

Digital Sovereignty for National Cybersecurity

Razil Mirzeyev¹ , Tofiq Mirzeyev¹ , Faig Musayev²  and Shakir Aliyev¹  

¹Department of Design and Industrial Technologies, Azerbaijan Technological University, Ganja, Azerbaijan

²Department of Information Technology and Security, Azerbaijan Technological University, Ganja, Azerbaijan

Received: 04.09.2026

Accepted: 29.09.2026

Published: 09.10.2026

<https://doi.org/10.54414/RGMW6792>

Copyright: © 2026 by the authors.
Licensee: Journal of Smart Technologies and Computational Systems, Western Caspian University, Baku, Azerbaijan. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Abstract: In modern times, the rapid development of information technologies has led to the formation of new directions in the security policies of states. The digitalization process affects all sectors of the economy, public administration, and society. Alongside this process, cybersecurity issues are also becoming increasingly relevant. State information systems, strategic infrastructures, and personal data databases are exposed to various cyber threats. In this regard, the concept of digital sovereignty has become a crucial component of national security. Digital sovereignty refers to a state's ability to independently manage and protect its own information space, data, and digital infrastructure. This concept ensures the protection of the state's technological resources, databases, and communication systems against external influences. The article examines the essence of digital sovereignty, its role in the national cybersecurity system, and the strategies implemented by states in this area. Furthermore, issues regarding the development of local technologies, the protection of national databases, and the formulation of cybersecurity policy in ensuring information security were analyzed. The results of the study show that strengthening digital sovereignty enhances states' resilience against cyber threats and serves to protect national interests.

Keywords: digital sovereignty, cybersecurity, information security, national security, information technologies, cyber threats, digital infrastructure

1. Introduction

Cybersecurity emerged with the development of information technologies and has become an increasingly important field over time. Cybersecurity is a set of measures and technologies that ensure the protection of computer systems, networks, and data against unauthorized access, attacks, and malicious software. The emergence of this field is closely linked to the development of computers and the Internet. The history of cybersecurity begins with the advent of computers in the mid-20th century. The first electronic computers, created in the 1950s, were primarily used for military and scientific purposes. At that time, computers were not interconnected, and data security was ensured primarily through physical protection. In other words, the computers were kept in special rooms, and only certain individuals were permitted to use them. The creation of computer networks in the 1960s gave impetus to the development of the cybersecurity field. During this period, ARPANET, one of the first major computer networks, was created in the United States. This network facilitated the exchange of information among various universities and research centers. With the interconnection of computers, the issue of data protection and secure transmission became increasingly important [1].

The first computer viruses and malicious programs began to appear in the 1970s. In 1971, the Creeper Virus, considered one of the first computer viruses in history, was created. This virus spread across the

network and displayed a message on the computer screen. Subsequently, a program named Reaper was developed to remove this virus. This program is considered the first antivirus program in history. With the spread of personal computers in the 1980s, the number of viruses also increased. Many new malicious programs emerged during this period. One of them was Brain Virus, created in 1986. This virus is considered one of the first widely spread computer viruses in the world and primarily spread via disks.

The widespread adoption of the Internet in the 1990s further exacerbated cybersecurity issues. With the increase in the number of internet users, hacker attacks, data theft, spam, and other cybercrimes have also begun to rise. During this period, antivirus programs, firewall systems, and other security technologies were developed [2].

Since the 2000s, cybersecurity has become an increasingly strategic field. Banking systems, government agencies, companies, and individual users began to be targeted by cyberattacks. In the modern era, cybersecurity encompasses the protection not only of computers but also of mobile devices, cloud systems, and all technologies that operate via the internet. Artificial intelligence, encryption technologies, and modern defense systems are considered key tools in this field. Cybersecurity emerged alongside the development of computer technologies and has today become one of the most important areas of security in the world. In the modern information society, data protection is of great importance for states, organizations, and individual users alike. As a result of the rapid development of information technologies in the 21st century, the global economy and public administration have been integrated into the digital environment. The widespread adoption of the Internet, along with the use of cloud technologies, artificial intelligence, and big data, plays a significant role in the operations of states. At the same time, the digital environment also gives rise to new security risks.

Cybersecurity issues are among the most significant challenges facing states in the modern era. Attacks on the information systems of government agencies, data theft, and interference with the operation of critical infrastructure pose a serious threat to society. For this reason, states implement various strategies to protect their information space and ensure their independence in the digital environment. It is precisely in this context that the concept of digital sovereignty has emerged. This concept entails states exercising control over their digital resources and ensuring their security. Digital sovereignty encompasses not only technical issues but also legal, political, and economic aspects. In modern times, many states pay special attention to the issue of digital sovereignty in their national cybersecurity strategies. The development of local technologies, the protection of national databases, and the training of cybersecurity specialists are among the key measures being implemented in this field.

2. Relevance of the topic

The acceleration of the digitalization process and the widespread adoption of internet technologies have made the issue of cybersecurity even more pressing. Cyber threats pose a serious risk because government institutions, banking systems, energy infrastructure, and other strategic sectors rely on digital systems. For this reason, the issue of digital sovereignty occupies a significant place in the security policies of states. Protecting information resources and ensuring independence in the digital environment is one of the key priorities for states in the modern era.

3. The aim of the study

The main objective of this study is to examine the role of digital sovereignty in the national cybersecurity system and to analyze the existing challenges in this field. The objectives of the study are as follows:

- to define the essence of the concept of digital sovereignty;
- to examine its role in the national cybersecurity system;
- to analyze the strategies implemented by states in this area;

4. Object of the study

The object of the study is the role of digital sovereignty in ensuring national cybersecurity and its impact on the state's information security. In the study, the digital infrastructure, information systems, databases, and cybersecurity strategies of states were taken as the primary objects of research. In this context, cyber threats emerging in the digital environment, data protection mechanisms, and measures implemented by states to ensure digital sovereignty have been examined. Issues regarding the protection of national information resources and the enhancement of technological independence are also included in the main scope of the research.

5. Novelty of the research

The scientific novelty of the research lies in the comprehensive analysis of the concept of digital sovereignty within the context of national cybersecurity. The study systematically examines the impact of digital sovereignty on state security, its formation mechanisms, and the challenges arising in the modern era. Furthermore, a comparative analysis of the cybersecurity strategies of various countries was conducted, and modern approaches implemented to ensure digital sovereignty were identified. This approach has enabled a broader and more up-to-date exploration of the topic.

6. Practical significance of the research

The results of the research are of practical importance for the development of the national cybersecurity system and the strengthening of digital sovereignty. The research findings may be useful for government agencies, organizations operating in the information technology sector, and cybersecurity specialists. Furthermore, the research findings can be used in the educational process within the fields of information security and cybersecurity. These materials can help students in higher education institutions acquire broader and more systematic knowledge of the subject.

7. Materials and discussions.

Digital sovereignty is considered one of the key principles in ensuring national cybersecurity. This concept entails state control over digital infrastructure, databases, and communication systems. Many countries are paying special attention to the development of domestic software and hardware to reduce dependence on foreign technologies. This both increases economic independence and reduces cybersecurity risks. Excessive reliance on foreign platforms and technologies can negatively affect the information security of states. The following areas are of great importance for ensuring digital sovereignty. Furthermore, the recommendations put forward in the article can support the development of practical measures aimed at enhancing security in the digital environment and protecting national information resources.

Development of national information infrastructure- States ensure that data is stored within the country by developing their own data centers and server systems. Formulation of a cybersecurity strategy. National cybersecurity strategies aim to ensure the information security of government agencies and the private sector. Data protection and privacy assurance. Specific legislative and technical mechanisms are implemented to protect personal data. Training cybersecurity specialists. Training information security specialists in educational institutions plays a crucial role in strengthening digital sovereignty. Discussions indicate that digital sovereignty is not merely a technological issue but also a crucial aspect of state policy. The measures implemented by states in this area enhance their resilience against cyber threats [3].

8. Research method

Various scientific methods were used during the research process. Methods of comparative analysis, analysis of scientific literature, and an analytical approach were primarily employed. To investigate the topic, reports from international organizations, scientific articles, and studies on information security were

examined. Furthermore, the cybersecurity strategies of various states were compared, and the measures taken to ensure digital sovereignty were analyzed. Through an analytical method, the role of digital sovereignty within the national security system has been determined, and existing problems in this area have been examined [4], [5].

9.Result

Research shows that digital sovereignty is one of the key elements of national cybersecurity in the modern era. Protecting the information resources of states and ensuring the security of their digital infrastructures play a crucial role in safeguarding national interests. The development of local technologies, the formulation of cybersecurity strategies, and the training of specialists are of great importance for strengthening digital sovereignty. These measures enhance the resilience of states against cyber threats and ensure their independence in the digital environment. In conclusion, it can be said that digital sovereignty is not merely a technological issue but also one of the strategic aspects of state security.

Author Contributions

The sole author is responsible for conceptualizing, collecting, and analyzing data, and writing and editing the manuscript

Conflict of Interest

The authors declare no conflicts of interest

Funding

This study received no external funding

References

- [1] Anisimov, A. A. (2009). *Menedzhment v sfere informatsionnoy bezopasnosti* Internet-Universitet Informatsionnykh Tekhnologiy; BINOM. Лаборатория знаний.
- [2] Singer, P. W., & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know®*. Oxford University Press.
<https://doi.org/10.1093/wentk/9780199918096.001.0001>
- [3] Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. Ecco.
- [4] Yusupov, R. M., & Shishkin, V. M. (2013). Informatsionnaya bezopasnost i kiberbezopasnost: Semanticheskiy konflikt ili sosushchestvovanie. *Informatizatsiya i svyaz*, (6), 22–27.
- [5] Shishkin, V. M. (2011). Pokazateli nadyozhnosti i bezopasnosti: Vozmozhnosti nelineynogo perekhoda. *Trudy Mezhdunarodnogo simpoziuma "Nadezhnost i kachestvo"*, 1, 101–103.