VAL.TECH.CD?locations=UA-EU.
[65] Yakoviyk, I., & Novikov, Ye. (2023). European technological sovereignty. In *Materials of the III international scientific conference "Innovative trends of the present in the field of natural, humanitarian and exact sciences"* (pp. 62-64). Rivne: European Scientific Platform. doi: 10.36074/mcnd-29.09.2023.
[66] Yakoviyk, I.V., Shestopal, S.S., Baranov, P.P., & Blokhina, N.A. (2018). State sovereignty and sovereign rights: EU and national sovereignty. *Opcion*, 34(87), 376-385.
[67] Zang, L., & Xiong, F. (2020). How (when) does technological innovation improve government effectiveness? An empirical investigation with cross-national evidence. *Science and Public Policy*, 47(1), 103-113. doi: 10.1093/scipol/scz050.

Технологічний суверенітет держави: практичний досвід України та Європейського Союзу

Євген Новіков
Кандидат юридичних наук, докторант
Науково-дослідний інститут державного будівництва та місцевого самоврядування
Національної академії правових наук України
61024, вул. Чернишевська, 80, м. Харків, Україна
https://orcid.org/0000-0002-6085-8258

Анотація. Метою дослідження було всебічне вивчення впливу технологічного суверенітету на економічну та національну безпеку. У роботі розглянуто ключові аспекти технологічного суверенітету. Результати дослідження засвідчили, що технологічний суверенітет чинить значний і багатогранний вплив на національну безпеку, охоплюючи економічну, енергетичну стабільність та військову безпеку країни. Це забезпечує стійкість національних економік, знижує залежність від глобальних ринків та критичних технологій, що особливо важливо у контексті зростаючої конкуренції з великими технологічними гравцями. Забезпечення економічної незалежності також дозволяє країні контролювати стратегічно важливі ресурси, сприяючи більш стійкому розвитку в умовах міжнародної турбулентності. Вплив на енергетичну безпеку проявляється через впровадження інновацій у галузі відновлюваних джерел енергії, розвитку власних технологій з енергоефективності та створення національних мереж для управління енергоресурсами, що сприяє зниженню залежності від імпортованих енергоресурсів і підвищує стійкість до зовнішніх впливів, таких як енергетичні кризи та економічні санкції. Військова безпека, як важливий компонент національної безпеки, також значно зміцнюється завдяки технологічному суверенітету. Зокрема, розвиток власних кібертехнологій, оборонних систем, систем штучного інтелекту та технологій аналізу даних мінімізує ризики зовнішнього втручання в оборонні процеси та забезпечує країні незалежність у сфері національної оборони. Технологічний суверенітет дозволяє ефективніше захищати критичну інфраструктуру від кібератак і знижувати залежність від іноземних розробок. Досвід України та ЄС свідчить про різні підходи до досягнення технологічної незалежності, що включають підтримку національних досліджень, розробку власних напівпровідників, розвиток цифрових технологій, програм кібербезпеки та ініціатив для зменшення технологічної залежності. Ці фактори підкреслили необхідність інтеграції державних стратегій для побудови технологічного суверенітету як ключової складової національної та економічної безпеки

Ключові слова: технологічний суверенітет; економічна незалежність; цифрова інфраструктура; захист даних; інновації; кібербезпека; енергоефективність