Digital Transformation in University Libraries and Cybersecurity Challenges

Prepared by :

Dr. Abbes Fathi
Professor of Library and Information Science
Department of History, Mohamed Boudiaf University
, M'sila – Algeria
Personal Phone (WhatsApp): +213670382423
Email: Abbes.fathi@univ-msila.dz

Dr. Smail Radjai
Professor of Library and Information Science
Department of History, Mohamed Boudiaf University
, M'sila – Algeria
Personal Phone (WhatsApp): +213782982725
Email: smail.radjai@univ-msila.dz

Received: 11/01/2025 **Accepted: 10/04/2025** **Published: 20/05/2025**

Study Summary:

The university library sector is undergoing a rapid digital transformation aimed at improving access to educational and research resources while facilitating the management and organization of information. Digital transformation in university libraries is a fundamental step toward keeping pace with technological advancements in our era, including the use of digital library management systems, electronic databases, and artificial intelligence technologies to enhance user experience and improve academic services.

Despite the benefits of digital transformation in facilitating access to information, significant challenges arise, particularly in the field of cybersecurity. As university libraries transition to the digital environment, cybersecurity risks and threats, such as cyberattacks, breaches, and the theft of sensitive data, increase. Additionally, technical challenges such as difficulties in updating systems and protecting vast amounts of data pose significant risks to digital libraries. Furthermore, university library staff face human-related challenges, including limited awareness of cybersecurity importance and inadequate training on handling digital-age threats. Moreover, data protection regulations, such as the General Data Protection Regulation (GDPR), impose pressures on libraries to ensure full compliance.

To achieve and enhance cybersecurity in university libraries, comprehensive strategies must be implemented, including enforcing strict security policies such as encryption and developing multi-layered protection systems. It is also essential to train staff on security policies and utilize advanced technologies, such as artificial intelligence, to detect cyber threats at an early stage.

Keywords: Cybersecurity, University Libraries, Digital Transformation, Artificial Intelligence .

Introduction:

In recent decades, university libraries have undergone a radical transformation, evolving from traditional centers for printed books and resources into integrated digital platforms that offer a wide range of knowledge services. The concept of digital transformation has recently become associated with technological advancements and the developments in information and communication technologies. This new approach has led to significant changes in work fields and related patterns, raising service standards and highlighting the urgent need for institutions to adopt these technologies, which collectively represent digital transformation.

Digital transformation concerns the strategic use of technology within institutions, whether in the public or private sector, to enhance operational efficiency, improve services provided to clients and target audiences, support scientific research, and enable effective communication between researchers and students. It optimally employs technology to streamline workflows across all departments and facilitate interactions with users, ensuring better service delivery while saving time and effort simultaneously.

Throughout history, libraries have been the cornerstone of preserving and disseminating human knowledge. They began as repositories for books and manuscripts stored on traditional shelves, from the ancient Library of Alexandria to medieval libraries. With the advent of technology in the 20th century, libraries gradually transitioned to digitization. This digital transformation was not merely about converting books into electronic formats but also involved developing library management systems and digital catalogs, significantly improving information accessibility in both speed and efficiency.

Digitization is a crucial step in keeping pace with modern advancements. Libraries can now serve a much wider audience via the internet, providing round-the-clock access to educational and research resources from anywhere in the world. Technologies such as artificial intelligence and machine learning have further enabled libraries to analyze and understand user needs, enhancing personalized user experiences and making libraries more effective in meeting these demands.

The digital transformation extends beyond books and references to include images, maps, and historical manuscripts, granting newer generations access to knowledge treasures that were once confined within library walls. Additionally, libraries have enhanced their services through mobile applications and interactive websites, making information retrieval easier and faster. Libraries now play a crucial role in disseminating knowledge in ways that align with the digital age, offering online educational programs, hosting virtual seminars, and providing remote research support, thereby opening new horizons for learning and cultural interaction.

Moreover, these advancements have facilitated greater collaboration among libraries worldwide, allowing for easier resource and information sharing. This enriches global databases and provides researchers with access to diverse and reliable sources.

However, this digital transformation is accompanied by numerous challenges, most notably cybersecurity concerns. Cybersecurity is no longer a luxury or an option but a critical necessity for any country striving to safeguard its national security and stability. The rapid expansion of digital technology and its increasing reliance in all aspects of life have amplified the scale and complexity of cyber threats to an unprecedented degree. University libraries, as part of this digital ecosystem, have become prime targets for cyberattacks, which threaten data privacy, information integrity, and service continuity. This presents a significant dilemma for academic institutions, which must strike a balance between offering innovative digital services and ensuring the security of their sensitive data.

In this article, we explore the dimensions of digital transformation in university libraries, discuss the challenges related to cybersecurity, and present recommendations to enhance security strategies and protect digital resources.

Methodological Framework of the Study:

Research Problem:

With the rapid advancement of technology, university libraries are striving for digital transformation to enhance their services and meet the needs of the modern academic community. However, this shift presents a significant challenge in the form of cybersecurity. University libraries face increasing threats that endanger the security of sensitive data and information, whether related to users or digital academic resources.

The main research problem can be formulated as follows:

How can university libraries achieve comprehensive digital transformation while ensuring the protection of data and digital assets from cyber threats? What policies and strategies can balance technological innovation and information security in this context?

To address this central issue, the study seeks to answer the following sub-questions:

Sub-questions of the Study:

1. What is the concept of digital transformation, and how does it contribute to the development of university library services?
2. What are the key digital technologies used in university libraries to achieve digital transformation?
3. What challenges do university libraries face during the digital transformation process?
4. What is the concept of cybersecurity, and what is its significance in the digital library environment?
5. What are the most common cyber threats facing digital university libraries?
6. How can university libraries balance digital transformation with strengthening cybersecurity measures?
7. What strategies and policies can be proposed to enhance cybersecurity in digital university libraries?

Significance of the Study :

The significance of this study lies in highlighting the growing role of digital transformation in enhancing university library services. It contributes to improving access to academic information and resources while increasing the efficiency of internal operations. Moreover, the study emphasizes the importance of addressing security challenges associated with digital transformation, such as safeguarding sensitive data and securing the digital infrastructure of libraries.

This study holds great value for decision-makers in academic institutions and researchers in the fields of digital transformation and cybersecurity. It provides a comprehensive perspective on how to balance technological innovation with the protection of digital assets, ensuring the sustainability of university library services in a secure digital environment.

Objectives of the Study :

1. Explain the concept of digital transformation and its significance in enhancing university library performance.
2. Examine the key digital technologies used in university libraries to achieve digital transformation.
3. Identify the challenges university libraries face during the digital transformation process.
4. Explore the cybersecurity threats associated with digital transformation in university libraries.
5. Analyze the importance of cybersecurity in protecting digital university libraries.
6. Propose strategies to enhance cybersecurity in the context of university library digital transformation.
7. Provide recommendations for university decision-makers to develop policies that ensure secure digital transformation.

Previous Studies:

The digital transformation of university libraries and cybersecurity challenges are critical topics addressed by numerous academic studies. Below is an overview of some of these studies:

1. Cybersecurity Policies to Enhance Digital Transformation in Egyptian Universities: A Future Vision:

This study aimed to identify the challenges and obstacles facing the implementation of digitization in Egyptian universities and its negative impact on university administration priorities. The study highlighted that the most significant challenge for universities until 2035 is digitization and the ability to integrate technology extensively in education and university management.

2. The Role of Digital Transformation in Achieving Cybersecurity: An Applied Study on the Ministry of Justice in Qatar:

In this study, Mai Mohammed Hamad Abdullah Al Khalifa examined the impact of digital transformation on cybersecurity in government services. The findings indicated a significant effect of digital transformation on cybersecurity and emphasized the importance of government entities adhering to high-quality digital service standards and raising public awareness about these services.

3. Digital Transformation of National Institutions and Cybersecurity Challenges: Perspectives of Academic Police Officers in Kuwait :

This study, authored by Khaled Makhlaf Al-Janfaoui and published in 2021, focused on the digital transformation of national institutions and cybersecurity challenges in Kuwait from the perspective of academic police officers. The study recommended enhancing awareness and training in cybersecurity to keep pace with digital transformation.

4. The Necessity of Enhancing Cybersecurity Culture in the Digital Transformation Era: A Case Study of Prince Sattam bin Abdulaziz University:

Conducted by Alia Omar Kamel Faraj and published in 2022, this study aimed to highlight the need to enhance cybersecurity culture within digital transformation at Prince Sattam bin Abdulaziz University. It analyzed differences in respondents' perspectives based on variables such as faculty, specialization, and years of experience. The study concluded that enhancing cybersecurity culture at the university is driven by societal and cognitive factors.

5. Digital Transformation in Higher Education Institutions in the Arab World:

This study examined the challenges faced by higher education institutions in transitioning to remote learning during the pandemic. It provided several recommendations to improve and develop digital transformation in these institutions.

These studies underscore the importance of digital transformation in advancing university libraries and educational institutions while emphasizing the need to address cybersecurity challenges through effective policies and continuous awareness efforts.

Theoretical Framework of the Study:

1. Digital Transformation in University Libraries:

With the rapid advancement of modern technology, traditional libraries find themselves in urgent need of redefining their roles and functions to remain centers of knowledge and culture in the digital era. Libraries initially adapted their services with the emergence of Web 2.0, but the major leap in digital transformation occurred with the outbreak of the COVID-19 pandemic in 2019.

This crisis led to the complete shutdown of institutions worldwide, including libraries. To ensure continuity, it became necessary to shift towards digital and virtual services provided through online platforms and websites. The COVID-19 period witnessed widespread digital transformation in academic libraries, leading to the creation of new library functions and services based on advanced technologies. These include artificial intelligence (AI), Quick Response (QR) codes, self-service tools such as Library Kiosks, and Radio Frequency Identification (RFID) technology , among others. (**Keziz, 2024, p. 88**).

1.1. Definition of Digital Transformation in Academic Libraries:

Digital transformation refers to the process of changing work methods and practices in academic libraries through the use of digital technologies. This transformation also involves changes in organizational structure, operations, institutional culture, and relationships with clients and partners.

Some scholars view digital transformation as the comprehensive utilization of all available digital technologies to improve performance, increase productivity, and provide faster and better services to users (**Qasem AlJamal, 2023, p. 12**).

Digital transformation is not merely about digitizing library collections; rather, it is a comprehensive strategy aimed at converting library resources into digital formats while ensuring their accessibility through electronic platforms or digital libraries (**Keziz, 2024, p. 88**).

1. 2. Utilizing Information Technology to Facilitate Access to Resources and Information:

The technological boom in digital transformation has brought a paradigm shift to institutions that recognize the need to embrace modern technological advancements. This shift has made them more aware, flexible, and capable of innovation and creativity. As a result, digital transformation in libraries has become an inevitable necessity and a contemporary trend aligned with the rapid global changes and the aspirations of nations for progress and prosperity (**Ibrahim Bayoumi Ali Marai, 2023, p. 08**).

Currently, there is a growing focus on the application of information technology, including computing and telecommunications, in the field of libraries and information services , especially in the context of digital transformation in academic libraries. This shift has necessitated the move toward "digital libraries," where information resources are made available to users through digital electronic media. This transformation involves technical and functional requirements, standards, protocols, and a redefined role for libraries, reshaping their mission, infrastructure, and capabilities. Libraries have thus become a fundamental pillar in the transition of society toward a fully digital information era (**Al-Munim, 2010, p. 53**).

Mohamed Mohamed El-Hadi broadly defines information technologies as encompassing all technologies related to the collection, processing, storage, dissemination, and distribution of information. The term "information technology" gained widespread use in the late 1970s, and today, it is generally used to integrate and unify communication technologies with all associated software (**Mohamed El-Hadi, 2007, p. 55**).

1. 3. Transition from Traditional Management Systems to Digitally Integrated Systems:

With the initial efforts to adopt digital transformation in academic institutions, university libraries have shown a strong desire to benefit from the early outcomes of digital transformation, considering their active role in the academic community and university institutions. Indeed, they have leveraged this transformation and worked on developing a range of services and aspects that represent digital transformation, primarily associated with Web 2.0 technologies, including the following:

- Digital Collections: These have enabled libraries to organize and provide access to their information resources, allowing users to utilize them effectively. These collections were established by information institutions through the implementation of Web 2.0 applications and digitization processes.

- **Use of Technology**: The need to adopt technology has emerged due to its role in enhancing service efficiency and streamlining daily routine operations within libraries. Libraries have strategically embraced these new technologies to fulfill their ambition of serving their user communities through tools such as:

- RFID - QR Code - Social Media .

- **Digitization:** It is well known that digitization encompasses various analog processes associated with transforming physical entities available in libraries into digital formats. This shift responds to modern developments, enhances library operations, and keeps pace with ongoing changes.

- **Digital Library**: A digital library consists of websites that represent libraries in the digital space, containing library outputs such as references, study documents, and other materials. These resources can be accessed via the internet or through digital media on which they are stored.

- **Digital Repositories**: As one of the digital representations of libraries on the web, digital repositories serve as a storage hub for the academic community's scientific works. These repositories are managed using specialized software such as **Eprints** and **Dspace** .

- **Digital Platforms**: Digital platforms are another key aspect of digital transformation in academic libraries. They result from the use of technology to foster innovation and creativity. Libraries establish their presence on the web through these platforms, which offer various services, including automated search engines, subscriptions, current awareness services, and many other essential functions. (**Ghalem & Ghanem, 2024, pp. 87–88**)

1. 4. Digital Transformation Tools and Technologies:

1. 4.1. Digital Library Management Systems (LMS):

- **Content Management Systems (CMS):** Used to manage and publish library content, including announcements, events, and digital resources.
- **Integrated Library Systems/Digital Library Systems (ILS/DLS):** Used for managing library collections, books, digital resources, and circulation processes.
- **Electronic Portals**: Provide users with an interface to access digital library resources and electronic databases.
- **Search Technologies**: Enhance the user search experience on the library's website and direct them to relevant resources.
- **Visualization and Virtual Reality**: Offer interactive and educational experiences within the library, such as virtual tours and digital exhibitions.
- **Cloud Computing**: Used for securely and efficiently storing and sharing digital resources and data.
- **Automation and Robotics**: Improve cataloging, resource classification, inventory management, and enhance the user experience within the library. (Al-Zein & Hazima, 2024).

1. 4.2. Digital Databases and Electronic Search Interfaces:

The first type of initiative brought together several projects such as **Gale** , **Questa** , and **e-Brary** , which were developed by groups of publishers or publishing consortia. These initiatives involve the creation of digital collections, making them available for use and circulation. It is important to note that these collections are not limited to books alone but also include periodicals, journals, newspapers, bibliographic lists, official reports, and more.

For example, the **Gale** initiative provides reliable data, as most of its collections were initially produced by other providers before being adopted by **Gale** . However, this type of initiative has faced several criticisms, mainly focusing on:

- The quality and relevance of the documents, as well as the consistency and logical coherence of the collection as a whole.
- The methods of organizing and presenting content, including structuring, classification, text presentation, and search engines, all of which aim to facilitate searching and accessing texts.

The services offered by these digital databases vary from one platform to another. Some require users to pay a subscription fee before accessing documents, while others adopt the opposite approach, allowing users to browse the database freely but charging fees for reproduction and printing, a model known as "pay-per-print." **(Tasho, 2005, pp. 77–78).**

With the growing interest in databases and their development, modern databases have evolved into repositories that can store audiovisual data, including videos and images. Moreover, databases have become a means for storing program files, effectively functioning as data banks. These data banks do not generate information but process it to make it accessible to users through structured data organization. This structuring facilitates the retrieval of documents and information when needed by organizing metadata fields that simplify access to information.

Digital databases on the web consist of interconnected and structured data in electronic format, which can be accessed and processed using specialized computer software. **(Zein Al-Din, 2009, pp. 53–54).**

1. 4.3. Transition to Electronic Books and References:

This initiative focuses on enabling the circulation of entire books online rather than just excerpts, as implemented at the University of California. Among the most notable projects in this field is **NetLibrary** , which is specifically designed for libraries, particularly academic institutions. It is important to emphasize that the digital collection created through such initiatives is not directly accessible to users; instead, it is offered to institutions for the purchase of electronic books. These institutions then provide access to their users through a lending system that closely resembles traditional borrowing methods. **(Al-Hamza, 2008, p. 174).**

An electronic book (**e-book**) is defined as "an interactive digital learning resource primarily based on text, supplemented with images and illustrations. Its content can be presented in either a nonlinear (hyperlinked) or linear format, using nodes and links. Users can freely browse its content, and it can be stored on a **CD-ROM** or accessed online." (**Al-Shuboul, 2014, p. 380**).

1. 5.Emerging Technologies and Their Potential Use in Library Service Development:

Emerging technologies have represented a qualitative leap and a revolution in digitalization and modernization. While digital transformation concepts and strategies have long been associated with digital technologies, the rapid pace of technological advancement continues to accelerate dramatically in recent years. This has led to the emergence of new, high-performance technological models known as "emerging technologies," which include artificial intelligence (AI), the Internet of Things (IoT), augmented reality (AR), big data, cloud computing, and more.

1. 5.1. Artificial Intelligence (AI):

Artificial intelligence is defined as "a computer system capable of mimicking human behavior, intelligence, performance, and tasks." Some experts view AI as referring to machines and devices that perform tasks requiring a level of intelligence, such as understanding cognitive processes, knowledge representation, planning, learning, problem-solving, adaptation, and interaction. From a mathematical perspective, AI aims to activate these processes within a computer system and includes the methods needed to achieve this, such as algorithms and computational structures. (**Ben Berghouth, 2023, p. 448**).

In recent years, artificial intelligence (AI) has gained significant momentum, expanding rapidly across multiple sectors. This surge has led to the emergence of various AI-driven applications and platforms, which institutions have adopted according to their specific needs. Consequently, discussions have arisen regarding the integration of this technology into library environments. Libraries have substantial potential to incorporate AI in various aspects, including automating routine services through AI-powered applications, conducting both quantitative and qualitative data analysis, utilizing AI-driven chatbots to interact with library users, implementing AI-based notification and referral systems to enhance user experience, and establishing AI-integrated spaces to support both staff and users. By embracing AI, libraries can enhance operational efficiency, improve service delivery, and create a more interactive and user-friendly environment. (**Ghalem & Ghanem, 2024, pp. 89-90).**

1.5. 2. Big Data :

Big data is considered the real wealth in the post-information society and the primary fuel for all smart technologies. It is like the blood that runs through human bodies; without it, designing artificial intelligence technologies, robots, and self-driving vehicles would be impossible. Additionally, it would be difficult to analyze people’s needs and preferences to provide them with better smart services, and creating efficient and effective smart cities and communities that manage resources optimally would be unattainable. In summary, big data is the true essence of smart technologies. (**Khalifa, 2019, p. 87)**

1.5. 3. Internet of Things (IoT) :

We are moving towards connecting "things" to people through significantly enhanced interfaces. This trend includes industrial control systems for operating critical infrastructure, as well as wearable medical devices, agriculture, and more. (Al-Hazani, 2023, p. 83). The Internet of Things (IoT) works by linking personal and electronic devices to the internet, creating a network of interconnected smart devices. When applied in libraries, this model can streamline daily routine operations by integrating the internal network with various equipment and supporting AI technology with IoT to achieve a competitive advantage. (**Ghalem & Ghanem, 2024, p. 90**)

1.5. 4. Cloud Computing :

Cloud computing has become one of the most widely used terms in recent years. It refers to the collective processes of storing and retrieving data, as well as sharing and applying it in a purely digital model. This is achieved through the availability of various essential components such as "servers, applications, networks, etc.," which are provided rapidly by a service provider upon request. (**Ghalem & Ghanem, 2024, p. 91**)

1. 6. Benefits of Digital Transformation in Libraries

Digital transformation is reshaping vital sectors into business models that rely on digital technologies to innovate products and services while providing new channels to enhance performance efficiency to unprecedented levels. As a result, digital transformation reduces time and costs, increases flexibility and efficiency in production processes and data management, leverages artificial intelligence technologies, improves quality, simplifies procedures, and creates opportunities to offer innovative services beyond traditional methods. As a key driver and catalyst for the development of the digital economy, digital transformation also plays a role in enhancing transparency, reducing bureaucracy and corruption, expanding operations, and reaching a larger segment of beneficiaries. (**Al-Jabour, 2024, pp. 787–788)**

The benefits of digital transformation in university libraries can be highlighted in the following points:

1.6. 1. Providing Access to Digital Resources :

Users no longer need to visit traditional libraries for reading, browsing, or accessing information. Instead, they can explore dozens of digital libraries to search for references and sources, gaining entry to digital repositories that include e-books, audiobooks, digital journals, and databases. This enables users to access the resources they need from anywhere, borrow materials, and return them online, requiring only a computer and an internet connection. (**Al-Munim, 2010, p. 84)**

1.6. 2. Journals and Newspapers :

Many libraries subscribe to digital platforms, such as **Press Reader** , which partners with thousands of newspaper and magazine publishers worldwide. This platform allows users to access thousands of newspapers and periodicals—more than 7,000 publications from over 100 countries, available in 60 languages. This service enables beneficiaries with diverse needs to access electronic resources remotely from anywhere and at any time via their personal devices. Additionally, features such as adjustable font sizes and text-to-speech conversion enhance the digital reading experience.

1.6. 3. Streaming Media Services (Live Broadcasting) :

Many libraries provide **Streaming Media** services to their users, offering access to a wide range of digital content, including lectures, TV programs, documentaries, and audiobooks. Libraries may require users to obtain a membership card or a dedicated account to access these services.

1.6. 4. Providing Access to Databases :

Libraries offer access to a variety of resources and databases, allowing users to enter search terms and view results optimized for mobile devices. This service includes online library catalogs, integrated search systems, and original document retrieval, expanding the library's reach beyond its physical location. One example is the **PubMed** mobile database, which serves as a web-based gateway for accessing the "**Medline"** medical database.

1.6. 5.Digital Archives :

Some libraries digitize their special collections, historical documents, local archives, and rare or fragile materials, making them accessible online for research and exploration while ensuring their preservation. By digitizing rare and unique materials, libraries provide broader access to resources that were previously limited to in-person viewing.

1.6.6. Digital Communication :

Libraries use various methods to keep users informed about events, services, and trends. These include hosting webinars on different topics, writing blog posts, updating the library's website, uploading videos to YouTube, and providing access to online platforms where users can join book clubs, participate in discussions, and share annotations. These initiatives foster a sense of community among readers and enhance the social aspects of reading.

1. 6.7. Virtual Events :

Some libraries conduct virtual tours, author talks, and other events via platforms such as **Zoom** or **Skype** . Virtual visits are often easier to schedule than in-person visits and are generally more cost-effective. From a user engagement perspective, these events have a positive impact on audiences, especially students, by encouraging them to read.

Library specialist Jennifer Lewis states, "The greatest benefit of author visits for students is that they read more books." This enhances their skills, builds vocabulary, boosts creativity and confidence, and improves academic performance—not only in reading and writing but across all subjects. When authors discuss their writing process, students connect with the written word in entirely new ways, transforming books from abstract objects into living experiences. They gain insight into the journey from idea to publication as told by the person who created it, which sparks enthusiasm for reading more books and exploring a wider variety of literature. (**Unified Arab Catalog , 2024**)

1. 6. 8. Supporting Scientific Research in the Digital Age :

Libraries facilitate scientific research by establishing reliable communication channels that enable researchers to access and exchange scientific and technical information efficiently. This ensures that scientists, experts, and researchers obtain relevant data related to their fields with high accuracy. Digital libraries provide full-text access to resources, indexes, abstracts, query response services, selective information dissemination, hyperlinked texts, and direct bibliographic searches. They also offer interactive interfaces that allow researchers to stay updated in their field and receive requested documents and materials promptly. (**Al-Hamza, 2008, p. 248**)

Libraries offer diverse digital resources to support scientific research and education. Students and researchers can access scientific journals, academic databases, open-source materials, Open Course Ware (OCW), Open Educational Resources (OERs), webinars, virtual classrooms, and open researcher/contributor identifiers **(ORCID**). They can also utilize citation management tools such as **Mendeley** and **Zotero** , which are provided through library websites. Additionally, libraries develop comprehensive online information services and grant access to citation management programs, which are particularly beneficial for students and academic library users. (**Unified Arab Catalog , 2024**).

2. Challenges Facing Cybersecurity in University Libraries :

With the increasing reliance on information systems and internet-connected devices in our daily lives—ranging from mobile phones to personal computing devices—the number of users in cyberspace continues to grow (General Authority for Small and Medium Enterprises , 2022, p. 3). Cyberspace is a double-edged sword, offering numerous benefits while also posing significant risks and threats. Cybercrimes have become increasingly complex, sophisticated, and highly dangerous.

In addition to the various risks associated with cyberspace, cybersecurity itself faces numerous and complex challenges that many institutions struggle to overcome, especially as these threats have been continuously escalating in recent years. (**Boukers , 2022, p. 61**).

2. 1. Cybersecurity Threats in University Libraries :

In recent years, libraries have undergone significant changes and developments that have enhanced their performance, improved services, and helped achieve their goals. However, integrating libraries with the external world through the internet has also exposed them to numerous risks and cyberattacks that threaten the security, confidentiality, and integrity of their information, devices, applications, and networks (**Ali Sheta , 2023, p. 203**).

Information security can be defined as the field concerned with protecting information from threats and unauthorized access by implementing the necessary tools and measures to safeguard data from both internal and external risks. It also includes the standards and procedures designed to prevent unauthorized individuals from accessing sensitive information. Although information security is not a new concept, its practical implementation has become crucial with technological advancements, particularly with the expansion of the internet. Information security focuses on several key aspects, including secure access control, operating system security, application and software protection, and database security **(Kadi , 2015, p. 66**).

Cybersecurity, on the other hand, refers to the activities and processes involved in protecting and securing information and communication systems from damage, unauthorized use, modification, or exploitation. It requires extensive knowledge of potential threats such as viruses and other malicious entities (**Al-Namouri , 2023, p. 39**).

Among the major cybersecurity threats that university libraries may face are:

2. 1.1. Malware Attacks :

These attacks involve the introduction of malicious software and harmful code into the victim's system by disguising software downloads and exploiting security vulnerabilities (Mohamed Hussein , 2023, p. 9). Malware is designed to steal personal or institutional information and disrupt operations and computer systems. It often tricks users into downloading infected programs, allowing hackers to gain access to the victim's device and even the entire institutional network. In 2022, approximately 5.5 billion malware attacks were detected globally, with the majority occurring in the Asia-Pacific region. This figure is lower than the peak recorded in 2018, which reached 10.5 billion attacks (**Ali Sheta , 2023, pp. 224–225).**

2.1.2. Surface Breach Attacks :

These attacks target networks or devices directly by exploiting security vulnerabilities or using advanced hacking techniques. Attackers attempt to gain unauthorized access to systems, which can lead to data breaches or system failures.

2. 3.1. Phishing Attacks :

Phishing attacks aim to obtain users' sensitive information by sending fraudulent emails or text messages that appear to come from trusted sources. Attackers often trick users into sharing personal details such as passwords or banking information, compromising their security.

2. 4.1. Denial-of-Service (DoS) Attacks :

The objective of these attacks is to disrupt or restrict network services by overwhelming them with excessive traffic or an immense number of requests, ultimately leading to service failure and downtime.

2. 5.1. Wireless Network Attacks :

These attacks exploit vulnerabilities in wireless connections, including quick-pairing attacks and WPA/WEP key-cracking attacks , which can compromise the security of Wi-Fi networks and expose sensitive data.

2. 6.1. Social Engineering Attacks :

Social engineering involves psychological manipulation to trick users into revealing confidential information or creating unauthorized accounts. Cybercriminals often use deceptive emails or phone calls to persuade victims to provide sensitive data (**Mohamed Hussein , 2023, pp. 8–9**).

2. 7.1. Ransomware Attacks :

Ransomware is a type of malware designed to lock or encrypt a victim's system or files, demanding a ransom payment for their release. These attacks typically spread through malicious downloads or software vulnerabilities . Some ransomware variants exploit system flaws, preventing users from accessing their data until payment is made

(Hassan Ali , 2023, p. 28).

2. 8.1. The Role of Artificial Intelligence in Cyber Threats :

While AI has been instrumental in enhancing cybersecurity , it has also enabled more sophisticated and destructive cyberattacks . Malicious actors leverage AI-powered tools to develop advanced cyber threats, making them harder to detect and counter (**Sabik and others , 2024, p. 219**).

2.2. Technical Challenges:

- Difficulty in regularly updating digital systems.
- Protection against advanced cyberattacks.
- Managing the burdens associated with big data.

2. 3. Human Challenges:

- Limited awareness among library staff regarding the importance of cybersecurity.
- Human errors in handling data.
- Difficulty in training employees to cope with increasing digital threats.

2. 4. Legal and Regulatory Challenges:

- Laws related to data protection.
- Challenges in complying with regulations such as the General Data Protection Regulation (**GDPR**) .
- The need for cybersecurity legislation to evolve rapidly and adapt to the growing complexity of cybercrimes to ensure timely and effective countermeasures (**Boukers, 2022, p. 74**).

3. Cybersecurity Tasks:

The primary goal of cybersecurity is to protect and secure data, networks, computers, and software from cyber intrusions and unauthorized access (**Boukrin, 2022, p. 51**). Cybersecurity encompasses numerous crucial tasks, including: **(Tawaher , 2023, p. 282**)

3. 1. Protecting Users and Ensuring Device Security:

This is achieved through specialized protocols, such as encrypting emails, files, and other critical data, ensuring their security during transmission and safeguarding them from loss or theft.

3. 2. Protecting Computer Systems from Viruses:

Viruses can cause severe issues, making their prevention essential to maintaining system integrity.

3.3. Reducing Cybercrimes:

As cybercrimes continue to rise alongside rapid technological advancements, cybersecurity plays a vital role in:

- Protecting sensitive personal and organizational data from breaches and theft.
- Shielding institutions and businesses from malware attacks, phishing, and fraudulent schemes.
- Preventing extortion attempts and digital fraud.

3. 4. Preventing Unauthorized Use of Information:

Cybersecurity measures ensure that data is not exploited illegally, thereby preventing harm to individuals and organizations.

3. 5. Maintaining Public Safety and Security:

This involves protecting private information across all sectors without exception, particularly in critical fields such as healthcare, education, finance, and energy services, among others...

4. Strategies for Enhancing Cybersecurity in University Libraries:

Digital transformation initiatives require a comprehensive plan to ensure network security, which is crucial for protecting sensitive data from increasing threats. Integrating cybersecurity into digital transformation plans is essential, as it helps build trust among clients and partners. A previous study emphasized that organizations investing in cybersecurity technologies are more successful in reducing risks associated with digital transformation (**Hussein and others, 2024, p. 187)**.

Undoubtedly, any national strategy to combat cybercrimes must start with awareness of the severity of cybercrime and the need to address this phenomenon due to its regional and global implications. This requires providing the necessary legislative environment and highly skilled administrative and technical personnel (**Dalali & Belbachir, 2021, p. 556**). Achieving this necessitates fulfilling a set of essential requirements, which include:

4.1. Financial Requirements:

- Availability of **firewall** devices to protect network security.
- Designing an appropriate computer network and providing modern computing devices for the information system.
- Equipping devices with specialized software for cybersecurity protection and threat detection.
- Ensuring securely connected computers and mobile devices with appropriate specifications, linked to a protected database.
- Providing information system security to safeguard sensitive data.
- Deploying strong and well-protected servers to enhance data storage and processing security.
- Ensuring the availability of antivirus software to combat malware (**Ahmed Al-Haddad, 2022, pp. 711-712**).
- Regular updates of devices, as software updates often include critical security patches. Successful hacker attacks primarily target outdated systems that lack the latest security updates (**Al-Samhan, 2020, p. 16).**

4.2. Administrative Requirements:

- Regularly backing up files on an external storage unit (**Kadi, 2015, p. 70**).
- Encrypting data and administrative information systems to ensure confidentiality.
- Establishing administrative procedures within the university to enhance cybersecurity for administrative information systems .
- Protecting administrative data and information against cyber threats.

- Ensuring the availability of technical and bibliographic skills among staff.
- Enacting appropriate laws and regulations related to cybersecurity (**Ahmed Al-Haddad, 2022, p. 712)**.
- The cybersecurity management team in the library should define cybersecurity policies and procedures , including security controls and requirements. These should be documented, approved by the library authority, and communicated to all relevant staff and stakeholders.
- The library must comply with national cybersecurity regulations and adhere to any international agreements or obligations related to cybersecurity **(El Doussari, pp. 126, 129**).

4. 3. Human Requirements:

- Training and qualifying employees in information technology.
- Raising awareness among employees about the importance of information security and cybersecurity in university libraries.
- Defining responsibilities for work, monitoring, and oversight.
- Hiring qualified specialists in information technology, particularly in library systems.
- Organizing training sessions for administrative and academic staff on cybersecurity concepts.
- Educating staff on the importance of data protection and information security.
- Encouraging openness regarding the right to access, transfer, and share information securely (**Ahmed Al Haddad, 2022, p. 712).**

4.4. Technical Requirements:

- Avoid opening email attachments or clicking on links from unknown sources (**Mujahid, 2023, p. 64).**
- Provide essential security software , including antivirus programs, intrusion detection, and prevention systems.
- Install surveillance cameras and **biometric** devices and ensure network software updates.
- Implement robust information systems, firewalls, and original security applications.
- Ensure the availability of library protocols and programs for data improvement and protection.
- Monitor website access and combat viruses and malicious code.
- Secure documentation, passwords, encryption, logical access control, and file integrity verification.
- Provide vulnerability scanning tools and **VPN** services.
- Equip cybersecurity learning tools for staff and students.
- Utilize modern and high-quality computing and communication devices.
- Address ethical hacking issues and enhance digital forensics capabilities.
- Develop secure analysis and programming techniques (**Ahmed Al-Haddad, 2022, p. 712**).
- Apply artificial intelligence techniques to detect potential cyber threats.
- Enhance multi-layered security protection systems.
- Collaborate with relevant organizations to improve cybersecurity.
- Engage with other universities and national and international institutions to exchange knowledge on threats and security solutions.
- Consult cybersecurity experts to continuously update systems and policies.

4.5. A Comparative Table Summarizing Cybersecurity Strategies in University Libraries in Some Countries

The State	Main Strategy	Salient Aspects	International Cooperation and Future Prospects
United Kingdom	Cybersecurity Policy for University Libraries 2022	- Spreading Cybersecurity Awareness among Library Staff. - User Data Protection	- Cooperation with Universities and Educational Institutions. - Participation in Government Initiatives to Enhance Cybersecurity.
United States of America	NIST Cybersecurity Framework (CSF)	- Implementing the NIST Framework in University Libraries. - Training Staff on Best Practices. - Developing Cybersecurity Policies and Procedures	- Cooperation with Educational Institutions and Research Centres. - Participation in International Workshops and Conferences
Turkey	A Study on the Impact of Cybersecurity Awareness on Compliance in University Libraries (2024).	- Assessing the Level of Awareness and Compliance among Library Staff	- Enhancing Cooperation between University Libraries. - Exchange of Knowledge and Expertise between Educational Institutions
China	Cybersecurity Law of the People's Republic of China 2016	- Protection of Users' Personal Data. - Developing Local Cybersecurity Technologies	- Developing Local Cybersecurity Technologies

Conclusion:

Based on the discussions presented, it is evident that the continuous adoption of modern technologies across various sectors, particularly in university libraries, has significantly accelerated the digital transformation of their processes, functions, and collections. This transformation necessitates thorough preparation, investment in digital infrastructure, and a well-trained workforce, while maintaining the highest cybersecurity standards. Additionally, legal regulations and policies must be enforced to address the rising complexities of cybercrime, preventing potential security breaches. This highlights the critical need for integrating cybersecurity with digital transformation in university libraries.

- Recommendations: To enhance cybersecurity in university libraries, the following recommendations are proposed:
- Enhancing Cybersecurity Awareness and Training: Libraries should train staff on the latest cybersecurity measures, including virus protection, phishing detection, and secure data handling.
- Developing Digital Infrastructure: Universities should upgrade their technological infrastructure by modernizing systems and strengthening networks to handle large volumes of digital data securely, while also shifting toward cloud-based solutions.
- Implementing Comprehensive Security Policies: Establishing clear cybersecurity policies to safeguard data confidentiality, ensure reliable backups, and comply with international data protection standards.

- Investing in Advanced Security Technologies: Adopting state-of-the-art security tools such as antivirus programs, intrusion detection systems, and encryption techniques to protect users' data and digital content.
- Balancing Open Access with Security: Libraries should find a balance between providing easy access to academic resources and ensuring these resources remain protected from unauthorized use or cyber threats.
- Fostering Collaboration with Cybersecurity Institutions: Strengthening partnerships with cybersecurity organizations to offer continuous training and expert consultations for library staff.
- Keeping Up with Legal and Regulatory Cybersecurity Developments: Staying updated with evolving legal frameworks on digital data protection, such as **GDPR**, and ensuring full compliance in all digital operations.
- Planning for Business Continuity in Emergencies: Developing comprehensive contingency plans to maintain library services in the event of cyberattacks or technical failures.
- Promoting Digital Literacy Among Users : Educating students and researchers on cybersecurity best practices, encouraging strong password management, and raising awareness about data protection when accessing digital resources.
- Conducting Regular Risk Assessments : Performing periodic security evaluations to identify vulnerabilities in digital systems and taking proactive measures to mitigate potential threats.

By implementing these recommendations, university libraries can create a secure digital environment that fosters academic research while safeguarding critical information from cyber threats.

Bibliography :

First: Books

1. Ahmed Qasim Al-Jamal, et al. (2023). **Digital Transformation in Arab Higher Education Institutions: Reality, Challenges, and Future Approaches**. [No Place], Arab Council for Scientific Research.

2. The General Authority for Small and Medium Enterprises. (2022). **Cybersecurity**. Saudi Arabia: General Authority for Cybersecurity.

3. Amal Keziz. (2024). **Digital Transformation and the Shift Towards Applications: Visions and Future Prospects.** Germany: Arab Democratic Center.

4. Ihab Khalifa. (2019). **Post-Information Society: The Impact of the Fourth Industrial Revolution on National Security**. Cairo: Al-Arabi Publishing & Distribution.

5. Hamad El Doussari. [No Date]. Your Path to Mastering Cybersecurity. [No Place], [No Publisher].

6. Sabik Amira, et al. (2024). **Artificial Intelligence: Multidisciplinary Perspectives**. Berlin (Germany): Arab Democratic Center for Strategic, Economic, and Political Studies.

7. Alaa Abdulkhalik Hussein, et al. (2024). **Cybersecurity: Principles and Practices for Information Security Assurance.** Iraq: Dar Al-Sard for Printing, Publishing, and Distribution.

8. Mohammed Mohammed Al-Hadi. (2007). **Educational Information Systems: Reality and Aspirations**. Cairo: Egyptian Lebanese House.

9. Mufeed Awad Hassan Ali. (2023). **Introduction to Cybersecurity**. Qatar: [No Publisher].

10. Muhannad Anwar Al-Shuboul & Rebhi Mustafa Alyan. (2014). **Electronic –Learning = e-learning** . Amman: Dar Safa for Publishing and Distribution.

11. Nabil Abdul Rahman Al-Munim. (2010). **Digital Libraries in Saudi Arabia: King Fahd National Library as a Model.** Riyadh: King Fahd National Library.

Second: Journals:

12. Ibtisam Abdel Salam Ali Sheta. (2023). **Securing Electronic Information in Al-Azhar University Libraries: The Central Library as a Model**. Journal of Humanities Studies Sector, Al-Azhar University, Vol. 32, No. 1.

13. Boukren Abdelhalim. (2022). **Cybersecurity and Its Conceptual Implications**. Tabna Journal for Academic Scientific Studies, Vol. 05, No. 02.

14. Dellali Djilali & Belbachir Yaakoub. (2021). **National Cybersecurity Challenges in the Era of Digital Transformation: A Review of Theoretical Foundations and Legislative Response Strategies**. Kuwait International Law College Journal, Year 10, No. 1, Serial No. 37.

15. Saad Bougueres. (2022). **Cybersecurity: Risks, Threats, and Challenges Requiring Specific Practices, Recommendations, and Strategies**. Journal of Social Protection Research, Vol. 3, No. 1.

16. Shorouk Mohammed Mohamed Al-Jabour. (2024). **The Importance of Digital Transformation in Improving Library Performance in Municipalities**. Arab Society Journal for Scientific Studies, Issue 71.

17. Tawaher Abdeljalil. (2023). **Cybersecurity Strategies as a Challenge to Digital Transformation in Government Organizations, with Reference to the UAE Experience.** Al-Risala Journal for Media Studies, Vol. 07, No. 01.

18. Faiza Ahmed Al-Husseini Mujahid. (2023). **Cybersecurity Awareness: A Luxury or a Necessity in the Information Age?** Research and Education Journal: National Institute for Educational Research, Vol. 13, No. 2.

19. Kadi Zine Eddine. (2015). **Security Measures and Prevention of Cybercrimes in Libraries and Information Centers**. "Ishara" Journal of Information Science, Archival Science, and Library Science, No. 04.

20. Layla Ben Berghouth. (2023). **Cybersecurity and Digital Privacy Protection in Algeria in the Age of Digital Transformation and Artificial Intelligence: Threats, Technologies, Challenges, and Countermeasures**. International Journal of Social Communication, Abdelhamid Ibn Badis University - Mostaganem, Vol. 10, No. 01.

21. Mohammed Reda Ghalem & Ghanem Nadhir. (2024). **Digital Transformation of University Libraries in the Context of Emerging Technologies: Reality and Aspirations - A Field Study at the Libraries of Batna 1 University**. Journal of Humanities and Social Sciences, Vol. 13, No. 4.

22. Mohammed Mahmoud Zain El-Din. (2009). **Digital Databases and Their Importance in Building Search Engines**. Informatics Journal, No. 29.

23. Mohammed Tashour. (2005). **From Traditional Libraries to Digital Libraries**. Journal of Libraries and Information, Constantine, Dar Al-Huda for Publishing and Distribution, Vol. 2, No. 2.

24. Mona Abdullah Al-Samhan. (2020). **Requirements for Achieving Cybersecurity in Administrative Information Systems at King Saud University**. Journal of the Faculty of Education, Mansoura University, No. 111.

25. Nabila Mohammed Abdel Dayem Ahmed Al-Haddad. (2022). **Requirements for Achieving Cybersecurity in Yemeni University Libraries: A Case Study**. Al-Bayda University Journal, Vol. 4, No. 2.

26. Noora Bint Nasser Bin Abdullah Al-Hazani. (2023). **Regulations and Requirements for Implementing Cybersecurity to Protect Data at Princess Nourah University**. King Fahd National Library Journal, No. 28.

27. Heba Ibrahim Bayoumi Ali Marai. (2023). **Requirements for Enabling Digital Transformation in the Educational Process in the Departments of Documentation, Libraries, and Information in Egyptian Public Universities: A Survey Study.** Scientific Journal for Libraries, Documentation, and Information, Vol. 5, No. 13.

28. Heba Salah El-Din Al-Namouri. (2023). **Internet Piracy: An Applied Study on a Sample of Egyptian Information Facility Websites**. Egyptian Journal of Information Sciences, Vol. 10, No. 2.

Third: Theses and Dissertations.

29. Mounir Al-Hamza. (2008). The Role of the Digital Library in Supporting Training and Scientific Research in Algerian Universities: The Digital Library of Emir Abdelkader University in Constantine as a Model. Master's Thesis, Department of Library Science, Mentouri University, Constantine.

Fourth: Webography

30. Unified Arab Index. (2024). **How Can Digital Resources in Libraries Create a Better Experience for Users?** [**Available Online**].
https://www.aruc.org/ar/%D8%A7%D9%84%D8%A3%D8%AE%D8%A8%D8%A7%D8%B1-%D9%88%D8%A7%D9%84%D9%81%D8%B9%D8%A7%D9%84%D9%8A%D8%A7%D8%AA/%D9%85%D8%AF%D9%88%D9%86%D8%A9-%D8%A7%D9%84%D9%81%D9%87%D8%B1%D8%B3/%D9%83%D9%8A%D9%81-%D9%8A%D9%85%D9%83%D9%86-%D9%84%D9%84%D9%85%D9%88%D8%A7%D8%B1%D8%AF-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9-%D9%81%D9%8A-%D8%A7%D9%84%D9%85%D9%83%D8%AA%D8%A8%D8%A7%D8%AA-%D8%A3%D9%86-%D8%AA%D9%86%D8%B4%D8%A6-%D8%AA%D8%AC%D8%B1%D8%A8%D8%A9-%D8%A3%D9%81%D8%B6%D9%84-%D9%84%D9%84%D9%85%D8%B3%D8%AA%D9%81%D9%8A%D8%AF%D9%8A%D9%86%D8%9F . Accessed: 22/01/2025 at 13:00.

31. Aya Al-Zein & Fatima Hazima . (2024). Information Technologies in Libraries and Information Centers. [Available Online].
https://www.slideshare.net/slideshow/ss-9949/267525195#2
Accessed: 09/01/2025 at 21:40.

32. Qasem Mohammed Hussein. (2023). Fundamentals of Cybersecurity. [Available Online]. https://www.researchgate.net/publication/380695935
Accessed: 25/01/2025 at 11:00.