Cybersecurity Education in Albania and the Development of a Supportive Training Platform

Klevisa SULA[1]

Agim KASAJ

Abstract

At a time when cybersecurity represents one of the greatest challenges for organizations, public and private institutions in Albania still face a lack of awareness and the necessary knowledge to protect sensitive systems and data. Cyberattacks have become a serious threat to the stability and security of institutions. Malicious actors increasingly employ advanced techniques to infiltrate information systems, aiming to steal data, disrupt services, or manipulate information. Ransomware, phishing, network attacks, and threats to critical infrastructure are among the most common forms of these challenges. The scale and complexity of cyberattacks have grown significantly, placing organizations in a reality where security is no longer optional but a necessity.

In addition to external threats, organizations also face internal risks related to the lack of proper knowledge and security practices. The absence of structured training, incident response protocols, and clear risk management policies makes it

[1] Klevisa Sula has completed her Bachelor studies in *Computer Engineering* with a specialization in *Software Development* at the European University of Tirana. She continued her academic journey at the same institution, earning a Master of Science degree in *Computer Engineering* with a specialization in *Information Systems Security*. Her research interests focus on cybersecurity, secure system design, and the development of educational platforms aimed at raising awareness and strengthening defensive skills in information security.

even more difficult to confront such attacks. In Albania, these problems are further emphasized due to limited institutional awareness and the lack of a well-established cybersecurity culture. This situation requires immediate intervention to build a sustainable foundation of knowledge and defensive capabilities.

The primary objective of this thesis is to identify these challenges and develop an educational mechanism to address them. As part of this goal, an interactive platform called Albania Cyber Learning System has been developed, offering both theoretical and practical content on cybersecurity. The platform is designed to enhance the knowledge and defensive skills of employees across various institutions, representing an important step toward building a sustainable and inclusive cybersecurity culture in Albania.

Keywords: *Cybersecurity, Albania, awareness, cyber threats, education platform, resilience.*

Introduction

In recent years, cyberattacks have become more frequent and sophisticated, creating serious risks for organizations of all sizes. While technological defenses are advancing, employees often remain the most vulnerable point in the security chain. Many lack the knowledge and practical skills necessary to recognize and respond effectively to phishing, ransomware, and other threats. This situation highlights the urgent need for new approaches to cybersecurity education that go beyond static lectures and provide more interactive and practical learning experiences.

This research introduces the *Albania Cyber Learning System*, an interactive platform designed to improve knowledge, awareness, and defensive skills in cybersecurity. The platform combines theoretical content, practical simulations, and self-assessment tests, allowing users to learn progressively and measure their progress through certification. It is designed to be accessible, sustainable, and adaptable, providing a foundation for building a stronger cybersecurity culture in Albania.

The study is guided by four research questions:

First research question

How can the level of employee knowledge about cybersecurity concepts and practices be improved in Albania?

This question addresses the knowledge gap that exists among employees, who often represent the weakest link in digital defense. It investigates how structured

and interactive training modules can strengthen their understanding of cyber threats and provide them with the necessary skills to protect organizational systems and data.

Second research question

How does an interactive learning platform influence the awareness of cybersecurity in Albanian organizations?

Awareness is a critical element of effective cybersecurity. This question examines how interactive learning, simulations, and gamified experiences can raise awareness and ensure that employees become more vigilant, proactive, and responsible in their daily use of digital tools.

Third research question

What training formats are most effective in improving user responses to cyber threats? Different training formats—ranging from theoretical lectures to practice-based simulations—have varying levels of effectiveness. This question seeks to identify which approaches produce the best outcomes in terms of user readiness, enabling them to detect, report, and respond effectively to cyber incidents.

Fourth research question

How can an educational platform be designed to remain sustainable, accessible, and adaptable for teaching cybersecurity in institutions?

Beyond content, the long-term impact of such a system depends on its design. This question focuses on how the platform can be developed to ensure scalability, cost-effectiveness, and adaptability to the needs of different institutions, making it a reliable tool for continuous learning in cybersecurity.

Hypothesis

> The use of an educational platform for cybersecurity will positively influence the improvement of knowledge, defensive skills, and awareness of employees and organizations in Albania.

By providing interactive and structured training, the platform is expected to bridge existing knowledge gaps, enhance proactive responses to threats, and foster a stronger cybersecurity culture.

In order to validate this hypothesis, the research is guided by several key objectives:

- To identify the current limitations of traditional training methods that rely on static lectures and lack practical engagement.
- To design and implement an interactive platform that combines theoretical modules, practical simulations, and self-assessment tools to improve learning outcomes.
- To evaluate the effectiveness of different training formats in enhancing user preparedness and response to cyber threats.
- To determine how the platform can be made sustainable, accessible, and adaptable for the long-term needs of Albanian institutions.

Literature Review

The growing importance of cybersecurity education has been emphasized across both academic and professional contexts. As digital infrastructures expand, organizations increasingly depend on effective training to protect against cyber threats. Traditional training methods, however, often rely on static lectures and theoretical content, which fail to equip users with practical skills or adaptive responses to evolving attacks.

Research in cybersecurity awareness highlights the role of interactive and experiential learning in shaping user behavior. Studies suggest that training formats that incorporate simulations, case studies, and gamification are more effective than conventional approaches. These methods not only improve knowledge retention but also foster active engagement, which is crucial in ensuring that employees can apply concepts in real-world scenarios.

Another recurring theme in the literature is the centrality of user awareness. While technical defenses are necessary, human error remains one of the leading causes of successful cyberattacks. Awareness programs that emphasize phishing recognition, safe browsing practices, and incident reporting have proven to reduce risks significantly. However, the challenge lies in sustaining awareness over time, which requires platforms that provide continuous, adaptive learning rather than one-time workshops.

Several international frameworks and best practices stress the importance of integrating cybersecurity education into organizational culture. Approaches such as the NIST Cybersecurity Framework and other global initiatives encourage not only compliance but also ongoing development of digital resilience. Despite these advancements, gaps remain in adapting these strategies to local contexts such as Albania, where structured and scalable platforms are still limited.

This literature review indicates that while progress has been made in cybersecurity training globally, there is a clear need for innovative, sustainable, and localized solutions. Interactive platforms that combine theory with practice stand out as promising tools to address this gap, offering a foundation for building a stronger cybersecurity culture.

Methodology and Technology Used

The *Albania Cyber Learning System* was developed following a structured approach inspired by the Software Development Life Cycle (SDLC), ensuring that the process evolved in well-defined phases: planning, analysis, design, implementation, testing, and maintenance. This methodological framework provided clarity in managing requirements, consistency in development, and flexibility in adapting to feedback. By applying SDLC, each critical aspect of the system, particularly user interaction, content delivery, assessment mechanisms, and security, was systematically addressed to guarantee both reliability and scalability.

FIGURE 1. User interface of the Albania Cyber Learning System (Dashboard view)

FIGURE 2. Example of training module in the Albania Cyber Learning System

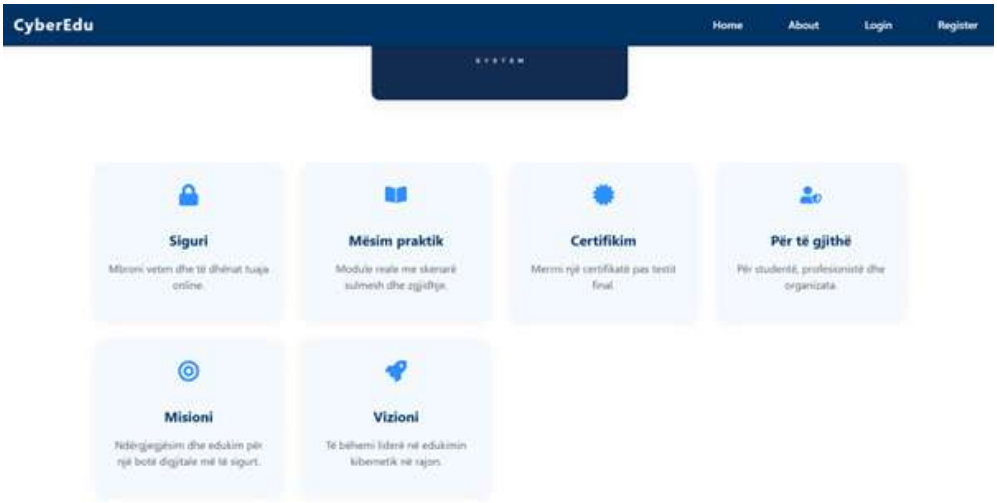
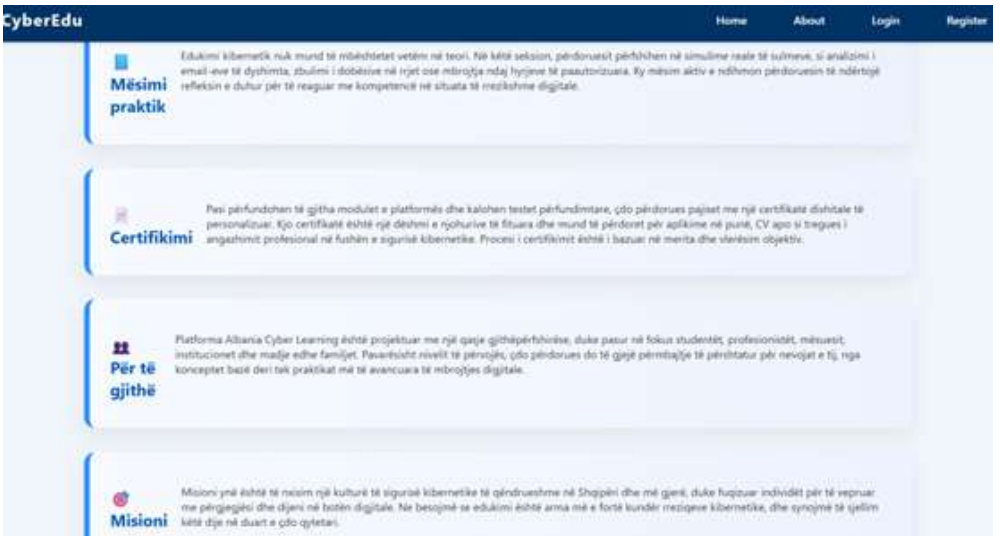


FIGURE 3. Example of training module in the Albania Cyber Learning System (homepage section and introduction of cybersecurity education).

FIGURE 4. Functional components of the Albania Cyber Learning System (training modules, certification, inclusiveness, and mission).



Frontend Development with ReactJS

The user interface of the platform was implemented using ReactJS, a widely adopted JavaScript library chosen for its modular structure and dynamic rendering capabilities. React allowed the development of an intuitive and responsive interface where users could easily navigate training modules, attempt quizzes, and visualize their progress. Its component-based architecture provided flexibility, enabling the reuse of UI elements across different modules, while its virtual DOM ensured fast updates and seamless user interactions. The focus on simplicity and usability aimed to minimize technical barriers and enhance engagement for both technical and non-technical learners.

Backend Development with Node.js and Express

The application logic and server-side functionalities were developed with Node.js and Express. Node.js was selected due to its non-blocking, event-driven architecture, which enables high performance and scalability for handling concurrent user requests. Express provided a lightweight and robust framework for building RESTful APIs that connected the frontend with backend services. Through this layer, the platform manages authentication, role-based access control, progress tracking, and secure communication between the client and server. By adopting industry standards in coding and modular design, the backend ensured reliability and maintainability.

Database Management with MongoDB

For persistent data storage, the platform integrated MongoDB, a NoSQL document-oriented database known for its scalability and flexibility. MongoDB was used to store user profiles, progress data, test results, and certificate records. Its schema-less structure allowed for the efficient handling of diverse data types, supporting quick updates and scalability as the platform grows. The database was designed to ensure secure data handling, incorporating encryption methods and access controls to protect sensitive user information.

Security Measures and Encryption

Given the platform's focus on cybersecurity, strong security mechanisms were integrated into its design. Passwords were stored using hashing algorithms to prevent unauthorized access, while communication between client and server was protected with HTTPS and token-based authentication. Sensitive user data and test results were handled with confidentiality and integrity principles, aligned with best practices for cybersecurity education platforms.

Training Module Design

The platform was structured into ten progressive training modules, covering both fundamental and advanced cybersecurity concepts. Modules included topics such as phishing, ransomware, malware, DDoS, social engineering, and secure data management. Each module combined theoretical explanations with interactive exercises and practical simulations of real-world attack scenarios. To reinforce learning, self-assessment quizzes were embedded, while progress tracking mechanisms provided users with continuous feedback. Successful completion of all modules allowed learners to earn a personalized certificate, validating their knowledge and skills. By combining a rigorous methodological framework with modern web technologies, the *Albania Cyber Learning System* delivers a sustainable and scalable solution for cybersecurity education, bridging theoretical knowledge with practical skill development.

Methods and Analysis

The development of the *Albania Cyber Learning System* followed a modular approach, combining best practices in web application design with a strong focus on cybersecurity education. The platform was structured into key layers, frontend, backend, and database, each contributing to functionality, usability, and security.

System Architecture

The platform is based on a modern client–server architecture, with a clear separation between the frontend and backend components. The frontend, developed in **React.js**, provides users with a responsive and intuitive interface for accessing training modules, completing quizzes, and tracking progress. The backend, built with **Node.js** and **Express**, handles application logic, authentication, and communication with the database. Data is stored in **MongoDB**, which allows for flexible management of user information, test results, and certification records.

Authentication and Security

User authentication was implemented using **JSON Web Tokens (JWT)** to ensure secure session management. For higher-privileged accounts such as administrators and instructors, **two-factor authentication (2FA)** was integrated to provide an additional security layer. Sensitive data was encrypted, and all communication between client and server was protected with **HTTPS**, following best practices for secure online learning systems.

FIGURE 5. User login interface in the Albania Cyber Learning System

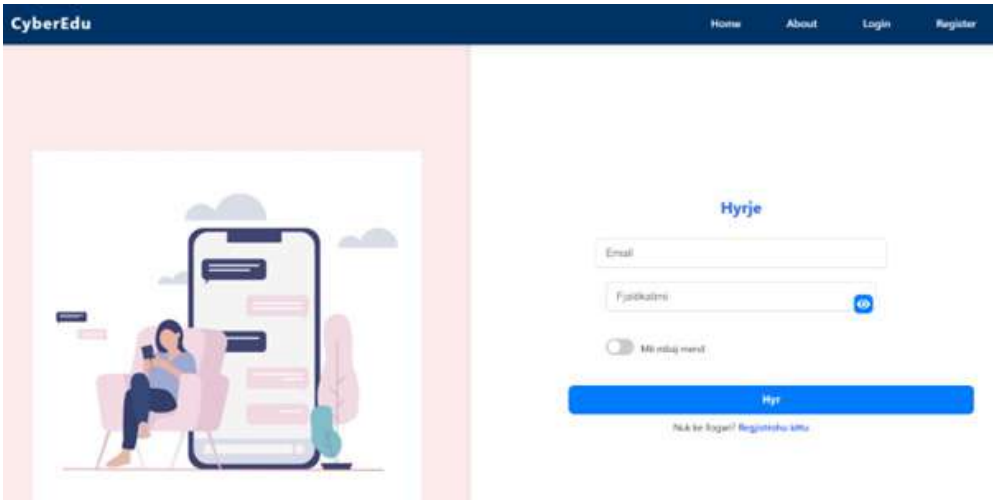


FIGURE 6. Two-factor authentication (2FA) in the Albania Cyber Learning System

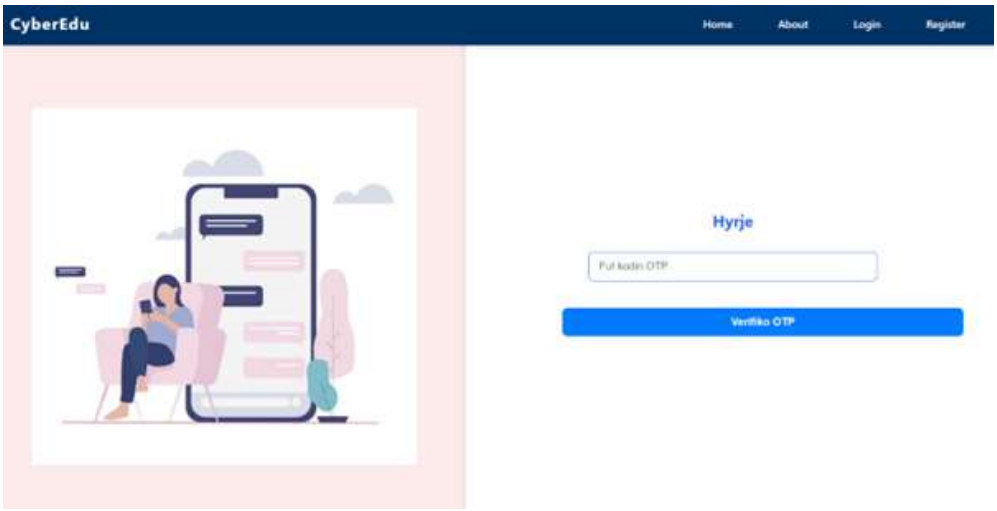


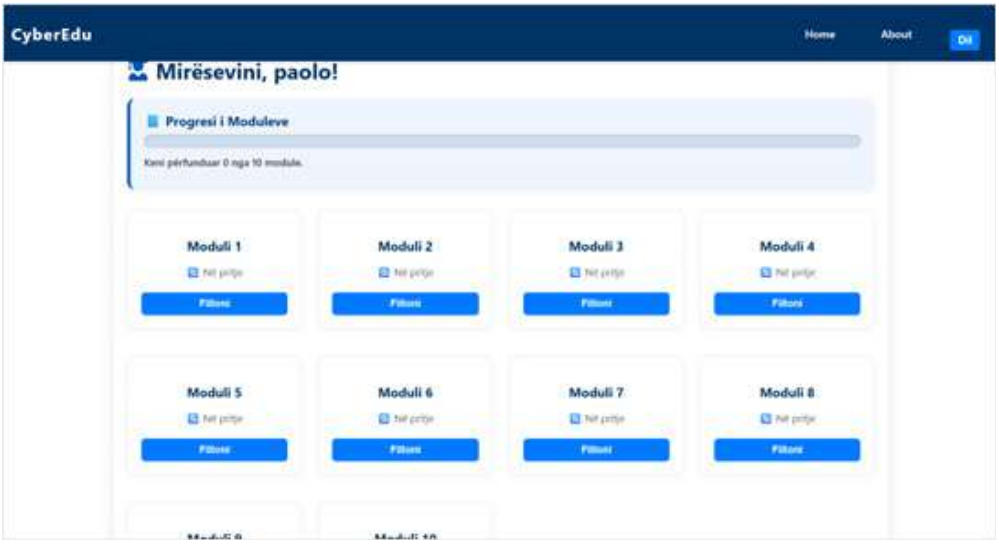
FIGURE 7. Email service for OTP verification in the Albania Cyber Learning System.

```
backend > utils > JS emailService.js > ...
1   const nodemailer = require("nodemailer");
2
3   const transporter = nodemailer.createTransport({
4     service: "gmail",
5     auth: {
6       user: process.env.EMAIL_USER,
7       pass: process.env.EMAIL_PASS,
8     },
9   });
10
11  const sendOTP = async (to, otp) => {
12    const mailOptions = {
13      from: process.env.EMAIL_USER,
14      to,
15      subject: "Kodi juaj i verifikimit",
16      text: `Kodi juaj për verifikim është: ${otp}`,
17    };
18
19    await transporter.sendMail(mailOptions);
20  };
21
22  module.exports = { sendOTP };
23
```

Training Modules

The system consists of **ten training modules**, structured around core cybersecurity principles and common threats. Topics include confidentiality and secure password practices, phishing and malware recognition, social engineering, ransomware defense, backup strategies, and safe data management. Each module contains theoretical explanations, illustrations, and an interactive quiz. Immediate feedback is provided after each test, reinforcing user understanding and allowing learners to identify and correct mistakes.

FIGURE 8. Dashboard view of the Albania Cyber Learning System.



Progress Tracking and Motivation

To ensure continuity in learning, the platform was designed to track user progress automatically. Successful completion of one module is required to unlock the next. A personal dashboard provides users with an overview of their completed modules, test results, and overall progress. Motivation is further enhanced by the issuance of a personalized digital certificate upon completion of all modules and the final test, downloadable in PDF format.

FIGURE 9. Module progress tracking in the Albania Cyber Learning System

FIGURE 10. Completion status of all training modules in the Albania Cyber Learning System

Administration and Audit

Administrators are provided with a dedicated panel to monitor user activity, progress, and results. The system also supports auditing functionalities, enabling the tracking of platform usage and detection of potential misuse. This feature ensures accountability and strengthens the overall security of the platform.

FIGURE 11. Administrator dashboard for monitoring user progress and certificate status

FIGURE 12. Administrator interface for adding and managing training modules

Technical Implementation

The platform integrates several components to achieve functionality:

Backend APIs manage registration, login, progress tracking, and certification.
Progress Controller stores completed modules, final test results, and activates certification eligibility.
AuthMiddleware validates JWTs and protects private routes, ensuring only authenticated users can access sensitive data.
Dashboard Component dynamically displays progress, percentage completion, and certificate availability.
Certificate Component generates downloadable PDF certificates using **jsPDF** and **html2canvas**, providing tangible recognition of user achievements.

This modular design allowed the system to remain scalable, secure, and user-friendly. By combining technical implementation with pedagogical strategies, the *Albania Cyber Learning System* ensures that learners not only acquire theoretical knowledge but also develop practical defensive skills against real-world cyber threats.

Conclusions

In the current digital era, cybersecurity has become one of the most pressing challenges facing individuals, organizations, and governments alike. The rapid adoption of digital systems in Albania has expanded opportunities for efficiency and growth, but it has also exposed institutions to a wide range of cyber threats. These threats include phishing, ransomware, malware, denial-of-service attacks, and social engineering, which are becoming increasingly sophisticated. Against this background, cybersecurity education can no longer be considered optional. It is an urgent necessity for building resilience, protecting sensitive data, and ensuring the sustainability of digital transformation.

The primary objective of this research was to design and implement a practical educational platform that directly addresses the gaps in cybersecurity awareness and training in Albania. The result of this effort was the development of the *Albania Cyber Learning System (ACLS)*, an integrated e-learning solution that combines theoretical modules, quizzes, simulations, progress tracking, and certification. This platform was developed to be inclusive and accessible, designed not only for IT professionals but also for employees, students, and individuals with limited technical knowledge. A central contribution of this research lies in its ability to combine international best practices with the realities of the local context. By analyzing successful models such as Cyber Aware (UK), the NIST

NICE Framework (USA), and CSA initiatives in Singapore, the project integrated their strengths while adapting them to the specific needs of Albanian organizations and users. In doing so, ACLS becomes not just a technical product, but also an educational intervention with potential to influence behavior and strengthen cybersecurity culture nationally.

The conclusions of the study can be discussed in direct response to the four research questions:

> RQ1: How can the level of employee knowledge about cybersecurity concepts and practices be effectively improved in Albania?

The findings highlight that the limitations of current training in Albania do not lie only in the amount of content delivered, but in the lack of personalization, engagement, and performance measurement. Traditional workshops or yearly awareness sessions are insufficient because they rely on static lectures and standardized materials that fail to influence user behavior. The ACLS addresses this challenge by offering structured modules, immediate feedback after quizzes, and practical exercises that replicate real-world scenarios such as phishing emails or ransomware infections. This approach ensures that employees do not simply consume information passively but engage with it actively, building long-term knowledge and defensive habits.

> RQ2: How does an interactive learning platform influence the level of awareness of cybersecurity in Albanian organizations?

The implementation of ACLS demonstrates that interactive platforms provide a measurable advantage over passive training methods. Features such as gamification, dynamic testing, and personalized dashboards increase motivation and retention. In pilot evaluations with academic staff and IT specialists, the platform showed clear improvements in users' ability to identify suspicious emails, recognize unsafe behaviors, and implement stronger password practices. This confirms that awareness is more effectively built when learners are engaged in active participation rather than exposed to static information. Moreover, the availability of a digital certificate at the end of the program provides an additional motivational factor, giving users tangible recognition of their efforts.

> RQ3: What training formats are most effective in improving user responses to cyber threats?

The analysis reveals that interactive and experiential learning formats are significantly more effective than traditional lecture-based models. By combining short, focused lessons with quizzes and simulations, ACLS ensures that users

test their understanding in real time. Mistakes are immediately corrected, and knowledge is reinforced through repetition. This cycle of learning and assessment prepares users to respond more effectively when faced with actual threats. In particular, simulations of phishing attacks and social engineering scenarios proved to be highly impactful, as they replicated the situations users are most likely to encounter in their daily work. These findings align with international literature that emphasizes experiential learning as the key to building resilience against human-centered cyber risks.

> RQ4.How can an educational platform be designed to remain sustainable, accessible, and adaptable for teaching cybersecurity in institutions?

The sustainability of ACLS lies in its modular design and technical architecture. By building the platform on widely used technologies such as ReactJS, Node.js, and MongoDB, the system remains scalable, easy to maintain, and adaptable for future needs. Accessibility was also a priority: the interface is designed to be simple, clear, and understandable even for non-technical users. Looking forward, the platform can be extended with advanced features such as artificial intelligence for adaptive testing, multilingual support, and mobile applications. These improvements will ensure long-term relevance and usability, allowing the system to serve diverse institutions—from public administration to private businesses and educational environments.

Beyond answering the research questions, this project contributes to the broader objective of building a sustainable cybersecurity culture in Albania. Cybersecurity is not only a technical challenge but also a human and organizational one. Since the majority of successful attacks exploit human error, education and repeated awareness are among the most powerful defenses available. ACLS was designed with this principle in mind: cybersecurity education is not a one-time process but a continuous cycle of training, reinforcement, and adaptation to new threats.

Another significant conclusion is the importance of personalization. Generic training materials are less effective because they do not reflect the real responsibilities and risks of specific user groups. ACLS addresses this by enabling role-based customization, ensuring that the content is relevant and meaningful for each type of user. This approach increases motivation, engagement, and knowledge retention, making the platform not just informative but transformative.

Finally, ACLS represents a starting point rather than a finished product. While the current version already provides a functional and effective system, future developments are envisioned to enhance its scope and impact. These include:

- Adaptive testing with AI, adjusting difficulty based on user performance.
- Advanced gamification, including badges, levels, and leaderboards to increase motivation.

- Multilingual support for regional scalability.
- Mobile applications for flexible access.
- Administrative analytics dashboards for institutional oversight.
- Integration with educational systems in schools and universities.
- Internationally recognized certifications in collaboration with organizations such as ENISA or NIST.

In conclusion, the *Albania Cyber Learning System* represents a concrete step forward in addressing the pressing need for cybersecurity education in Albania. By combining theory with practice, interactivity with personalization, and local needs with international standards, the platform offers a model for sustainable, scalable, and effective training. With future enhancements, it has the potential to evolve into a regional leader in cybersecurity education, contributing not only to national resilience but also to global best practices.

Recommendations

Moving forward, several developments could further enhance the Albania Cyber Learning System (ACLS) platform:

Adaptive Testing with Artificial Intelligence: Implementing AI-driven adaptive assessments that adjust the difficulty of questions in real time based on user responses. This would ensure personalized evaluation, reduce uniformity, and improve the accuracy of measuring knowledge and skills.

Advanced Gamification: Beyond certificates, future versions could integrate motivational mechanisms such as badges, levels, and leaderboards. These elements would enhance learner engagement and encourage continuous participation.

Multilingual Support and Mobile Accessibility: Expanding the platform with multilingual options (English, Macedonian, Serbian, etc.) and developing a dedicated mobile application (Android/iOS) would increase accessibility and extend usage beyond linguistic and technological barriers.

Analytical Administrative Panel: Building an advanced analytics dashboard for administrators to monitor user progress, identify difficult modules, and analyze completion rates. Such tools would support informed decision-making and continuous improvement.

Notification and Reminder System: Introducing automated reminders for pending modules, new publications, or certificate availability would help maintain user engagement and reduce drop-out rates.

AI-driven Personalized Learning: Leveraging artificial intelligence to recommend tailored content and generate custom quizzes based on each user's risk profile and learning behavior, ensuring a more effective and individualized learning path.

Integration with Existing Educational Systems: Extending ACLS to function as an additional module for schools, universities, or professional training institutions, with institution-specific login and reporting features.

Internationally Recognized Certifications: Partnering with ENISA, NIST, or other European and international organizations to issue certifications with high value in the labor market. This would transform ACLS into a hub for professional development with recognized credentials.

Bibliography

Agjencia Kombëtare e Shoqërisë së Informacionit. (2023). *Raporti vjetor për aktivitetin e sigurisë kibernetike në sektorin publik*. AKSHI.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Cyber Aware (UK). (2023). *Government campaign to help you stay secure online*. https://www.ncsc.gov.uk/cyberaware

Cybersecurity Agency of Singapore. (2023). *CSA Academy*. https://www.csa.gov.sg

ENISA. (2021). *Cybersecurity education and awareness guidelines*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

ENISA. (2023a). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA. (2023b). *Cybersecurity skills development in the EU*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/skills-and-competences

Federal Bureau of Investigation. (2023). *Internet Crime Complaint Center (IC3) annual report*. FBI.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. Wiley.

IBM Security. (2023). *X-Force threat intelligence index 2023*. https://www.ibm.com/think/x-force/2023-x-force-threat-intelligence-index-report

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems — Requirements*. ISO.

Jansson, K., & Von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology, 32*(6), 584–593.

Kaspersky. (2023). *The state of supply chain security*. Kaspersky Research.

KnowBe4. (2022). *Security awareness training report*. https://www.knowbe4.com

Këshilli i Ministrave. (2020). *Strategjia kombëtare e sigurisë kibernetike 2020–2025*. Qeveria e Shqipërisë.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). The effect of experience on security behaviours and knowledge. *Computers & Security, 70*, 663–674.

Organisation for Economic Co-operation and Development. (2022). *Policy framework for cybersecurity skills*. OECD Publishing. https://www.oecd.org/en/publications/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c.html

Saini, M., Rao, S., & Panda, T. (2019). *Cybersecurity awareness and training: Challenges and opportunities*. Springer.

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security, 119*, 102756. https://doi.org/10.1016/j.cose.2022.102756

van Steen, T., & Deeleman, J. R. A. (2021). Successful gamification of cybersecurity training. *Cyberpsychology, Behavior, and Social Networking, 24*(9), 593–598. https://doi.org/10.1089/cyber.2020.0526

Verizon. (2023). *Data breach investigations report 2023*. https://www.verizon.com/business/resources/reports/dbir/

World Economic Forum. (2022). *Global cybersecurity outlook 2022*. WEF.

Yamin, M. M., & Katt, B. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security, 88*, 101636. https://doi.org/10.1016/j.cose.2019.101636