


UDC: 32.; 323.

LBC: 63.3(2)6-6; 63.3 (2)64; 63.3(5 e)64

MJ № 422

 10.33864/2617-751X.2025.v8.i8.497-506

ENHANCING MEDIA SECURITY: THE ROLE OF CYBERSECURITY AND DATA ANALYSIS IN PROTECTING DIGITAL CONTENT

Vafa Isgandarova*

Said Isgandarli**

Abstract. In today's digital era, the majority of information have been releasing via digital tools as well as online sites. Media outlets face increasing threats to their digital content and infrastructure from various organizations and communities. These grown threats are related to the risks of cyberattacks, data breaches, and unauthorized access. Protecting digital content is no longer just about securing files; it requires a strategic combination of cybersecurity measures and advanced data analysis. This article is about the main cyber-attacks to media companies and the role of data analysis in protecting local digital content, generally enhancing media security.

Keywords: media, content, cyber, digital, security, data

* Doctor of Philosophy in Philology,

Baku State University, Faculty of Journalism, International journalism and information policy department; Baku, Azerbaijan

E-mail: vafal.aslan@gmail.com

<https://orcid.org/0000-0002-4167-7531>

** Fourth-year student at BAU's Faculty of Business Administration; Istanbul, Turkiye

E-mail: saidiskenderli777@gmail.com

<https://orcid.org/0009-0002-1909-3756>

To cite this article: Isgandarova, V., & Isgandarli, S. [2025]. ENHANCING MEDIA SECURITY: THE ROLE OF CYBERSECURITY AND DATA ANALYSIS IN PROTECTING DIGITAL CONTENT. "Metafizika" journal, 8(8), pp.497-506.

<https://doi.org/10.33864/2617-751X.2025.v8.i8.497-506>

Article history:

Received: 09.10.2025

Accepted: 13.11.2025

Published: 01.12.2025




Copyright: © 2025 by AcademyGate Publishing. This article is an open access article distributed under the terms and conditions of the CC BY-NC 4.0. For details on this license, please visit

<https://creativecommons.org/licenses/by-nc/4.0/>.

УДК: 32.; 323.

ББК: 63.3(2)6-6; 63.3 (2)64; 63.3(5 е)64

МЖ № 422

 10.33864/2617-751X.2025.v8.i8.497-506

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ МЕДИА: РОЛЬ КИБЕРБЕЗОПАСНОСТИ И АНАЛИЗА ДАННЫХ В ЗАЩИТЕ ЦИФРОВОГО КОНТЕНТА

Вафа Искендерова*

Саид Искендерли**

Абстракт. В современную цифровую эпоху большая часть информации распространяется через цифровые инструменты и онлайн-площадки. Средства массовой информации сталкиваются с растущими угрозами своему цифровому контенту и инфраструктуре со стороны различных организаций и сообществ. Эти возросшие угрозы связаны с рисками кибератак, утечек данных и несанкционированного доступа. Защита цифрового контента - это уже не просто обеспечение безопасности файлов; она требует стратегического сочетания мер кибербезопасности и углубленного анализа данных. В этой статье рассматриваются основные кибератаки на медиакomпании и роль анализа данных в защите локального цифрового контента, что в целом способствует повышению безопасности медиа.

Ключевые слова: медиа, контент, киберпространство, цифровые технологии, безопасность, данные

* Доктор философии по филологии,
Бакинский Государственный Университет; Баку, Азербайджан
E-mail: vafal.aslan@gmail.com
<https://orcid.org/0000-0002-4167-7531>

** Студент четвертого курса факультета делового администрирования ВАУ; Стамбул, Турция
E-mail: saidiskenderli777@gmail.com
<https://orcid.org/0009-0002-1909-3756>

Цитировать статью: Искендерова, В., & Искендерли, С. [2025]. ПОВЫШЕНИЕ БЕЗОПАСНОСТИ МЕДИА: РОЛЬ КИБЕРБЕЗОПАСНОСТИ И АНАЛИЗА ДАННЫХ В ЗАЩИТЕ ЦИФРОВОГО КОНТЕНТА. *Журнал «Metafizika»*, 8(8), с.497-506.
<https://doi.org/10.33864/2617-751X.2025.v8.i8.497-506>

История статьи:

Статья поступила в редакцию: 09.10.2025

Отправлена на доработку: 13.11.2025


Принята для печати: 01.12.2025



UOT: 32.; 323.

KBT: 63.3(2)6-6

MJ № 422

 10.33864/2617-751X.2025.v8.i8.497-506

MEDIA TƏHLÜKƏSİZLİYİNİN ARTIRILMASI: RƏQƏMSAL MƏZMUNUN QORUNMASINDA KİBERTƏHLÜKƏSİZLİK VƏ MƏLUMAT TƏHLİLİNİN ROLU

Vəfa İsgəndərova*

Səid İsgəndərli**

Abstrakt. Bugünkü rəqəmsal dövrdə məlumatların əksəriyyəti rəqəmsal alətlər, eləcə də onlayn saytlar vasitəsilə yayılır. Media orqanları rəqəmsal məzmunu və infrastrukturunu üçün müxtəlif təşkilatlar və icmalar tərəfindən artan təhlükələrlə üzləşirlər. Bu artan təhlükələr kiberhücumlar, məlumatların pozulması və icazəsiz giriş riskləri ilə bağlıdır. Rəqəmsal məzmunun qorunması artıq yalnız faylların təhlükəsizliyini təmin etmək deyil; kibertəhlükəsizlik tədbirlərinin və qabaqcıl məlumat təhlilinin strateji birləşməsini tələb edir. Bu məqalə media şirkətlərinə edilən əsas kiberhücumlardan və məlumatların təhlilinin yerli rəqəmsal məzmunun qorunmasında, ümumiyyətlə media təhlükəsizliyinin artırılmasında rolundan bəhs edir.

Açar sözlər: media, məzmun, kiber, rəqəmsal, təhlükəsizlik, verilənlər

* Filologiya üzrə fəlsəfə doktoru,

Bakı Dövlət Universiteti, Jurnalistika fakültəsi, Beynəlxalq jurnalistika və informasiya siyasəti kafedrası; Bakı, Azərbaycan

E-mail: vafal.aslan@gmail.com

<https://orcid.org/0000-0002-4167-7531>

** BAU-nun Biznesin idarə edilməsi fakültəsinin 4-cü kurs tələbəsi; İstanbul, Türkiyə

E-mail: saidiskenderli777@gmail.com

<https://orcid.org/0009-0002-1909-3756>

Məqaləyə istinad: İsgəndərova, V., & İsgəndərli, S. [2025]. MEDIA TƏHLÜKƏSİZLİYİNİN ARTIRILMASI: RƏQƏMSAL MƏZMUNUN QORUNMASINDA KİBERTƏHLÜKƏSİZLİK VƏ MƏLUMAT TƏHLİLİNİN ROLU. “Metafizika” jurnalı, 8(8), səh.497-506.

<https://doi.org/10.33864/2617-751X.2025.v8.i8.497-506>

Məqalənin tarixçəsi:

Məqalə redaksiyaya daxil olmuşdur: 09.10.2025

Təkrar işlənməyə göndərilmişdir: 13.11.2025

Çapa qəbul edilmişdir: 01.12.2025



Copyright: © 2025 by AcademyGate Publishing. This article is an open access article distributed under the terms and conditions of the CC BY-NC 4.0. For details on this license, please visit

<https://creativecommons.org/licenses/by-nc/4.0/>.

1.Introduction

With the continuing trend of more and more devices being connected to the Internet, the risk of exposure to some kind of cyber threat increases, even though digital skills of Internet users increase, and the number of Cyber security solutions is on the rise [9]. In the modern era the audience give preference to vast amounts of valuable digital content from media especially from social media in the form short news, story telling's, videos, reels and other creative types. Cybercriminals often target these assets for ransom, intellectual property theft, or to spread misinformation. Moreover, the rise of streaming services, social media, and digital publishing has expanded the attack surface, making it easier for malicious actors to exploit vulnerabilities. These malicious cyber attacks are sometimes used on a larger scale to weaken the political-ideological structures and financial support of states.

2.Methodology

The article includes a descriptive analysis of scientific sources on the topic, monitoring of media subjects. At the same time, an interview was conducted with a leading experts in the field of cyber security at one of the leading Internet media sites in Azerbaijan.

3.Literature review

The main researchers in this field are computer science specialists from technical universities, data institutions in various countries, information technology researchers from various think tanks, and public and private technology organizations. About the relationships between media and cybersecurity has been written by Myriam Dunn Caveley, called BookRoutledge Handbook of Media, Conflict and Security. Currently one of the major researchers in named area is Suresh Babu from Hindustan Institute of Technology and Science. He has written various articles such as "Principles and applications of adaptive artificial intelligence", "Adaptive AI for Dynamic Cybersecurity Systems: Enhancing Protection in a Rapidly Evolving Digital Landscape", "Revolutionizing conversational AI: unleashing the power of ChatGPT-Based applications in generative AI and natural language processing", "Cyber Physical Systems and Network Security: The Present Scenarios and Its Applications Evaluation and quality assurance for rapid e-learning and development of digital learning resources", "Cloud-Enabled Fire Safety in Industry", "Smart Factories: Leveraging IoT and Sensor Networks for Real-Time Monitoring and Proactive Prevention", "The future of cyber security starts today, not tomorrow" etc. Worldwide popular Stephan Miller has been written research about "Diving deep into data analytics and its importance in cybersecurity". About the role of Big Data and Data Science in the context of information security and cybersecurity wrote authors Dariusz Prokopowicz, Anna Gołębiowska, Małgorzata Such-Pyrgiel. Other authors

engaging with similar topic are Samar Hendawi, Shadi AIZu`bi, Ala Mughaid and Nayef Algahtani who researched "Ensuring Cybersecurity while Leveraging Social Media as a Data Source for Internet of Things Applications". Mohammed Khadar has written conference paper about Assessing the Effectiveness of Masking and Encryption in Safeguarding the Identity of social media publishers from advanced metadata analysis. Nir Kshetri researched blockchain's roles in strengthening cybersecurity and protecting privacy. About the digital information transparency for cyber security: Critical points in social media trends have been written by Miftachul Huda, Langgeng Sutopo, Liberty, Febrianto and Mazlina Che Mustafa. Naeem AllahRakha from Tashkent State University wrote research paper about "Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds". One of the vital topics in this sphere is related to data journalism. Danda B.Rawat, Ronald Doku and Moses Garuba researched "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security". And the research paper called "The Role of AI in Cyber Security: Safeguarding Digital Identity" has been written by collective authors from British University Dubai (Mohammad Binhammad, Shaikha Alqaydi, Azzam Othman, Laila Hatim Abuljadayel). In general, there is a large amount of literature and research on this topic in various countries, especially the USA, India and Arabian countries.

4. Conceptualization and main types of cyber attacks

The word 'security' is defined in the online version of the Oxford English Dictionary as "The state of being free from danger or threat" [Oxford University Press, 2015]. According to Morten Bay from UCLA Information Studies, the term is used to cover the measures government institutions take to protect the public and the institutions themselves from threats in the 'cyber'-domain, also known as 'cyberspace'. Yet it is also used on a level that is somewhat closer to the individual, when it refers to protection against viruses and other malware on a computer, whether this is personally owned or used in the work situation [3]. These threats are able to be made by the groups, individuals as well as by various criminal communities of other countries deliberately.

Here are some common widespread cyber threats and challenges undertaken by hackers and cyber criminals:

4.1. Malware

This is a computer program or a piece of code which is created to do harm to a computer, network as well as to a server. It is the most common type of cyberattack and encompasses many subsets, including ransomware, trojans, spyware, viruses, worms, and others.

4.2. Denial-of-service (DoS) attacks

This is a targeting attack which floods a network with false requests, disrupting business operations and leaving users unable to perform any tasks, accounts, or resources on a compromised computer or network.

4.3. Phishing attacks

A cyberattack which uses email, SMS, phone, social media, and social engineering techniques to trick a user into sharing sensitive information, such as passwords or account numbers, or to download a malicious file that will install a virus on their device.

4.4. Spoofing

Common spoofing attacks are domain spoofing, when an attacker impersonates a business or person with a fake website, and email spoofing, which uses forged sender addresses.

4.5. Internet of things (IoT) attacks

These attacks target an IoT device or network to take control of the device, steal data and digital assets, or join a group of infected devices together to launch a DoS attack. Examples of IoT devices include traditional endpoints such as computers, laptops, smartphones, and tablets, as well as nontraditional devices such as printers, cameras, appliances, smart watches, health trackers, navigation systems, and smart thermostats.

4.6. Artificial intelligence attacks

Artificial intelligence and machine learning is growing in ability and usage, so it's no surprise that cyber criminals have also begun to use it for their own personal gain. Attackers create fake chatbots or virtual assistants in AI-generated social engineering attacks, or carry out identity theft crimes by using deepfakes [4].

Data analysis is the process of inspecting, cleansing, transforming, and modeling data with the goal of discovering useful information, informing conclusions, and supporting decision-making. It involves applying statistical and logical techniques to describe, illustrate, condense, recap, and evaluate data.

In short, data analysis is the practice of working with data to glean useful information, which can then be used to make informed decisions [5] There are four types of data analysis: descriptive, diagnostic, predictive and prescriptive. Also, there are five steps of data analysis: Identify the question you'd like to answer; collect the raw data sets you'll need to help you answer the identified question; clean the data to prepare it for analysis; analyze the data and interpret the results of your analysis to see how well the data answered your original question [5].

5. The best practices for securing personal data online

Despite the wide range of cyber threats criminals are employing to steal personal data and information. This issue is mainly widespread related to

media outlets as well. Here is one of the major editing authorities of Azerbaijani internet media site Azxeber.com Gunel Huseynli's interview. Speaking about the main cyber threats encountered on social media resources in Azerbaijan, she stated that, cyberattacks on social media have always been presented. The majority of cyberattacks on social media occurred during the 44-day Patriotic War. During the war, there were attacks on our information portal as well as our social network accounts, which were prevented by our professional IT team. The enemy organized DoD Ddos attacks and sent massive traffic to our information portal and social network accounts to stop their activities. The cyberattacks were not limited to this. They created deepfake and fake content, damaged the reputation of our followers and caused the spread of false information. Commercial phishing attacks (i.e. phishing attacks) are widespread and their main goal is to deceive people and capture their personal and financial information (card numbers, passwords, logins, corporate information, etc.). These attacks are usually carried out through e-mail, SMS, social media, fake websites and even phone calls. Considering all this, we have called on our readers and followers not to click on fake and suspicious links and to be careful.

Regarding how to combat the aforementioned cyber threats, H.Gunel emphasized that, it is necessary to use spam and phishing filtering systems. In addition, in addition to using antivirus and security programs, it is necessary to use two-step authentication (2FA) - systems that require not only a password, but also additional confirmation (SMS code, application confirmation). What is more important is not to click on dangerous links and enter.

There are some best practices which everyone can use to help keep themselves safe online and to keep their devices` secure. Here are included:

- Strong passwords
- Regular software updates
- Secure network
- Secure Wi-Fi
- Data back-up
- Incident response plan
- Cyber security training [4]

6.Also there are a lot of cybersecurity tools for protecting our digital content

Mainly cybersecurity protocols such as encryption, multi-factor authentication, and secure access controls are essential to safeguard media content. Implementing robust firewall protections and intrusion detection systems helps prevent unauthorized access and mitigate the risk of attacks like Distributed Denial of Service (DDoS) or ransomware. Additionally, media companies must ensure regular software updates and security patches to close

vulnerabilities that hackers could exploit. Employee training on recognizing phishing attacks and social engineering tactics further strengthens defenses by reducing human error, often the weakest link in cybersecurity. Robust firewall protections and intrusion detection/prevention systems (IDS/IPS) help prevent unauthorized access and mitigate attacks like Distributed Denial of Service (DDoS) or ransomware. Recent years the majority of social media sector companies employ comprehensive firewall architectures and strict access controls to protect their content delivery network.

7.Leveraging Data Analysis to Strengthen Security

While traditional cybersecurity measures are vital, integrating data analysis elevates the ability to detect and respond to threats proactively. By collecting and analyzing network traffic, user behavior, and system logs, media organizations can identify unusual patterns indicative of cyber threats. Machine learning and artificial intelligence (AI) tools enhance this analysis by learning from historical attack data to predict and prevent future breaches. These technologies enable real-time threat detection, automated responses, and continuous monitoring, significantly reducing the time to respond to incidents.

8.Actionable Recommendations for Media Companies

1. Implement Multi-Layered Security Controls
2. Invest in Real-Time Data Analytics
3. Adopt Digital Rights Management (DRM) Solutions
4. Conduct Regular Security Audits and Penetration Testing
5. Train Employees Continuously
6. Collaborate Within the Industry
7. Ensure Regulatory Compliance

9.The future of media in terms of cyber security

Data protection can cost companies millions of dollars. The breach's consequences and repercussions are complex and long-term [2]. Cyber threats evolve continuously, with hackers deploying increasingly sophisticated methods like deepfakes, AI-powered phishing, and supply chain attacks. The media industry must adopt a multi-layered defense strategy that combines cybersecurity best practices with cutting-edge data analysis techniques.

As cyber threats evolve, the media industry must adopt a multi-layered defense strategy that combines cybersecurity best practices with cutting-edge data analysis techniques. Investing in AI-driven security tools, fostering cross-industry collaboration, and prioritizing user education will be crucial for media companies aiming to protect their digital assets effectively.

Investment in AI-driven security tools, fostering cross-industry collaboration (such as information sharing on emerging threats), and prioritizing ongoing user education will be crucial. Additionally, regulatory compliance, like GDPR

and CCPA, mandates stringent data protection measures, pushing media organizations to enhance their security postures further.

10. Conclusion

As digital media continues to dominate global communication and entertainment, the importance of securing digital content cannot be overstated. Cybersecurity alone is no longer sufficient to combat the sophisticated and ever-evolving nature of cyber threats targeting media organizations. By harnessing the power of data analysis, media companies can move from a reactive to a proactive security stance, identifying and neutralizing threats before significant damage occurs. The integration of cybersecurity with advanced analytics not only protects valuable digital assets but also helps maintain user trust, comply with regulations, and safeguard revenue streams in a fiercely competitive industry.

11. REFERENCES

1. Ghelani, D. (2025, September 5). Cyber security, cyber threats, implications and future perspectives: A review. *Authorea*. Retrieved from <https://www.authorea.com/doi/full/10.22541/au.166385207.73483369> (in English)
2. Bay, M. (2025, August 27). What is cybersecurity? In search of an encompassing definition for the post-Snowden era. *ResearchGate*. Retrieved from https://www.researchgate.net/profile/Morten-Bay/publication/308609163_WHAT_IS_CYBERSECURITY_In_search_of_an_encompassing_definition_for_the_post-Snowden_era/links/673666db69c07a411447404e/WHAT-IS-CYBERSECURITY-In-search-of-an-encompassing-definition-for-the-post-Snowden-era.pdf (in English)
3. City St. George's University of London. (2025, October 7). Cybersecurity: Protecting your data in the digital age. *City St. George's University of London*. Retrieved from <https://technology.online.city.ac.uk/blogs/cybersecurity-protecting-your-data-in-the-digital-age/> (in English)
4. Coursera Staff. (2024, October 15). What is data analysis? *Coursera*. Retrieved from <https://www.coursera.org/articles/what-is-data-analysis-with-examples> (in English)
5. Kapoor, M., Aggarwal, R., Madan, S. (2024). Cyber-Security: Critical Analysis on Attacks, Classification, and Issues. In: Hassanien, A.E., Anand, S., Jaiswal, A., Kumar, P. (eds) *Innovative Computing and Communications. ICICC 2024*. Lecture Notes in Networks and Systems, vol 1020. Springer, Singapore. https://doi.org/10.1007/978-981-97-3588-4_40 (in English)

6. Ahrend, J.M., Jirotko, M. (2017). *Anticipation in Cyber-Security*. In: Poli, R. (eds) *Handbook of Anticipation*. Springer, Cham. https://doi.org/10.1007/978-3-319-31737-3_26-1 (in English)
7. Jakimoski, K. (2023, September). Automation improvement in cyber risk management. *2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, 2023, pp. 1-6, <https://doi.org/10.23919/SoftCOM58365.2023.10271658> (in English)
8. Liu, X., Ahmad, S. F., Anser, M. K., Irshad, M., Ul-Haq, J., & Abbas, S. (2022, October 19). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*. Retrieved from <http://doi.org/10.3389/fpsyg.2022.927398> (in English)