SCIENCE SET
OPEN ACCESS PUBLISHERS

Research Article

World Journal of Sensors Network Research

Cybersecurity and Privacy Concerns in Digital Governance in Albania

Shqipe Xhaferri[1], Blerim Brahja[2*], Era Tiço[3], Marlind Nuriu[4], & Amina Nuriu[5]

[1]*Aleksandër Moisiu", University of Durrës, Albania*
[2]*Student "Aleksandër Moisiu", University of Durrës, Albania*
[3]*Student at Metropolitan University of Tirana, Albania*
[4]*Ministry of Finance, Tirana, Albania*
[5]*Klo-nu" Tirana, Albania*

[*]**Corresponding author:** Blerim Brahja, Student Aleksandër Moisiu, University of Durrës, Albania.

Submitted: 24 November 2024 **Accepted:** 04 November 2024 **Published:** 22 November 2024

Citation: *Haferri, S., Brahja, B., Tiço, E., Nuriu, M., & Nuriu, A. (2024). Cybersecurity and Privacy Concerns in Digital Governance in Albania. Wor Jour of Sens Net Res, 1(1), 01-05.*

Abstract

Although smart governance is starting to appear in underdeveloped nations, there are serious privacy and cybersecurity concerns that need to be addressed. This has the potential to revolutionize government operations. A study was carried out to pinpoint particular cybersecurity and privacy issues in the context of smart governance in developing nations. The results show that since smart governance systems rely on a lot of personal data that could be exploited for things like profiling or monitoring, data collecting and storage are significant privacy concerns. Developing nations might not have the means or expertise to put robust cybersecurity safeguards in place, making them open to cyberattacks. Third-party contractors may have laxer cybersecurity policies, and trusted insiders may abuse their access credentials, adding to the risk to government networks. Cybercrime poses a serious risk, and political attacks could target intelligent governance systems, jeopardizing their integrity and undermining public confidence in governmental institutions. The study's conclusions emphasize how crucial it is to address cybersecurity and privacy issues while creating intelligent governance systems in underdeveloped nations. Enacting strict data protection legislation, funding cybersecurity infrastructure, and giving government workers priority cybersecurity awareness and training are all imperative.

Albanian citizens suffered from cyberattacks more than once where most of their private data from the official government app "E-Albania" was leaked. In addition, there should be regular risk assessments, audits, and the establishment of explicit protocols and procedures for handling cybersecurity issues. In order to strengthen cybersecurity skills and effectively counter cyber threats, international collaboration and information exchange might also be beneficial.

Introduction: *Sh.XH. contributed to defining the overall scope of the study by identifying the key cybersecurity and privacy challenges within the Albanian digital governance context. Sh.XH. led the framing of the research question, drawing from the national case of Albania and emphasizing the importance of international best practices in securing government networks.*

Literature Review: *A. N. conducted an extensive review of prior research on smart governance and cybersecurity threats, particularly in developing countries. She. identified key works by West (2005), Heeks (2006), and Kshetri (2010), and contextualized them within the Albanian landscape. A.N. provided critical insights into how the findings of previous research could inform current efforts to enhance Albania's cybersecurity infrastructure.*

Methodology and Data: *B.B. designed and executed the data collection methods. He conducted quantitative analysis of cybersecurity breaches in Albania and the broader Balkans, analyzing statistical trends in attacks, particularly post-2020. B.B. also ensured that the data gathered from respondents were anonymized and ethically handled.*

Research Results and Comments: *M. M. interpreted the research results, analyzing the trends and patterns emerging from the data. He provided key insights into the relationship between insider threats and the vulnerabilities of Albanian digital governance systems. M.M. also led the discussion on the implications of these findings, particularly focusing on the increased attacks on Credins Bank and other private sector targets.*

Conclusion and Recommendations: *E.T. synthesized the findings into actionable recommendations for policymakers. She drafted the final policy recommendations, advocating for stronger legal frameworks, improved digital literacy programs, and phased implementation of smart governance systems. E.T. also emphasized the need for Albania to collaborate with international cybersecurity bodies and integrate two-factor authentication for sensitive government services. The team collaborated on the final editing and approved the version for publication.*

JEL Classification: *H83, K24, L86, O33, O38*

Keywords: Cybersecurity Concerns, Data Collection, Data Security, Albania, Privacy Concerns, Smart Governance

Introduction

A new era of interconnectedness and efficiency in government operations has been ushered in by the digital age. The benefits of technology improvements include seamless communication, easily available information, and streamlined services. But this advancement comes at a cost: a greater susceptibility to attackers. Malicious actors frequently target governments because they own a lot of sensitive data and are looking to steal it, profit from it, or jeopardize vital infrastructure. This study examines the privacy and cybersecurity issues related to digital governance in Albania, emphasizing particular difficulties and possible solutions. The study underscores the necessity for continuous vigilance and adaptation in government cybersecurity strategies. By acknowledging the challenges, understanding the motivations of attackers, and implementing robust security measures, governments can safeguard sensitive data, protect critical infrastructure, and maintain public trust.

Literature Review

Information and communication technologies (ICTs) are being used as part of the shift to smart governance to increase the effectiveness, responsiveness, and transparency of public services. However, there are also a lot of privacy and cybersecurity dangers associated with the integration of these technologies. Prior research has demonstrated that substantial privacy issues may arise when smart governance systems rely heavily on personal data (West, 2005; Heeks, 2006). Practices for gathering and storing data must be closely monitored to avoid abuse and unauthorized access. These problems are made worse in developing countries by a lack of resources and knowledge necessary to put strong cybersecurity measures in place (Souter, 2010).

The risk to government networks is increased by trusted insiders abusing their access credentials and third-party contractors with inadequate cybersecurity practices (Kshetri, 2010). According to Bishop and Gates (2008), there is an increasing risk to the integrity of intelligent governance systems due to cybercrime and political threats, which also erode public confidence in governmental institutions.

A cyber expert named Genti Progni filed accusations against the organizations in charge of preventing these types of attacks due to the recurrent cyberattacks and the government's alleged lackluster reaction. A group of about 800 IT specialists support Progni's position. He wants to increase awareness and hold responsible parties responsible for safeguarding personal information.

Progni emphasized the serious dangers that come with identity theft and improper use of internet information, including the pilfering of social media accounts like Facebook and Instagram. Thousands of worried people wrote to him asking for legal action, which suggested that anxiety was common among the population.

Methodology and Data

For this study, a mixed-methods strategy was used, integrating qualitative and quantitative data collection techniques. Surveys and interviews with government representatives, cybersecurity professionals, and individuals impacted by cyberattacks were used to collect primary data. We gathered secondary data from government reports, cybersecurity publications, and scholarly journals. By examining the frequency and kind of cyberattacks against government targets, the threat's extent was determined. The reasons for these attacks were investigated, and particular occurrences in Albania were looked at to comprehend the background there. Potential solutions based on best practices and international standards were put forth, along with an identification of the difficulties the Albanian government had in putting strong cybersecurity measures in place.

Research Results and Comments

Since 2001, the number of people who have fallen victim to cyberattacks has shockingly increased by 16 times. The problem was made worse by the COVID-19 pandemic, which led to a 125% rise in cyberattacks globally until 2021. Government organizations are now major targets for cybercriminals, with a 95% increase in attacks between 2021 and 2022, according to CloudSEK XVigil study. These attacks can take many different forms, including as physical loss or theft of unsecured devices storing sensitive data, social engineering, and system invasions.

It's interesting to note that 85% of these breaches come from inside the company, underscoring the significance of taking a multifaceted strategy to cybersecurity. The primary drivers of cyberattacks on governments include espionage, financial gain, and ideological goals. Financially driven cybercriminals usually target government agencies in an attempt to pilfer money or extract ransomware payments. Foreign organizations looking to steal classified material pertaining to national security also find governments to be attractive targets. Even though they are less common, some attacks could be motivated by ideologies that seek to divide people or obstruct government operations.

Albania and Cyberattacks - Albania has experienced significant cyberattacks, notably severing diplomatic ties with Iran after suspecting them as the culprit. An intense hack that was thought to be retaliation for Albania's protection of an Iranian opposition group set off this historic action. Albania is a target for both Russia and Iran due to its affiliation with the US and its harboring of Afghan refugees and Iranian dissidents. While this has improved efficiency, the quick digitization of Albanian government services has also revealed serious security flaws.

After concentrating on state institutions, the Iranian-backed hacker group Homeland Justice turned its attention on Albania's private bank, Credins Bank, in January 2023. The hackers leaked the data of business clients and general account holders, causing widespread concern among the bank's customers. This incident marked a new front in the cyberattacks, expanding the threat from public to private entities.

Cybersecurity's Economic Impact Breaches in Digital Governance - There are numerous financial repercussions from cybersecurity breaches in Albania. A 2023 World Economic Forum study found that cyberattacks can result in large financial losses, including direct expenses like fines, lost productivity, and the price of fixing security breaches. By decreasing foreign investment and raising the price of cybersecurity insurance, security breaches indirectly undermine public confidence in government systems, which can hinder economic growth. For example, companies reported a significant drop in user confidence after the "E-Albania" platform hack, which decreased the uptake of digital services and raised transaction costs. Furthermore, OECD research from 2023 demonstrate that nations with lax digital security policies typically have slower rates of economic growth since both home and international businesses are reluctant to engage in a dangerous digital environment. The escalating expense of cybersecurity infrastructure, personnel training, and data recovery places a significant financial strain on both public and commercial organizations, making the investment in strong cyber defenses not merely technically necessary but also economically critical.

Legal and Social Repercussions - The NATO member state was rocked by a series of cyberattacks in the middle of 2022 that targeted official institutions and resulted in the online disclosure of thousands of people's personal information. The attack on Credins Bank added to the growing worry among Albanians regarding the protection of their personal information. The public's worry has not decreased despite attempts by authorities to regulate the situation, such as forbidding media outlets from reporting on the contents of the leaks.

A Severe Shortage of Cybersecurity Professionals - The scarcity of workers in cybersecurity has reached a critical point as cyber dangers continue to grow. The number of open cybersecurity jobs worldwide is currently close to 4 million, even with a 10% rise in employment last year. According to ISC2's most recent Cybersecurity Workforce Study, the workforce gap has grown by 12.6% year over year, which highlights the concerning trend and the growing need for skilled cybersecurity workers.

According to two-thirds of cybersecurity experts, their companies don't have enough employees to properly detect and resolve security problems. Organizations' ability to maintain strong cybersecurity defenses is fundamentally challenged by this gap, which is made worse by economic uncertainty, budget cuts, and hiring freezes. The lack of skills is especially harmful when it comes to crucial fields like machine learning, artificial intelligence, cloud computing security, and zero-trust architecture implementation. A startling 92% of businesses report having a skills gap in critical cybersecurity knowledge.

What Companies Are Doing to Combat Cybersecurity Threats - Given these labor shortages, a lot of businesses are being proactive in strengthening their cybersecurity. With the right instruction and training, cybersecurity hazards can be avoided and mitigated. Employers are using webinars and other training resources more frequently to educate staff members on cybersecurity best practices and procedures.

In addition, businesses are implementing new technologies and routinely auditing their security protocols to find weaknesses in their systems. Using seasoned cybersecurity experts or consultants has also grown to be a standard tactic for strengthening defenses and making sure businesses are ready to deal with new threats in an efficient manner. Organizations may enhance their ability to tackle the increasing variety of cybersecurity risks in 2024 and beyond by giving priority to education, technology adoption, and qualified workforce.

Types of Cybersecurity Threats - As digital landscapes evolve, so do the types of cyber threats that target them. These threats can be broadly categorized into several types, each with unique characteristics and methodologies:

- Malware continues to be prevalent, encompassing various forms such as viruses, ransomware and spyware. These malicious programs can disrupt operations, steal information or damage systems.
- Social engineering exploits human interactions to gain unauthorized access to valuable information and systems. Phishing, one of the most common forms, tricks users into divulging sensitive data.
- Insider threats arise from within an organization and can be accidental or malicious. These threats are particularly insidious as they bypass traditional security measures with legitimate access.
- Advanced persistent threats (APTs) are complex, stealthy and prolonged attacks aimed at specific targets to steal data or disrupt operations, often undetected for long periods.

- Distributed denial of service (DDoS) attacks overload systems with floods of internet traffic. These attacks disrupt services and can serve as a smokescreen for more invasive attacks.
- Ransomware attacks involve encrypting the victim's data and demanding payment for decryption keys. These attacks can paralyze critical systems and demand significant financial payouts.
- Man-in-the-middle (MitM) attacks intercept communications between two parties to steal or manipulate information.
- Supply chain attacks compromise software or hardware before they reach the consumer, exploiting trusted relationships.

Challenges and Solutions for Robust Government Cybersecurity - To address these challenges, the Albanian government must adopt a holistic approach to cybersecurity. This includes: Implementing Strict Cybersecurity Regulations: Developing and enforcing comprehensive cybersecurity policies that address specific risks and outline best practices for mitigation. Modernizing IT Infrastructure: Upgrading outdated computer systems with modern technology and security measures to enhance defenses against cyber threats.

Investing in Cybersecurity Awareness Training: Educating Government Employees on Cyber Hazards

- **Conducting Regular Risk Assessments and Audits:** Routine evaluations of cybersecurity measures are essential to identify and address vulnerabilities promptly. Regular audits ensure compliance with established standards and detect potential threats before they can cause significant damage. Enhancing Legal Frameworks: Strengthening data protection legislation to ensure strict penalties for data breaches and unauthorized access. This includes developing laws that support collective action or class-action lawsuits, allowing citizens to seek remedy collectively. Stablishing Explicit Protocols and Procedures: Creating clear guidelines for handling cybersecurity incidents, including immediate response measures, communication strategies, and recovery plans. These protocols ensure a swift and coordinated response to cyberattacks, minimizing their impact.
- **Promoting International Collaboration:** Engaging in international cooperation and information exchange to bolster cybersecurity capabilities. Partnerships with other nations and international organizations can provide access to advanced technologies, expertise, and intelligence on emerging threats. Phased Implementation of Digital Services: Gradually introducing digital governance initiatives to allow for proper testing and adjustment. This approach ensures that potential issues are identified and addressed before a full-scale rollout, reducing the risk of widespread cyberattacks.
- **Improving Public Education and Digital Literacy:** Implementing programs to enhance digital literacy among citizens, especially older populations, ensures that everyone can safely and effectively use online services. This includes educating the public on recognizing phishing attempts and other cyber threats. Providing Alternatives to Digital Services: Offering both paper-based and digital solutions ensures inclusivity and respects personal preferences. Citizens who are uncomfortable with digital services should have the option to use traditional methods, preventing exclusion and reducing anxiety over data security.
- **Implementing Strong Authentication Mechanisms:** Utilizing two-factor authentication (2FA) and other advanced security measures to protect sensitive accounts and systems. This adds an extra layer of security, making it more difficult for unauthorized individuals to gain access.
- **Changing Unique Personal ID Numbers:** Considering the renewal of citizens' ID numbers to mitigate the risk of identity theft. While complex, this measure can significantly reduce the impact of previous data breaches.

Conclusion

The digital landscape is constantly evolving, and so must government cybersecurity strategies. By acknowledging the challenges, understanding the motivations of attackers, and implementing robust security measures, governments can safeguard sensitive data, protect critical infrastructure, and maintain the public trust essential for a well-functioning democracy. Continuous vigilance and adaptation are key to ensuring a secure digital future for governance.

Albania is making a sincere effort to transition to a more modern system by pushing for digital government. However, significant challenges remain in the transition to the digital era. Although digitization offers convenience and efficiency, a large portion of Albania's population is older and may find it difficult to use internet resources. Implementing this plan hastily and lacking adequate preparation leaves the system vulnerable to possible cyberattacks. People who are wary of digital services now face an unfair scenario since they could not have a choice in how their information is handled.

Phased implementation holds the key to a solution. Better public education and adaptation, including senior digital literacy initiatives, would be possible with this phased implementation. Investing in strong cybersecurity defenses is also essential to safeguarding private information kept online. Lastly, providing residents with an option between paper-based and digital solutions guarantees inclusion and honors personal preferences. Albania can guarantee the long-term viability of its digital governance system while providing advantages to all residents by addressing these issues. The following recommendations are proposed to enhance cybersecurity and privacy in Albania: Develop Comprehensive Cybersecurity Policies: The Albanian government should draft and enforce detailed cybersecurity regulations that address specific risks and outline best practices. These policies should be regularly updated to keep pace with evolving threats.

- **Invest in Modernizing IT Infrastructure:** Upgrading legacy systems is crucial to defend against modern cyber threats. This includes investing in new technologies and ensuring that all systems are equipped with the latest security features. Enhance Cybersecurity Awareness Training: Government employees must be trained regularly on cybersecurity best practices and the latest threats. This reduces the likelihood of human error and ensures a proactive approach to data security.

- **Promote International Cooperation:** Collaborating with other countries and international organizations can enhance Albania's cybersecurity capabilities. Sharing information and strategies can help prevent and respond to cyber threats more effectively. Conduct Regular Risk Assessments and Audits: Routine evaluations of cybersecurity measures and compliance with standards are essential. These assessments help identify vulnerabilities and ensure that they are addressed promptly.
- **Improve Public Education and Digital Literacy:** Implementing programs to educate the public, especially older populations, on digital literacy and cybersecurity can help mitigate the risks associated with digital governance. This includes awareness campaigns on recognizing phishing attempts and protecting personal information online.
- **Provide Alternatives to Digital Services:** Offering both digital and traditional paper-based services ensure that all citizens can access government services without compromising their security or comfort.
- **Implement Strong Authentication Mechanisms:** Utilizing advanced security measures, such as two-factor authentication, can significantly enhance the protection of sensitive accounts and systems. Consider Changing Unique Personal ID Numbers: While complex, renewing citizens' ID numbers may be necessary to address the risks posed by previous data breaches.
- **Strengthen Legal Frameworks:** Developing laws that support collective action or class-action lawsuits can empower citizens to seek remedy collectively. This provides a stronger legal recourse for those affected by cyberattacks.

References

1. Center for Strategic and International Studies (CSIS). (2024). Cybersecurity and governance. Retrieved from https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/cybersecurity
2. Fjori Sinoruka. (2023). Albanians mull options as data security takes new hit. Retrieved from https://balkaninsight.com/2023/01/25/albanians-mull-options-as-data-security-takes-new-hit/
3. James B. D. Joshi. (2003). Security and privacy challenges of a digital government. Retrieved from https://www.researchgate.net/publication/2480339_Security_and_Privacy_Challenges_of_a_Digital_Government
4. Keane, J. (2023). Digital democracy: Declining trust and rising risks in the network society.
5. Libicki, M. C. (2023). The age of cybersecurity.
6. Michelle Moore. (2022). Top cyber security threats. Retrieved from https://onlinedegrees.sandiego.edu/top-cyber-security-threats/
7. Mohammad J Sear. (2023). Digital government cyber security issues in 2023. Retrieved from https://www.linkedin.com/pulse/digital-government-cyber-security-issues-2023-mohammad-j-sear/