The Importance of National Operating Systems in Ensuring Information Security

Kamran Z. Huseynov

Azerbaijan Technical University, Baku AZ1073, Azerbaijan
kmrnhsynov@gmail.com

Abstract. In the context of escalating cyber threats, information security issues are becoming a priority for all nations. The use of foreign operating systems carries several serious risks. Dependence on foreign developers and update providers, the possibility of external interference in critical information processes, the potential presence of undeclared tools and vendor capabilities that could harm the user country, hidden vulnerabilities, and similar threats are just some of these risks. These factors threaten the digital sovereignty and stability of national infrastructure. Modern cybersecurity challenges require the development and implementation of national operating systems capable of ensuring reliable information security and state digital sovereignty. National operating systems are a strategic tool for creating a reliable software and hardware environment that complies with national standards and regulatory requirements. Their implementation ensures the protection of important information systems, government agencies, and military, civilian, and corporate infrastructure. National operating systems play a key role in ensuring national information security, encompassing both the public and private sectors of digital infrastructure.

This study highlights the role of national operating systems in enhancing resilience to external cyberattacks and developing the local technological base. Attention is paid to the study of cybersecurity standards, a review of international experience, and their application in local conditions. It also examines the prospects for integrating national operating systems into Azerbaijan's digital ecosystem, their importance for strengthening the state's cyber resilience, and increasing competitiveness in the global digital economy.

Keywords: National Operating Systems, Information Security, Digital Sovereignty.

1 Introduction

Growing cyber threats and sanctions have elevated the importance of digital sovereignty and independence in information security. Developing national operating systems is a crucial element in maintaining control over software infrastructure and safeguarding critical data. To effectively mitigate cybersecurity threats and ensure rapid response capabilities including preemptive measures, military and government auto-

R. Rzayev et al. (eds.), *Proceedings of the International Conference on Current Problems in Engineering and Applied Sciences (ICCPEAS 2025)*, Advances in Engineering Research 299,
https://doi.org/10.2991/978-94-6239-668-5_95

mated systems must undergo improved automation and secure development. It is critical to revise the foundational principles of military and government systems to guarantee cybersecurity during both peacetime and wartime. Establishing a robust cybersecurity framework requires deploying hardware and software platforms within a trusted environment. Trust in this context implies guaranteed adherence to stringent information security, reliability, and functional stability requirements amidst modern information warfare, alongside maintaining technological independence. A trusted hardware and software environment encompasses the technical tools, software, and organizational measures necessary to securely create, utilize, and develop special-purpose systems.

1.1 Problem Statement

Despite the rapid development of information technology, most government and corporate structures remain dependent on foreign operating systems and software. This dependence creates risks of unauthorized access, data leakage, and the violation of technological independence.

The problem lies in the lack of a stable ecosystem of national operating systems capable of ensuring a high level of information security, compatibility with existing solutions, and a trusted execution environment. Therefore, an analysis of the role of national operating systems as a tool for ensuring digital sovereignty and protecting critical information infrastructure is required.

2 Risks of Dependence on Foreign Operating Systems

Despite the absence of physical borders in cyberspace, countries develop cybersecurity strategies independently, based on their own understanding of security, resulting in significant differences between them. When developing a national cybersecurity strategy, complex questions arise regarding its content, objectives, and implementation methods.

Dependence on foreign operating systems carries several serious risks that directly impact national security and the state's digital sovereignty. First and foremost, such dependence limits technological oversight, as most foreign operating systems are closed source, preventing a full security audit and the identification of potentially dangerous functions. A state or organization is forced to rely on updates and technical support from a foreign supplier, which can stop providing them at any time or restrict access for political reasons. This creates a threat of cyberespionage, as the presence of undeclared capabilities (so-called backdoor mechanisms) or hidden data transmission channels can allow external actors to obtain confidential information. Additional risks are associated with the possibility of remote interference in the operation of systems, which is especially dangerous for critical infrastructure facilities such as energy, defense, and transportation [1].

There are also legal and sanctions risks: in the event of international conflicts, a country may lose access to licenses, updates, or cloud services, which would destabilize government and corporate systems. Furthermore, the use of foreign operating systems

leads to a drain on financial resources abroad in the form of license fees and technical support, reducing incentives for the development of the national IT industry. All of this undermines digital sovereignty, limiting the state's ability to control its own information space and ensure cyber resilience in the face of global threats.

In the US, for example, we see that the government is incapable of ensuring cyber-security on its own and requires the active participation of the private sector. A balanced regulatory model is needed, one in which businesses are required to comply with security standards but also supported by incentives and protection from excessive costs. The current situation has been characterized as a "market failure in cyber-security," as a laissez-faire approach is ineffective against large-scale threats. The proposed solution is to strengthen cooperation between the government and private companies, introduce uniform standards and mandatory requirements for data protection, and promote the use of open-source software in critical systems [2].

2.1 National OS as an Information Security Tool

The role of the information component in the national security system increased significantly in the early 20th century, and this process continues today. The rapid development and widespread adoption of modern information technologies is occurring not only in national security but also in related fields that are fundamental to ensuring the security of a modern state.

The information component is particularly important in national security, and its role in this process will continue to increase, at least in the medium term. A significant portion of national security forces is also focused on solving strategic tasks directly or indirectly related to information security. A corresponding policy is implemented to manage and coordinate the actions of these forces and the use of these resources in the information domain.

National operating systems have quite logical and understandable tasks: the ability to monitor end users, the ability to guarantee the absence of backdoors at the software level, the ability to enforce various laws and detect crimes, as well as several other similar tasks related to state control. It would probably be logical for all government agencies to operate exclusively on domestic operating systems and components. However, this requires that these components be competitive with other developments. This requires a certain amount of experience and significant, even enormous, funding.

The use of national operating systems allows for independent source code review, the identification and elimination of vulnerabilities, and the implementation of proprietary security mechanisms and cryptographic algorithms that comply with national security standards. Furthermore, national operating systems facilitate the creation of a unified, trusted digital space where data security, information integrity, and access control are implemented at a level determined by state requirements. This is particularly important for protecting government agencies, defense structures, the banking sector, and strategic enterprises, where a breach of information security could lead to serious political and economic consequences [3].

From a digital sovereignty perspective, national operating systems allow the state to independently manage the lifecycle of software solutions—from development and updates to certification and maintenance. This eliminates external influence on data processing and increases resilience to sanctions, technological, and cyber threats. The development and implementation of national operating systems also stimulate the growth of the domestic IT industry, promotes the development of scientific and engineering competencies, and strengthens the state's independence in the strategically important field of information technology. Thus, national operating systems are not simply software products, but an element of national security and the foundation for the formation of a sovereign digital ecosystem.

3 International Cybersecurity Standards and Strategies

International cybersecurity standards and strategies play a key role in developing a unified approach to information security and the resilience of digital infrastructure. They serve as the basis for developing national policies and regulations aimed at mitigating the risks of cyberattacks, protecting personal data, and ensuring the continuity of critical systems. To enhance effectiveness, it is necessary to consider the recommendations of international organizations, which help develop common approaches and values, ensuring alignment of national strategies with global cybersecurity principles. Among the most recognized international standards are the ISO/IEC 27000 family of standards, which regulates information security management systems, the NIST Cybersecurity Framework developed in the United States, and the ENISA Guidelines used in the European Union [4]. These documents define the fundamental principles of cybersecurity, including risk assessment, incident management, access control, encryption, auditing, and user awareness.

International organizations such as the UN, ITU, OECD, and ENISA actively promote the development of global norms and the exchange of experience in cybersecurity. Their recommendations facilitate the development of coordinated approaches to regulating the digital environment and building trust between countries. At the same time, each country adapts these standards to its own national interests, level of technological development, and threat landscape. For Azerbaijan, the application of international cybersecurity standards is particularly important: it facilitates integration into the global digital space, enhances the protection of national infrastructure, and ensures interoperability with international partners. Thus, international cybersecurity standards and strategies provide the foundation for the development of an effective, resilient, and trusted digital ecosystem capable of countering modern cyberthreats [5].

An analysis of international experience in legal support for information security shows that approximately 100 countries have adopted laws on the right to information. Of interest to our country is the European Union's experience in creating a system of legal regulation for telecommunications and information protection. Within this system, a set of relevant legal acts aimed at ensuring information security has been adopted. In particular, the concept of network and information security was introduced, the conceptual framework for European policy on its implementation was formulated,

and the European Commission Directives on privacy and electronic communications and on data protection were adopted.

To ensure Azerbaijan's digital transformation, improve public administration, digitalize the economy, and enhance the quality of life of its citizens, the Republic of Azerbaijan adopted the Digital Development Concept in 2025. Although not explicitly stated in the document, the need for a national operating system is indirectly expressed. In the coming years, plans are underway to consolidate the information systems of government agencies onto a single platform, create a reliable hardware and software environment within government information systems, and ensure software certification in accordance with national standards.

It's difficult to predict whether an operating system will appear in Azerbaijan in the coming years. It's possible to create another clone based on an open-source distribution, such as Linux Ubuntu but creating a full-fledged infrastructure with various network services, including integration with the mobile version of the operating system, and regular support is another matter entirely. This requires widespread implementation, staff training, and a host of other unobvious costs. This is precisely what Azerbaijan is doing with its development and implementation of its digital government strategy.

4 Conclusions

National operating systems play a key role in ensuring information security and strengthening the state's digital sovereignty. They serve as a strategic tool for protecting critical infrastructure, government, and corporate information systems, as they minimize dependence on foreign developers and ensure complete control over the internal processes of the software environment. In recent years, there has been a significant increase in the number and complexity of cyber threats, requiring enhanced protection of digital infrastructure and information systems. Improving security is possible through carefully configuring system parameters and implementing optimal protection measures. In response to these growing risks, international and national organizations have developed several cybersecurity standards defining the basic principles and requirements for information protection. Global cybersecurity experience demonstrates the need to create a comprehensive system that combines organizational, operational, and technical security measures with modern forecasting, analysis, and situation modeling methods.

Disclosure of Interests. The author have no competing interests to declare that are relevant to the content of this article.

References

1. Karpiuk, M.: Organization of the National System of Cybersecurity: Selected Issues. Studia Iuridica Lublinensia 30(2), 233–244 (2021)
2. Etzioni, A.: Cybersecurity in the private sector. Issues in Science and Technology 28(1), 58–62 (2011)

3. Amanowicz, M.: Towards building national cybersecurity awareness. International Journal of Electronics and Telecommunications 66(2), 321–326 (2020)
4. Kovacs, L.: National cyber security as the cornerstone of national security. Land Forces Academy Review 23(2), 113–120 (2018)
5. Hamdani, S.W.A., Abbas, H., Janjua, A.R., Shahid, W.B., Amjad, M.F., Khan, A.W.: Cybersecurity standards in the context of operating system: Practical aspects, analysis, ans comparisons. ACM Computing Surveys (CSUR) 54(3), 1–36 (2021)