THOMAS ADEWUMI UNIVERSITY, OKO, KWARA STATE
Science | Technology | Medicine

Thomas Adewumi University Journal of Innovation, Science and Technology (TAU-JIST)

ISSN: 3043-503X

REVIEW ARTICLE

DIGITAL THREATS TO LIBRARIES AND THEIR IMPACT ON SUSTAINABLE DEVELOPMENT GOALS (SDGS)

Tunde Toyese Oyedokun

Ag. University Librarian, Thomas Adewumi University, Oko-Irese, Kwara State Nigeria.

Correspondence Author E-mail: Tunde.oyedokun@tau.edu.ng

This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ARTICLE DETAILS

Article History:

Received 02 July 2024
Accepted 05 October 2024
Available online 10 November 2024

ABSTRACT

This review article explores the complex challenges posed by digital threats to achieving Sustainable Development Goals (SDGs), focusing specifically on libraries as primary targets. It underscores the crucial role libraries play in advancing the SDGs and proposes strategies to mitigate digital threats in the digital era. The researcher conducted an extensive review of existing literature on digital threats and the attainment of SDGs, emphasizing libraries' roles. Using search terms such as "digital threats AND libraries," "cybersecurity AND SDGs," and "privacy breaches AND libraries," and accessing databases like PubMed, Scopus, Web of Science, and Google Scholar, the review identified key digital threats, library vulnerabilities, and mitigation strategies. A total of 98 sources were analyzed, including case studies illustrating the impact of digital threats on libraries and their efforts to advance SDGs. Findings reveal the severity of cyber threats faced by libraries, with case studies such as the British Library's ransomware attack highlighting the need for modernized infrastructure and cybersecurity preparedness. The London Public Library's refusal to pay ransom demonstrated resilience and ethical principles, while the Toronto Public Library's response underscored challenges in restoring services and protecting data post-attack. Through transparency, proactive communication, and investment in cybersecurity, libraries can mitigate risks and uphold their mission of providing equitable access to information. However, the research is limited to specific incidents and may not capture the diversity of global cyber threats. Future research could explore more case studies and long-term impacts of cyberattacks. The findings emphasize the importance of prioritizing cybersecurity, fostering resilience, and collaboration among policymakers, government agencies, and international organizations to support libraries. This study contributes to the growing literature on library cybersecurity, offering practical guidance for safeguarding patron privacy and advancing SDGs in the digital age.

KEYWORDS

Digital Threat, Sustainable Development Goals (SDGs), Libraries, Cybersecurity, Misinformation

Quick Response Code	Access this article online	
	Website: https://journals.tau.edu.ng/index.php/tau-jist	**DOI:** https://doi.org/10.5281/zenodo.14202358

Introduction

The Sustainable Development Goals (SDGs), established by the United Nations in 2015, represent a global commitment to address social, economic, and environmental challenges by 2030. Covering issues such as poverty, health, education, gender equality, clean water, affordable energy, economic growth, infrastructure, inequality, sustainable cities, climate change, ocean and forest conservation, and peace, these 17 goals were adopted by all 193 UN member states as part of the 2030 Agenda for Sustainable Development (United Nations, 2015). However, the COVID-19 pandemic, rising inequalities, climate change, and biodiversity loss have impeded progress. Moreover, the advent of the digital age has introduced new complexities. Digitalization has transformed information access and utilization, presenting opportunities and risks (Popkova, 2023; Alojail & Khan, 2023; Renn, Beier & Schweizer, 2021; IASS, 2021). Libraries, as purveyors of reliable information, face significant digital threats, including misinformation, cybersecurity attacks, and privacy breaches, which compromise their role in advancing the SDGs.

Cyberattacks disrupt essential functions like cataloging, circulation, and online access, impacting literacy, education, and research (Igbinovia & Ishola, 2023; Aregbesola & Nwaolise, 2023; Ibrahim & Umar, 2020). For instance, the British Library's ransomware attack in October 2023 highlighted the need for robust cybersecurity (British Library, 2024). Libraries must invest in cybersecurity measures, staff training, multi-factor authentication, and strong backup strategies to ensure service continuity and protect data (Petrowicz, 2021). Additionally, libraries combat misinformation by promoting media literacy, offering training on assessing online source credibility, and collaborating with media organizations and fact-checking initiatives (Sullivan, 2019b). However, the digital divide exacerbates disparities in access to and proficiency in digital technologies, hindering SDG progress, particularly in low-income and rural areas (Bogdan-Martin & Steiner, 2023; United Nations, 2023). Libraries play a crucial role in bridging this divide by providing digital access and literacy training. They also face ethical challenges in protecting patron privacy while complying with data protection regulations (Corrado, 2020).

Despite these challenges, libraries remain resilient and adaptable, leveraging their role as community hubs to promote digital inclusion and foster innovation. Recognizing their pivotal role and investing in their capacity to address digital threats, policymakers and communities can unlock libraries' full potential as drivers of sustainable development (Hoving, 2023; Aslan, Aktug, Ozkan-Okay, Yilmaz & Akin, 2023; Oladokun, Yemi-Peters & Owolabi, 2021). This review article examines the intersection of digital threats and the SDGs, focusing on libraries as both targets and agents of change.

Method and Procedure

The researcher conducted a comprehensive review of existing literature on the intersection of digital threats and the achievement of Sustainable Development Goals (SDGs), with a focus on the role of libraries. The review identifies key digital threats affecting the SDGs, the vulnerabilities of libraries to these threats, and the existing strategies employed by libraries to mitigate them. Selected relevant case studies that illustrate the impact of digital threats on libraries and their efforts to advance the SDGs. These case studies provide real-world examples of challenges faced by libraries, such as cyberattacks, misinformation campaigns, or digital divide issues, and the strategies they have implemented to address them. The following search terms and strategies were employed, beginning by searching academic databases such as PubMed, Scopus, Web of Science, and Google Scholar using combinations of search terms such as "digital threats AND libraries", "cybersecurity AND SDGs", "privacy breaches AND libraries", etc. Utilized Boolean operators (AND, OR, NOT) to refine searches and combine different concepts. For instance, "(cybersecurity OR data breaches) AND libraries AND SDGs". Include specific terms related to the types of digital threats faced by libraries, such as "ransomware", "malware", "misinformation", "digital divide", etc., to capture relevant literature. A total of 98 sources was relevant and used for the review article.

Digital Transformation and its Impact on Sustainable Development Goals (SDGs)

Digital transformation signifies a profound shift in societal functions, driven by the integration of digital technologies into nearly every aspect of human life. This encompasses the adoption and utilization of digital tools, processes, and systems across diverse sectors, fundamentally altering how individuals, businesses, and governments operate (Omol, 2023). From the proliferation of smartphones and the Internet of Things (IoT) to the widespread adoption of cloud computing and artificial intelligence (AI), digital transformation has reshaped how people communicate, work, learn, and interact with their environment. At its core, digital transformation is propelled by the relentless pace of technological innovation, continuously introducing new opportunities and challenges for societies worldwide (Hai, Van & Tuyet, 2021). This transformation is not merely technological but a comprehensive reimagining of social, economic, and political structures in the digital age. It transcends geographical boundaries and affects people of all ages, backgrounds, and socioeconomic statuses, presenting both opportunities for progress and risks of exacerbating existing inequalities.

Against this backdrop, the Sustainable Development Goals (SDGs) emerge as a global agenda aimed at addressing the most pressing social, economic, and environmental challenges by 2030. Adopted by the United Nations in 2015, the SDGs comprise 17 interconnected goals and 169 targets, spanning areas such as poverty eradication, health and well-being, education, gender equality, climate action, and sustainable cities and communities. The SDGs embody a universal vision for a safe, just, and sustainable world, emphasizing inclusivity and shared responsibility. These goals are rooted in principles such as human rights, environmental protection, and inclusive development. They aim to improve the circumstances of all individuals globally, focusing on key aspects like poverty alleviation, sustainable resource management, climate action, and governance enhancement. The SDGs underscore the interconnectedness of social, economic, and environmental aspects of sustainable development, highlighting the need for collaboration among various actors, including state and non-state entities, to achieve these ambitious goals (Fallah-Shayan, Mohabbati-Kalejahi, Alavi & Zahed, 2022).

Digital technologies can play a pivotal role in accelerating progress towards the SDGs by unlocking new pathways for innovation, empowerment, and collaboration. According to a global analysis by ITU, UNDP, and partners, digital technologies can directly benefit 70% of the 169 SDG targets, including areas such as climate action, education, hunger, and poverty. Data suggests that countries which improved their digital maturity, as measured by digital affordability and infrastructure indices, outpaced their peers in SDG progress for selected income levels. The SDG Digital Acceleration Agenda highlights 34 digital solutions already demonstrating how tech can drive progress on the SDGs. However, realizing the full potential of digital technologies requires considerable investment in connectivity infrastructure, building digital skills, and creating conditions for job retraining and new opportunities. Funding the $3.7 trillion SDG financing gap should focus on enablers like infrastructure and connectivity while leveraging diverse financing methods and collaboration with the private sector. Digital public infrastructure built on robust governance and strong local digital ecosystems can deliver high impact across all 17 SDGs. By centering on people and fostering inclusive, sustainable, and responsible digital transformation, countries can accelerate progress on the 2030 Agenda (UNDP, 2023a). Digital transformation offers unprecedented opportunities to enhance access to information and services, catalyze economic growth, and promote social inclusion. For example, digital platforms and mobile applications enable individuals to access healthcare services, educational resources, and financial tools remotely, overcoming barriers of distance and infrastructure. Similarly, digital marketplaces and e-commerce platforms provide opportunities for small businesses and entrepreneurs to reach new markets and customers, driving economic empowerment and job creation (Mondejar et al., 2021).

Moreover, digital technologies are transforming the way governments make public policy decisions by enabling data-driven, evidence-based policymaking. Big data analytics is being systematically incorporated into various stages of the health policy cycle to enable more accurate and rapid policy decisions (Chao, Sarker, Ali,

Firdaus, Azman & Shaed, 2023). Descriptive, predictive, and prescriptive analytics are being used to inform public health policy choices based on data from electronic health records, public health databases, patient data, and social media. This allows policymakers to evaluate the impact and risk of policy changes at the population level (Hossin, Du, Mu & Asante, 2023). The Foundations for Evidence-Based Policymaking Act in the U.S. statutorily mandates federal evidence-building activities, open government data, and confidential information protection. It creates a new paradigm calling on agencies to re-evaluate how they organize evidence-building, data management, and data access functions to ensure an integrated connection to data and evidence needs. Fostering a data-driven culture is crucial for integrating data into policymaking. This involves mindsets, behaviors, and values that promote evidence-based decision making, collaboration, curiosity, and learning. It means considering data and evidence by default in the policymaking process. An analysis shows an average economic benefit of $32 for every dollar invested in data (ACT-IAC, 2019). Advanced analytics, machine learning, and predictive modeling techniques empower stakeholders to gain insights into complex social, economic, and environmental dynamics, informing targeted interventions and resource allocation strategies. Harnessing the power of big data and digital analytics, policymakers can optimize resource utilization, monitor progress towards the SDGs, and respond dynamically to emerging challenges and opportunities. In a nutshell, digital technologies are enabling a shift towards data-driven, evidence-based policymaking, but realizing its full potential requires cultural change, new mindsets, and overcoming technical barriers. Governments that embrace this transformation can make more informed, effective policy decisions to address societal challenges (Kumar, Sai, Hordiichuk, Menon, Aathy, Saha & Balaji, 2023).

Digital transformation plays a crucial role in promoting inclusive development by empowering marginalized communities and reducing inequalities. Digital transformation offers opportunities for those who are frequently left behind by encouraging innovation and improving access to information and services. It enables marginalized groups, including women, people with disabilities, and those in poverty, to participate meaningfully in the digital economy (Qureshi, 2023). Through initiatives like enabling online sales for market vendors, supporting MSMEs with digital capabilities, and implementing IoT solutions for agriculture, digital transformation helps create jobs, increase productivity, and improve livelihoods. Moreover, digital inclusion ensures that everyone, regardless of socioeconomic status, gender, ethnicity, or location, has equal access to digital technologies. Bridging the digital divide, digital inclusion reduces inequality, increases access to education and employment opportunities, and promotes social mobility. In the Philippines, for example, efforts to achieve digital inclusion have been instrumental in reducing poverty and creating economic opportunities, highlighting the importance of ensuring that all segments of society benefit from digital advancements (Munyoka, 2022).

In essence, digital transformation not only drives economic growth but also serves as a catalyst for social progress by empowering marginalized communities, fostering innovation, and creating a more inclusive society (Manzoor & Vimarlund, 2018). Governments and organizations can leverage digital technologies to bridge the digital divide, expand access to education and healthcare, and promote social and economic inclusion through targeted initiatives. For example, initiatives such as digital literacy programs, community internet centers, and mobile banking services empower underserved populations, including women, rural communities, and persons with disabilities, to participate more fully in the digital economy and society. Ensuring affordable access to the internet for all by 2030 involves promoting universal access to ICT infrastructure, addressing affordability, enhancing digital skills and literacy, and improving the relevance and awareness of being online (United Nations, 2021). Developing regulatory frameworks and policies that leverage digital technologies for sustainable development and support digital inclusion, such as promoting inclusive ICT design and aligning science, technology, and innovation policy with social development goals, is essential. Fostering multi-stakeholder partnerships between governments, public institutions, the private sector, academia, civil society, and marginalized groups to co-design and co-create inclusive digital policies and innovative solutions is

crucial. By implementing these targeted initiatives, governments and organizations can harness the power of digital technologies to bridge the digital divide, expand access to essential services, and promote social and economic inclusion for all (Mendez-Dominguez, Munoz, Diez & De-Mesa, 2023; Penesi, Bocconi & Ferlino, 2020).

However, there are still challenges in breaking down data silos, bridging legacy systems, and enabling a true data-driven policy ecosystem. Policymakers need to be aware of the value of data and be data literate enough to add value to policies in real-time. Early adopters who champion evidence-based practices are important for inspiring others and showcasing successful examples. Alongside its transformative potential, digital transformation, while offering significant benefits for achieving the SDGs, also poses complex challenges and risks that need to be addressed to ensure inclusivity and avoid leaving anyone behind in the pursuit of the SDGs. The intersection of digital innovation and sustainability governance highlights the importance of concerted action to prevent digital technologies from exacerbating inequalities and environmental degradation. Key actions include sharing lessons learned, enabling co-learning among disconnected actors, testing and co-developing digital solutions, and ensuring integration with local contexts for sustainable and inclusive digital transformation (Kumarasinghe, Gerard & Ventimiglia, 2022). Additionally, the need for a sustainable data governance framework, open data policies, and the development of digital and data-related skills are crucial to align digital transformation with the SDGs and drive progress while safeguarding against negative impacts and ensuring equitable access to the benefits of digital technologies. Addressing these challenges and risks is essential to harness the full potential of digital transformation in advancing sustainable development goals while ensuring that no one is left behind in this transformative journey. These challenges include digital exclusion, cybersecurity threats, privacy concerns, and the proliferation of misinformation and the digital divide.

Digital Divide and Access to Information

The digital divide refers to the gap between those who have access to modern information and communication technologies (ICT) and those who do not or have limited access. This divide can be seen between demographics, regions, urban and rural areas, educated and uneducated individuals, and different socioeconomic groups. Despite advancements, the digital divide remains a significant issue globally, with millions of households lacking broadband internet access in both rural and urban areas. In the context of underserved communities, the digital divide exacerbates existing inequalities by limiting access to information, technology, and opportunities for economic growth and social mobility. Bridging this gap is crucial for improving digital literacy, skills, democracy, and overall economic equality (Heeks, 2022). This disparity not only limits individuals' ability to participate fully in the digital economy and society but also hinders progress towards achieving Sustainable Development Goals (SDGs) related to education, health, and economic development. The digital divide is manifested in disparities in access to essential digital resources such as high-speed internet, computers, smartphones, and digital literacy skills. Underserved communities, including rural areas, low-income neighborhoods, and marginalized populations, often lack access to reliable broadband infrastructure and affordable devices, rendering them digitally excluded (Afzal, Khan, Daud, Ahmad & Butt, 2023). As a result, individuals in these communities, face barriers to accessing online information, educational resources, telehealth services, and economic opportunities, perpetuating cycles of poverty and inequality.

Limited access to digital resources indeed presents significant challenges to achieving Sustainable Development Goals (SDGs) related to education, health, and economic development (Mondejar et al., 2021). Without access to digital technologies and internet connectivity, students in underserved communities face barriers in participating in online learning platforms, accessing educational resources, and engaging in digital literacy initiatives. This situation exacerbates educational inequalities and widens the gap in academic achievement between digitally literate and digitally excluded students. The lack of access to digital resources hinders the ability of students to benefit from the advantages that technology offers in education. It impacts concentration,

comprehension, flexibility, critical thinking, communication between teachers and students, classroom productivity, collaborative work, motivation, and the incorporation of new learning methods. Additionally, the World Bank emphasizes the importance of addressing the digital divide to accelerate learning, reduce learning poverty, and support skills development, especially in low- and middle-income countries where learning poverty is a significant concern (The World Bank, 2024). Closing this gap requires efforts to bridge disparities in digital infrastructure, human infrastructure, and logistical and administrative systems to deploy and maintain technology in education.

Access to telehealth services, online medical information, and digital health records is essential for promoting health equity and addressing healthcare disparities. However, individuals in underserved communities often lack access to these digital resources, limiting their ability to receive timely medical care, access health information, and participate in preventive healthcare initiatives. Telehealth has the potential to improve access to healthcare, especially for patients in rural and remote areas who may have to travel long distances to see a provider (Zhang & Saltman, 2022). However, disparities in access to telehealth services persist due to factors like geographical location, socioeconomic status, age, disability, and race. Patients without reliable internet access, appropriate devices, or digital literacy skills face greater barriers to using telehealth. Integrating telehealth with interoperable electronic health record (EHR) systems can improve health outcomes, patient experience, and clinician satisfaction. But smaller and rural hospitals often lag behind in adopting advanced EHR systems and telehealth services due to limited resources and technical expertise. This uneven adoption contributes to disparities in access to telehealth and data sharing. To help address these challenges, health policies should accelerate telehealth adoption, hospitals should develop strategies for different telehealth services, and providers should offer the same standard of care via telehealth as in-person visits. Digital health systems also need to be designed with accessibility principles to support a range of technologies, settings, and diverse users. While digital health innovations like telehealth hold promise for improving healthcare access and equity, significant work remains to ensure these technologies are designed and deployed in an inclusive manner that serves the needs of marginalized populations. Addressing the digital determinants of health will be critical to realizing the full potential of telehealth to reduce disparities (Phuong, Ordonez, Cao, Moukheiber, Moukheiber, Caspi, Swenor, Naawu & Mankoff, 2023).

The digital economy presents significant opportunities for job creation, entrepreneurship, and economic empowerment, but it also risks exacerbating existing inequalities if the digital divide is not addressed. Individuals without access to digital technologies and reliable internet connectivity are excluded from participating in online job markets, accessing e-commerce platforms, and leveraging digital skills for economic advancement (Youssef, Boubaker, Dedaj & Carabregu-Vokshi, 2021). Closing the digital divide requires concerted efforts to expand broadband coverage to remote areas and low-income neighborhoods, as well as making digital devices more affordable (Afzal, Khan, Daud, Ahmad & Butt, 2023). Governments, private sector entities, and non-profit organizations must collaborate to invest in building the necessary infrastructure and providing subsidized devices or community computer centers. Digital literacy and skills training are crucial for empowering individuals from underserved communities to thrive in the digital economy (Mokhtari, 2023). They can leverage digital tools to start and grow their businesses, access global markets, and create employment opportunities by acquiring essential skills such as computer literacy, coding, data analysis, and social media marketing. Entrepreneurship plays a key role in driving economic growth and development, particularly in developing countries where it can help eliminate poverty, create jobs, and foster community development.

Entrepreneurs contribute to increased productivity and the creation of new markets, by introducing new products or services and creating efficient systems for utilizing resources. Digital empowerment through e-commerce has the power to transform economies by driving job creation, fostering entrepreneurship, and boosting trade. E-commerce platforms provide access to online marketplaces, digital

payment systems, and logistics services, which are crucial for the success of businesses in the digital age (Dabbous, Barakat & Kraus, 2023). However, challenges such as limited internet infrastructure, low digital literacy rates, and regulatory barriers pose significant obstacles to the growth of e-commerce and digital entrepreneurship in many regions (Kala, 2023). Addressing these challenges requires collaborative efforts from governments, private sector actors, and international organizations to improve digital connectivity, provide training and support for entrepreneurs, and create an enabling regulatory environment. While the digital economy offers immense opportunities for job creation, entrepreneurship, and economic empowerment, it also risks perpetuating cycles of poverty and unemployment if the digital divide is not addressed. Closing this divide requires a multi-stakeholder approach to expand digital access, provide digital skills training, and support entrepreneurship in underserved communities.

Various initiatives aim to bridge the digital divide and promote digital inclusion in underserved communities such as community-led initiatives to build and deploy broadband infrastructure in underserved areas, providing affordable high-speed internet access to residents and businesses. Educational programs and training initiatives aimed at improving digital literacy skills among individuals of all ages, empowering them to navigate digital technologies, access online resources, and participate in the digital economy (Azzahra & Amanta, 2021). Public libraries, community centers, and internet cafes offer free or low-cost access to computers, internet connectivity, and digital resources, providing vital lifelines for individuals without home internet access (WhoFi, 2023; Pressreader, 2023). These initiatives play a crucial role in narrowing the digital divide and promoting digital inclusion, but more concerted efforts are needed to address the root causes of inequality in access to information and technology. Policymakers, government agencies, private sector stakeholders, and civil society organizations must collaborate to develop comprehensive strategies for expanding broadband infrastructure, reducing the cost of digital devices and services, and promoting digital literacy and skills development in underserved communities. Stakeholders can unlock the transformative potential of digital technologies and advance progress towards achieving the SDGs, leaving no one behind in the journey towards a more equitable and inclusive future by bridging the digital divide.

Cybersecurity Threats and Data Integrity

Cybersecurity threats pose significant risks to libraries and other information institutions, jeopardizing data integrity and patron privacy. As custodians of vast collections of information and repositories of sensitive patron data, libraries are increasingly targeted by cybercriminals seeking to exploit vulnerabilities in their systems and networks. From data breaches and ransomware attacks to phishing scams and social engineering tactics, these cyber threats undermine the ability of libraries to fulfill their role as trusted sources of information and erode public trust in their services (Igbinovia & Ishola, 2023; Ashikuzzaman, 2023a). Cyberattacks targeting libraries and information institutions are indeed on the rise due to the increasing digitization of collections and services. These attacks involve unauthorized access to systems and databases, leading to the theft or exposure of sensitive patron information like personal identifiable information (PII) and login credentials. Academic institutions, including libraries, are particularly vulnerable to cyber threats, with ransomware attacks occurring every eight minutes globally. Criminals target these institutions for valuable research data and personal information, posing risks of espionage and economic exploitation (Lupton, 2023; Ibrahim & Umar, 2020).

The malicious software that encrypts library data, rendering it inaccessible until a ransom is paid, is known as ransomware. Ransomware attacks can disrupt library operations, compromise data integrity, and lead to substantial financial losses. These attacks often involve deceptive emails, messages, or websites that trick library staff and patrons into disclosing sensitive information or downloading malware onto library computers. Cybercriminals use manipulative tactics to exploit human vulnerabilities and gain unauthorized access to library systems and networks, sometimes through impersonation or pretexting. Ransomware poses a significant threat to libraries, emphasizing the

importance of robust cybersecurity measures and staff training to prevent and mitigate such attacks (Caverly, 2021). To protect against such attacks, institutions must implement robust cybersecurity measures, including regular software updates, managing end-of-life systems, data encryption, access administration, vulnerability scanning, risk assessments, testing, and incident response plans. Libraries need to invest in network security, intrusion detection systems, and staff training to combat phishing attempts and enhance overall cybersecurity. As cyberattacks continue to evolve, it is crucial for public institutions to prioritize cybersecurity to safeguard critical services and protect valuable knowledge repositories.

Cybersecurity threats pose significant risks to data integrity and patron privacy in libraries by exposing patron information to unauthorized third parties, compromising privacy, and undermining trust in library services. Data breaches can lead to identity theft, financial fraud, and harm the library's reputation. Encrypting library data can render it inaccessible, disrupting library operations and impeding access to essential resources and services (Li & Liu, 2021). Ransomware attacks pose significant risks to libraries, potentially leading to data loss if encrypted data cannot be recovered or if the ransom is not paid. Compromising staff credentials via phishing scams can grant cybercriminals unauthorized access to library systems, enabling them to steal sensitive information, deploy malware, or launch additional attacks. Social engineering tactics exploit human vulnerabilities, circumventing technical security measures and facilitating unauthorized entry into library systems and databases. These threats highlight the importance of robust cybersecurity practices and staff training to mitigate the risks associated with cyberattacks (Breeding, 2024).

To mitigate cybersecurity threats and enhance resilience, libraries can implement a range of strategies and best practices such as educating library staff about cybersecurity risks, best practices, and procedures for identifying and reporting suspicious activities can empower them to recognize and respond effectively to cyber threats. Implementing robust network security measures, such as firewalls, intrusion detection systems (IDS), and access controls, can help protect library systems and databases from unauthorized access and cyberattacks. Encrypting sensitive data stored on library systems and databases can safeguard patron privacy and prevent unauthorized access in the event of a data breach. Regularly updating software and firmware to patch known vulnerabilities can help mitigate the risk of exploitation by cybercriminals and enhance the overall security posture of library systems and networks. Developing and implementing incident response plans that outline procedures for detecting, containing, and mitigating cybersecurity incidents can help minimize the impact of cyberattacks on library operations and data integrity (Breeding, 2021).

Libraries can enhance their capacity to protect data integrity, preserve patron privacy, and maintain public trust in their services as trusted sources of information by prioritizing cybersecurity resilience and adopting proactive measures to address emerging threats. Collaboration with cybersecurity experts, information security professionals, and industry partners can further strengthen libraries' cybersecurity defenses and ensure the continued delivery of essential resources and services to their communities in the digital age. Cybersecurity in libraries is a critical aspect that requires attention to safeguard valuable digital collections and ensure the security of both the institution and its patrons. Libraries should collaborate with cybersecurity experts and form partnerships with specialized cybersecurity firms to develop robust cybersecurity frameworks tailored to their specific needs (Igbinovia & Ishola, 2023). Additionally, extending collaboration with other sectors, engaging with relevant government agencies, industry organizations, and cybersecurity companies can lead to innovative approaches and solutions for strengthening cybersecurity measures. Librarians play a crucial role in mitigating cyber threats by promoting research, collaboration, and information-sharing networks within the academic community (Aregbesola & Nwaolise, 2023). Encouraging further research and collaboration among academic libraries can lead to the development of workable cybersecurity frameworks and measures to mitigate risks and safeguard digital collections. Establishing a collaborative environment, sharing best practices, and fostering a culture of cybersecurity

awareness are essential steps for libraries to proactively protect against cyber threats and ensure the integrity of their services.

Misinformation and Disinformation

Misinformation refers to inaccurate or false information shared unwittingly, while disinformation involves the deliberate spread of false information with the intent to deceive. In the digital age, social media platforms and online forums have become fertile ground for the dissemination of misinformation and disinformation. These platforms amplify the reach and impact of false information, enabling it to spread rapidly and virally across vast networks of users. Malicious actors, including state-sponsored actors, political extremists, and profit-driven clickbait websites, exploit social media algorithms and echo chambers to target specific demographics and manipulate public opinion (Muhammed & Mathew, 2022). Social media platforms allow for rapid publication and peer-to-peer sharing, enabling ordinary users to quickly distribute information to large audiences with minimal oversight. Misinformation can often spread before it can be fact-checked and corrected. the combination of social media's structural features, psychological biases, and malicious actors' exploitation of these dynamics enables misinformation and disinformation to spread rapidly and widely online, with potentially serious consequences for public discourse and decision-making (Aimeur, Amri & Brassard, 2023).

Misinformation and disinformation have become pervasive in the digital age, fueled by the widespread use of social media platforms, online forums, and the deliberate efforts of malicious actors. This proliferation of false or misleading information poses significant challenges to achieving Sustainable Development Goals (SDGs) related to public health, environmental sustainability, and social cohesion. However, libraries are at the forefront of combating misinformation and disinformation through a variety of initiatives, including information literacy programs, fact-checking, and the promotion of critical thinking skills (Sullivan, 2019a). These efforts are crucial in achieving Sustainable Development Goals related to public health, environmental sustainability, and social cohesion. Libraries have been actively contributing to the fight against misinformation and disinformation by offering a framework to analyze the credibility of online sources, scientific or not. They have been providing information and media literacy programs for decades, which have transformed into online digital information literacy sessions (Bagani, 2021). These programs empower individuals with the knowledge to identify their own biases, analyze the source of an online scientific article or piece of news, and think twice before sharing or citing it. The role of public libraries in countering misinformation is multifaceted. They seek to oppose all forms of false information, including rumors, post-truth, confirmation bias, and echo chambers. Public libraries aim to promote information literacy and combat misinformation within their communities, fostering an informed populace and preserving democratic values (Andermann, 2023). The field of librarianship can help combat the epidemic of fake news by emphasizing the importance of information literacy and critical thinking. Libraries walk a fine line in addressing vaccine misinformation, reflecting the need for a nuanced approach to combating misinformation. Academic libraries, in particular, are battling against the fake news wave by teaching information literacy and using evaluation criteria to identify fake news (Paor & Heravi, 2020).

Misinformation about health topics, such as vaccines, COVID-19 treatments, and alternative medicine, can undermine public trust in scientific expertise and evidence-based interventions. This can lead to vaccine hesitancy, reduced uptake of preventive healthcare measures, and increased vulnerability to disease outbreaks and pandemics. A study found that a small minority of crowdfunding campaigns on GoFundMe explicitly sought funding for alternative COVID-19 treatments and opposition to public health interventions like masking. Over half of these campaigns contained verified false information about COVID-19 (Shaw, Hakam, Lui, Abbasi, Sudhakar, Leapman & Breyer, 2022). Another review synthesized evidence showing that misinformation about complementary and alternative medicine (CAIM) related to COVID-19 that spreads on social media can prompt unsafe and harmful behaviors (Ng, Liu, Maini, Pereira, Cramer & Moher, 2023).

Healthcare professionals reported that the spread of misinformation regarding alternative COVID-19 treatments affected their credibility and relationship with patients. Many were extremely concerned about the impact on trust in the medical profession. YouTube has policies prohibiting medical misinformation that contradicts local health authorities, promotes harmful substances as treatments, or denies the contagious nature of COVID-19 (Coman, Bulara, Repanovici & Rogozea, 2022).

Misinformation about climate change, environmental policies, and sustainable practices can indeed distort public perceptions and hinder efforts to address urgent environmental challenges. This misinformation, whether intentional (disinformation) or unintentional (misinformation), can impede the transition to renewable energy, undermine conservation efforts, and exacerbate the impacts of climate change on vulnerable communities and ecosystems. The spread of inaccurate information, whether due to genuine misunderstanding or deliberate falsehoods, can have negative implications for climate policy, delay urgent adaptation, and polarize public support for climate action. It is crucial to address climate misinformation urgently and decisively, as it can delay real climate action and create obstacles to meaningful progress in combating climate change. Misinformation and disinformation can fuel social divisions, polarize public discourse, and erode trust in democratic institutions and processes. This can undermine social cohesion, exacerbate political polarization, and increase the risk of social unrest and conflict, undermining efforts to promote peace, justice, and inclusive societies (Welle, 2024; Sethi, 2024; Tekisalp, 2022).

Libraries play a critical role in combating misinformation and promoting information literacy, critical thinking, and evidence-based reasoning. Libraries offer information literacy programs that teach patrons how to critically evaluate sources, discern fact from fiction, and navigate the digital information landscape responsibly. These programs empower individuals to become informed, discerning consumers of information and equip them with the skills to identify and combat misinformation. Libraries partner with fact-checking organizations and media literacy experts to verify the accuracy of information and debunk false claims. Libraries play a crucial role in promoting fact-checking initiatives to combat misinformation and provide patrons with reliable information. They offer educational resources, workshops, and interactive exhibits that enhance critical thinking skills. Through these efforts, libraries empower individuals to question assumptions, challenge biases, and evaluate evidence critically, enabling them to engage with information effectively, resist manipulation, and make informed decisions in today's complex information landscape (Paor & Heravi, 2020). Libraries can play a crucial role in promoting information literacy, countering disinformation, and achieving the Sustainable Development Goals by utilizing their position as reliable information sources and community centers. Libraries enable people to responsibly navigate the digital information ecosystem, separate fact from fiction, and make a positive impact on a more resilient, inclusive, and educated society by forming cooperative collaborations with educational institutions, media literacy advocates, and community-based groups (Young, Boyd, Yefimova, Wedlake, Coward & Hapel, 2021).

Privacy Concerns and Surveillance

Libraries have a fundamental responsibility to protect patron privacy and intellectual freedom, which can be challenging in the face of increasing data collection, government surveillance, and evolving data protection regulations. Patron privacy is a core value of the library profession, as it enables users to freely access information without fear of judgment or consequences (IFLA, 2015). However, libraries today collect and store vast amounts of patron data, from personally identifiable information to borrowing histories, which can be vulnerable to breaches by bad actors. To safeguard patron privacy, libraries should implement robust security measures like data encryption, secure servers, and strict access controls. Regular staff training on privacy best practices and having a comprehensive data breach response plan in place are also crucial. Libraries should obtain informed consent from patrons before collecting personal data, clearly explaining how it will be used. Whenever possible, patron data should be anonymized or pseudonymized to protect

individual identities (Malikowski, 2022). Government surveillance programs pose serious threats to intellectual freedom and access to information, particularly in authoritarian regimes. Libraries should reject any illegitimate monitoring or collection of patron data that would compromise privacy and affect the right to seek, receive and impart information. While some government access to user data may be unavoidable, it should be based on legitimate principles and be necessary and proportionate to legitimate aims. Libraries should support national and international advocacy efforts to protect individuals' privacy and digital rights. They should also educate patrons about data protection and provide guidance on using tools to safeguard their privacy. Ultimately, libraries must continue exploring and adapting robust measures to prevent unauthorized access and breaches, ensuring patrons' trust remains steadfast

Surveillance technologies, including closed-circuit television (CCTV) cameras, facial recognition systems, and data analytics tools, raise ethical concerns about privacy invasion and individual autonomy. The widespread adoption of these technologies in public spaces, including libraries, has sparked debates about the ethical use of surveillance and its impact on intellectual freedom. Moreover, data collection practices, such as tracking patrons' online activities and collecting personal information for targeted advertising, raise concerns about consent, transparency, and user control over their data. Ethical use of surveillance tech requires balancing security needs with privacy rights and intellectual freedom. Careful consideration of the societal impacts is critical before deploying these powerful tools (Almeida, Shmarko & Lomas, 2022). Libraries face significant challenges in balancing the need to protect patron privacy with compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the Children's Online Privacy Protection Act (COPPA) in the United States. While libraries have a duty to safeguard patron information and uphold intellectual freedom, they must also navigate legal and regulatory requirements related to data collection, retention, and sharing. This often involves implementing privacy-enhancing technologies, such as encryption and anonymization, and adopting data protection policies and procedures to ensure compliance with applicable laws and regulations (Ashikuzzaman, 2023b; ALA, 2020a).

Government surveillance programs indeed pose a significant threat to freedom of expression and access to information, especially in authoritarian regimes where dissent is suppressed. These surveillance technologies, such as mass surveillance, internet censorship, and content filtering, enable governments to monitor and control citizens' online activities, leading to the suppression of dissenting voices and the restriction of access to politically sensitive or subversive information. This undermines intellectual freedom, democracy, and human rights, stifling the free exchange of ideas and information crucial for a vibrant and informed society. Surveillance technologies, including monitoring, intercepting, and collecting communications data, infringe on the right to privacy and freedom of expression. They create a chilling effect, prompting self-censorship and inhibiting political participation. Human rights defenders, journalists, and political activists are particularly vulnerable to surveillance and censorship, impacting their ability to challenge human rights abuses and maintain transparency. The fear of surveillance can lead to self-censorship and deter individuals from accessing information, affecting the right to form opinions without interference. Additionally, surveillance undermines the essence of privacy and fundamental freedoms, necessitating clear legal frameworks and oversight to prevent abuse (Masferrer, 2023).

Libraries and information institutions face intricate challenges regarding privacy concerns and surveillance, necessitating a thorough examination of ethical, legal, and societal impacts. Prioritizing patron privacy, safeguarding intellectual freedom, and advocating for policies that uphold privacy rights and endorse transparency and accountability in surveillance practices are crucial steps for libraries to safeguard democracy, human rights, and the free exchange of ideas and information in the digital era. The erosion of privacy protections and the rise of surveillance, particularly by library vendors like RELX and Thomson Reuters, pose significant threats to user privacy within academic

institutions. The involvement of vendors in surveillance activities contradicts libraries' core values and raises concerns about the ethical collection and use of data. Libraries must address the ethical dilemmas surrounding data collection, storage, usage, and destruction transparently to protect user privacy and uphold their commitment to intellectual freedom (ALA, 2019). Libraries considering surveillance equipment installation must weigh the necessity against the potential privacy implications, ensuring strong policies are in place to protect user confidentiality and limit data retention. The use of surveillance equipment should be strictly for enhancing physical security, with clear protocols for data storage, destruction, and confidentiality protection. Additionally, libraries should refrain from monitoring user activities for inappropriate or illegal behavior without proper legal authorization or user consent (Avuglah, Owusu-Ansah, Tachie-Donker & Yeboah, 2020).

In the digital age, where technology can aggregate personal information and track online behaviors, libraries must navigate the balance between technological benefits and privacy concerns. The study highlights the overwhelming concern among librarians and students regarding online privacy, emphasizing the need to protect personal information from unauthorized access and surveillance. Libraries can mitigate the risks associated with surveillance capitalism and protect user privacy in online environments by incorporating privacy literacy into library practices, educating users, and advocating for privacy rights (Hartman-Caverly & Chisholm, 2023). The International Federation of Library Associations and Institutions (IFLA) emphasizes the critical role of libraries in safeguarding privacy rights and freedom of expression in the face of increasing data collection and surveillance practices. Excessive data collection poses threats to individual privacy, freedom of speech, and democracy, underscoring the importance of privacy as a fundamental human right that libraries must uphold to preserve intellectual freedom and civil engagement (IFLA, 2015). Libraries can adopt several strategies to protect patron privacy and intellectual freedom while addressing the challenges posed by surveillance and data collection practices by developing and implementing comprehensive privacy policies and procedures that outline the library's commitment to protecting patron privacy and complying with data protection regulations. Invest in privacy-enhancing technologies, such as encryption, anonymization, and secure communication tools, to safeguard patron information and mitigate the risks of surveillance and data breaches. Advocate for policies and legislation that protect privacy rights, promote transparency, and ensure accountability in government surveillance practices. Educate patrons about privacy risks and digital surveillance, empowering them to make informed decisions about their online activities and data sharing practices.

Case Studies and Best Practices

Libraries encounter various digital threats that can compromise data security and patron privacy. These threats include hacking, cracking, malware, misuse, errors, and data leakage. Understanding these threats is essential for libraries to protect sensitive information and ensure secure access to resources. Meanwhile, case studies provide crucial insights into real-world examples of digital threats faced by libraries and their impact on achieving Sustainable Development Goals (SDGs). Analyzing these cases and the best practices implemented by libraries to counter digital threats, safeguard patron privacy, and enhance inclusive access to information and technology, valuable lessons can be gleaned for broader application across various settings. The London Public Library and the British Library in the United Kingdom have both experienced cyberattacks. The London Public Library had to shut down most of its services due to a cyberattack, affecting its branches and digital resources. On the other hand, the British Library faced a ransomware attack that led to a prolonged IT outage, with hackers demanding a ransom and leaking private information when the library refused to pay. Additionally, the Toronto Public Library in Canada was also hit by a ransomware attack, compromising employee information and causing operational disruptions. These incidents highlight the vulnerability of libraries to cybercrime and the significant impact such attacks can have on their operations and users.

Cybersecurity Breach at British Library

The British Library fell victim to a severe ransomware attack orchestrated by the Rhysida gang, resulting in the theft of 600GB of data, including sensitive information about staff, users, authors, and textual collections. This cyberattack disrupted the library's IT infrastructure for six months, causing extensive damage to servers, databases, and network systems. The attack methods employed by Rhysida included targeted attacks on specific network drives, keyword scanning for sensitive files, and hijacking native utilities to create backup copies of databases. The impact of the attack led to delays in payments to writers and translators, suspension of fellowship programs, and the library's computerized catalog being offline for months. The British Library's reliance on aging legacy applications and complex network topology exacerbated the impact of the attack. Legacy systems were unable to be restored due to technical obsolescence and lack of vendor support. This situation highlights the challenges organizations face when dealing with outdated systems that lack modern support and infrastructure. The inability to restore legacy systems due to technical obsolescence and the absence of vendor support can significantly impede recovery efforts and increase vulnerability to cyber threats. The attack highlighted the importance of maintaining current infrastructure and implementing modern security controls to reduce vulnerabilities. The library's historically complex network topology allowed attackers wider access than would have been possible in a more modern design. Older defensive software on the library's servers was unable to resist the attack. The British Library's response to the attack, characterized by transparency and cooperation with authorities, has been commended by the UK's National Cyber Security Centre (Middleton, 2024; Scroxton, 2024b; Martin, 2024).

The cyberattack method used by the Rhysida gang against the British Library involved various tactics. They utilized defense evasion, anti-forensics, data exfiltration for ransom, encryption for impact, and server destruction to hinder recovery efforts. The Rhysida ransomware group, known for its double extortion model, targeted the British Library in a cyberattack that caused significant disruption, including stealing and auctioning off data, impacting services, and leaking internal documents. The attack exploited vulnerabilities like ZeroLogon and used phishing and stolen credentials to access victims' networks. The group operated on a ransomware-as-a-service (RaaS) model and engaged in double extortion, demanding ransom payments in Bitcoin. The attack led to a major technology outage at the British Library, affecting its computer systems, website, phone network, and public wireless network, with services remaining disrupted for weeks. The British Library responded by providing updates, confirming the ransomware nature of the attack, and taking protective measures to safeguard its systems and data. The incident highlighted the importance of cybersecurity preparedness and transparency in the face of evolving cyber threats (Scroxton, 2024a; Jones, 2023; Hill, 2023).

The British Library initiated a Rebuild & Renew program to coordinate long-term recovery efforts, focusing on enhancing network design, implementing cloud computing solutions, and establishing role-based access control for improved security. This program aims to redevelop the IT infrastructure in a resilient and secure way, aligning with the library's Knowledge Matters strategy and modernizing its technology estate, which includes many legacy systems. The library is expected to rely more on cloud-based technologies, with current email, finance, HR, payroll, and physical security systems already being cloud-based and largely unaffected by the attack. The Rebuild & Renew program includes significant changes to applications, culture, policies, and processes to reduce the impact of future attacks, embed security across the IT lifecycle, and enhance resilience against cyber threats (Jones, 2024). Despite the challenges posed by the cyberattack, the British Library sees an opportunity to transform its technology management practices, ensuring better preparedness for future incidents while maximizing the benefits of technological advancements. The library's transparency in reporting the attack and commitment to implementing necessary changes reflect its dedication to serving the public interest.

The London Public Library Cybersecurity Breach

The London Public Library has made significant progress in recovering from a ransomware attack that

occurred on December 13. The attack forced the library to temporarily close some branches and affected various services, including its website, catalogue, and internal network. However, the library did not pay a ransom to the hackers and has managed to restore most of its services, including access to its online catalogue and digital services like OverDrive and audiobook platforms. The library's CEO, Michael Ciccone, stated that they are "almost fully recovered" from the attack, with the only remaining issue being the finalization of some coding details for the website (Trevithick, 2024). The attack compromised the personal information of some library staff members, but the full extent of the data stolen is not yet known. The library has worked with police to investigate the incident and has fulfilled its obligations with the Information and Privacy Commissioner of Ontario. The cost of mitigating the impacts of the ransomware attack and shoring up its defenses against future ones is significant, but the exact amount has not been disclosed (Greig, 2023a). The incident highlights the importance of cybersecurity for public institutions like libraries, which are increasingly targeted by hackers. The British Library also recently experienced a major cyberattack, underscoring the need for libraries to implement robust security measures to protect their systems and data. Best practices in responding to such incidents include transparency and communication with the public, engaging cybersecurity experts, providing alternative services to minimize disruption, and refusing to pay ransom to hackers.

The London Public Library's response to a cyberattack highlights the significance of resilience, transparency, and investment in cybersecurity to protect critical services and patron information. This incident underscores the importance of proactive measures to mitigate cyber risks effectively, not only for libraries but also for other public institutions worldwide. The London Public Library demonstrated resilience by refusing to pay any ransom to the hackers behind the cyberattack. This decision not only adheres to ethical principles but also prevents incentivizing future attacks. The library's ability to nearly fully recover without succumbing to ransom demands highlights the importance of preparedness and recovery strategies. The library promptly communicated with the public about the cyber incident, keeping them informed about the situation and the steps taken for recovery. Transparent communication builds trust with patrons and stakeholders, enhancing their confidence in the library's ability to manage crises effectively. The cyberattack underscores the importance of investing in robust cybersecurity infrastructure to prevent and mitigate future incidents. Libraries, like other public institutions, must allocate resources to enhance their cybersecurity posture, including updating systems, implementing security protocols, and training staff on cybersecurity best practices. Despite the disruption caused by the cyberattack, the London Public Library prioritized the restoration of essential patron services, such as access to public computers and printers. This focus on meeting patrons' needs demonstrates the library's commitment to serving the community even during challenging times. These lessons can inform cybersecurity strategies for libraries and other public institutions worldwide, emphasizing the proactive measures needed to mitigate cyber risks effectively (Rivers, 2024).

Toronto Public Library Cyberattack

The aftermath of the ransomware attack on the Toronto Public Library was a challenging time for both staff and patrons. The attack, which occurred on October 28, 2023, disrupted the library's services for months, affecting the ability of patrons to access online accounts, use computers, and process returns. Despite these challenges, the library managed to keep its 100 branches open and host programs, albeit with limitations. The attack not only encrypted files but also led to the theft of employee data, including sensitive information like social insurance numbers and government-issued identification documents. During the ordeal, employees like Domenic Lollino worked tirelessly to address the backlog of books, with a million items awaiting processing. The library resorted to analog workarounds, such as pen and paper, to continue providing essential services to the community. This dedication to maintaining operations and serving the public, even in the face of a cyber crisis, highlights the library's commitment to its patrons and the community at large. Despite the challenges posed by the cyberattack, the Toronto Public Library's efforts to restore services and uphold its mission of providing

access to information and resources demonstrate resilience and a strong sense of public service (Enis, 2024; Bridge & Zoledziowski, 2024).

The attack not only disrupted essential services but also underscored the critical role libraries play in providing access to resources, particularly for underserved populations. It's concerning that such vital institutions are targeted by cybercriminals, highlighting the broader issue of cybersecurity vulnerabilities faced by organizations worldwide. The library's response to the incident, including engaging cybersecurity experts to assess and mitigate the situation, is a crucial step in restoring normal operations and preventing future attacks. However, the lengthy recovery process and the need to bring everything back in a way that allows it to prevent future attacks underscore the complexity and seriousness of the attack. The incident also raises concerns about the impact on vulnerable populations, such as low-income city residents and school children, who rely on the library as their primary source of internet access. The loss of access to technology for these individuals has been especially challenging and concerning, highlighting the critical role libraries play in bridging the digital divide. The decision not to pay the ransom and instead rebuild the systems reflects a principled stance against financing future attacks, although it comes with its own set of challenges, including the ongoing investigation into the extent of the data breach. The theft of employee data adds another layer of complexity and underscores the need for robust cybersecurity measures to protect sensitive information. The library's eventual restoration of services is a testament to resilience in the face of adversity. As they continue to recover and adapt, it's crucial for organizations and individuals alike to remain vigilant against the ever-evolving threat of cyberattacks (Lee, 2023; Creig, 2023b).

Conclusion

This review has underscored the critical role of libraries in addressing digital threats and advancing Sustainable Development Goals (SDGs) in the digital age. Libraries serve as essential community hubs, providing access to information, promoting digital literacy, and safeguarding patron privacy. However, they face increasingly complex challenges, including cybersecurity threats, misinformation, and digital divides, which can hinder progress towards achieving the SDGs. Key findings from this review highlight the importance of collaborative efforts among stakeholders to build resilient and inclusive information ecosystems. Libraries cannot address digital threats alone; it requires partnerships and collective action from policymakers, government agencies, international organizations, civil society, and the private sector. Stakeholders may support libraries in their goal to promote digital inclusion, protect patron privacy, and advance the SDGs by cooperating and utilizing their networks, knowledge, and resources.

Moving forward, it is imperative to prioritize investments in digital infrastructure, cybersecurity training, and information literacy programs to enhance the resilience of libraries and empower individuals, communities, and societies to thrive in the digital age. Stakeholders can create a more equitable and sustainable future where everyone has access to technology, knowledge, and opportunities for both individual and group progress by highlighting the value of cooperative efforts. In the digital age, libraries are beacons of knowledge, equity, and empowerment. Through collective action and shared commitment, we can harness the transformative potential of libraries to address digital threats, promote digital inclusion, and advance progress towards a more just, equitable, and sustainable world for all.

Policy Implications and Recommendations

Policy implications and recommendations are crucial for addressing digital threats to libraries and supporting their role in advancing Sustainable Development Goals (SDGs). Policymakers, government agencies, and international organizations play a pivotal role in shaping the regulatory framework, allocating resources, and fostering collaboration to safeguard libraries and promote digital inclusion. The following recommendations outline key policy actions to address digital threats, enhance the resilience of libraries, and advance the SDGs:

1. Policymakers should prioritize investments in digital infrastructure, including broadband connectivity, computer hardware, and software

systems, to ensure that libraries have the necessary resources to deliver digital services and resources to their communities.

2. Government agencies should allocate resources for cybersecurity training programs tailored to the needs of library staff. These programs should cover topics such as threat awareness, incident response, and best practices for safeguarding patron privacy and data integrity.
3. Policymakers should support the development and implementation of information literacy programs in libraries, aimed at empowering patrons with the skills to critically evaluate information, navigate digital platforms, and protect their privacy online.
4. Government agencies should invest in digital skills training initiatives that equip individuals with the technical skills and confidence to leverage digital technologies for personal and professional growth. These programs should target underserved communities, including rural areas, low-income neighborhoods, and marginalized populations.
5. Policymakers should advocate for the development of international standards and guidelines for protecting patron privacy in libraries. These standards should outline best practices for data collection, retention, and sharing, as well as mechanisms for ensuring transparency, accountability, and user consent.
6. International organizations should collaborate with libraries, media literacy experts, and fact-checking organizations to develop guidelines for combating misinformation and promoting ethical use of digital technologies. These guidelines should emphasize the importance of media literacy education, fact-checking initiatives, and collaborative approaches to addressing misinformation.
7. Policymakers, libraries, academia, and civil society organizations should collaborate to share knowledge, resources, and best practices for addressing digital threats and advancing the SDGs. This collaboration should involve regular dialogue, partnerships, and information sharing to foster innovation and collective action.
8. International organizations should facilitate networking opportunities and knowledge exchange among libraries and information institutions worldwide. Platforms such as conferences, workshops, and online forums can serve as forums for sharing experiences, lessons learned, and innovative solutions for addressing digital threats and promoting digital inclusion.
9. Libraries, professional associations, and advocacy groups should engage in policy advocacy campaigns to raise awareness about the importance of libraries in advancing the SDGs and the need for policy support to address digital threats. These campaigns should target policymakers, government agencies, and the general public to garner support for investments in library infrastructure, cybersecurity, and information literacy.
10. Governments should launch public awareness campaigns to educate citizens about the risks of digital threats, such as cyberattacks, data breaches, and misinformation. These campaigns should empower individuals to take proactive steps to protect their privacy, secure their digital devices, and critically evaluate information online.

Reference

ACT-IAC (2019). *Advancing data driven decision-making in the public sector: Guidance for implementing the foundations for evidence-based policymaking act and the federal data strategy action plan*. USA: American Council for Technology and Industry Advisory Council. https://www.actiac.org/system/files/Data%20Driven%20Decision%20Making%20Report.pdf

Afzal, A., Khan, S., Daud, S., Ahmad, Z., & Butt, A. (2023). Addressing the Digital Divide: Access and Use of Technology in Education. *Journal of Social Sciences Review*, 3(2), 883–895. https://doi.org/10.54183/jssr.v3i2.326

Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation and misinformation in social media: A review. *Social Network Analysis and Mining*, 13(1), 30. https://doi.org/10.1007/s13278-023-01028-5

ALA (2019, July 29). *Privacy and Confidentiality Q&A*. Chicago: American Library Association. https://www.ala.org/advocacy/intfreedom/privacyconfidentialityqa

ALA (2020b). *Media literacy in library*. USA: Institute of Museum and Library Services. https://www.ala.org/sites/default/files/tools/content/%21%20FINAL%20Media-Lit_Prac-Guide_WEB_040521.pdf

ALA (2020a, January 26). *Library privacy guidelines for data exchange between networked devices and services*. Chicago: American Library Association. https://www.ala.org/advocacy/privacy/guidelines/dataexchange

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 2(3), 377–387. https://doi.org/10.1007/s43681-021-00077-w

Alojail, M. & Khan, S.B. (2023). Impact of Digital Transformation toward Sustainable Development. *Sustainability*, 15, 14697. https://doi.org/10.3390/su152014697

Andermann, B.H. (2023). *The role of public libraries in countering misinformation: A Swedish perspective.* A master thesis submitted to the Department of Library and Information Science, Faculty of Librarianship, Information, Education and IT, University of Boras. https://hb.diva-portal.org/smash/get/diva2:1808239/FULLTEXT01.pdf

Aregbesola, A. & Nwaolise, E.L. (2023). Securing digital collections: Cyber Security best practices for academic libraries in developing countries. *Library Philosophy and Practice (ejournal).* 7822. https://digitalcommons.unl.edu/libphilprac/7822

Ashikuzzaman, M. (2023b, November 22). *Read-Write-Defend: A guide to cybersecurity in modern libraries*. Library and Information Science Network. https://www.lisedunetwork.com/a-guide-to-cybersecurity-in-modern-libraries/

Ashikuzzaman, M. (2023a, September 14). *Safeguarding patron privacy: Libraries' approach to data security*. Library and Information Science Network. https://www.lisedunetwork.com/safeguarding-patron-privacy-libraries-approach-to-data-security/

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A., & Akin, E. A. (2023). Comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12, 1333. https://doi.org/10.3390/electronics12061333

Avuglah, B., Owusu-Ansah, C., Tachie-Donkor, G., & Yeboah, E. (2020). Privacy Issues in Libraries with Online Services: Attitudes and Concerns of Academic Librarians and University Students in Ghana. *College & Research Libraries*, 81(6), 997. https://doi.org/10.5860/crl.81.6.997

Azzahra, N. F. & Amanta, F. (2021). *Promoting Digital Literacy Skill for Students through Improved School Curriculum.* Policy Brief, No. 11, Center for Indonesian Policy Studies (CIPS), Jakarta. https://www.econstor.eu/bitstream/10419/249444/1/CIPS-PB11.pdf

Bangani S. (2021). The fake news wave: Academic libraries' battle against misinformation during COVID-19. *Journal of Academic Librarianship*, 47(5), 102390. https://doi.org/10.1016/j.acalib.2021.102390

Bogdan-Martin, D. & Steiner, A. (2023). *SDG digital acceleration agenda*. International Telecommunication Union and United Nations Development Programme. https://www.undp.org/sites/g/files/zskgke326/files/2023-09/SDG%20Digital%20Acceleration%20Agenda_2.pdf

Bradley, F. (2014). *How libraries contribute to sustainable development and the SDGs*. International Federation of Library Associations and Institutions. https://www.ifla.org/wp-content/uploads/2019/05/assets/alp/103-fbradley-alp.pdf

Breeding, M. (2021). How to secure library systems from malware, ransomware, and other cyberthreats. *Computer Libraries*, 42(1). https://www.infotoday.com/cilmag/jan22/Breeding--How-to-Secure-Library-Systems-From-Malware-Ransomware-and-Other-Cyberthreats.shtml

Breeding, M. (2024). The systems librarian: Libraries under cyberattack. *Computer Libraries*, 44(2). https://www.infotoday.com/cilmag/mar24/Breeding--Libraries-Under-Cyberattack.shtml

Bridge, S. & Zoledziowski, A. (2024, February 27). *1 million books and 4 months later, Toronto's library recovers from a cyberattack*. Canada: CBC. https://www.cbc.ca/news/canada/toronto/toronto-library-ransomware-recovery-1.7126412

British Library (2024, March 8). *Learning lessons from the cyber-attack: British Library cyber incident review*. UK: British Library. https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf

Caverly, W. (2021, May 10). *Ransomware attacks at libraries: How they happen, what to do*. Chicago: Public Library Association. https://publiclibrariesonline.org/2021/05/ransomware-attacks-at-libraries-how-they-happen-what-to-do/

Chao, K., Sarker, M. N. I., Ali, I., Firdaus, R. B. R., Azman, A., & Shaed, M. M. (2023). Big data-driven public health policy making: Potential for the healthcare industry. *Heliyon*, 9(9), e19681. https://doi.org/10.1016/j.heliyon.2023.e19681

Coman, C., Bularca, M. C., Repanovici, A. & Rogozea, L. (2022). Misinformation about medication during the COVID- 19 pandemic: A perspective of medical staff. *PloS One*, 17(10), e0276693. https://doi.org/10.1371/journal.pone.0276693

Corrado, E. M. (2020). Libraries and protecting patron privacy. *Technical Services Quarterly*, 37(1), 44–54. https://doi.org/10.1080/07317131.2019.1691761

Creig, J. (2023b, December 21). Toronto Public Library 'remains a crime scene' after ransomware attack. The Record Recorded

Future News. https://therecord.media/toronto-public-library-remains-crime-scene

Dabbous, A., Barakat, K.A. & Kraus, S. (2023). The impact of digitalization on entrepreneurial activity and sustainable competitiveness: A panel data analysis. *Technology in Society*, 73, 102224. https://doi.org/10.1016/j.techsoc.2023.102224.

Enis, M. (2024, January 17). *Toronto public library recovers from ransomware attack*. Library Journal. https://www.libraryjournal.com/story/toronto-public-library-recovers-from-ransomware-attack

Fallah-Shayan, N., Mohabbati-Kalejahi, N., Alavi, S. & Zahed, M.A. (2022). Sustainable Development Goals (SDGs) as a framework for corporate social responsibility (CSR). *Sustainability*, 14, 1222. https://doi.org/10.3390/su14031222

Greig, J. (2023a, December 15). *Ontario Public Library shuts down most services due to cyberattack*. The Record Recorded Future News. https://therecord.media/ontario-public-library-shuts-down-services

Hai, T.N., Van, Q.N. & Tuyet, M.N. (2021). Digital Transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic. *Emerging Science Journal*, 5, 21-36. http://dx.doi.org/10.28991/esj-2021-SPER-03

Hartman-Caverly, S. & Chisholm, A. (2023). *Practicing privacy literacy in academic libraries: Theories, methods, and cases*. Chicago: ACRL. https://alastore.ala.org/content/practicing-privacy-literacy-academic-libraries-theories-methods-and-cases

Heeks, R. (2022). Digital inequality beyond the digital divide: conceptualizing adverse digital incorporation in the global South. *Information Technology for Development*, 28(4), 688–704. https://doi.org/10.1080/02681102.2022.2068492

Hill, M. (2023, November 11). *Rhysida ransomware group claims crippling British Library cyberattack: British Library continues to experience a major technology outage due to a disruptive cyberattack*. Cybersecurity Hub. https://www.cshub.com/attacks/news/rhysida-ransomware-group-claims-crippling-british-library-cyber-attack

Hossin, M. A., Du, J., Mu, L., & Asante, I. O. (2023). Big Data-Driven public policy decisions: Transformation toward smart governance. *Sage Open*, 13(4). https://doi.org/10.1177/21582440231215123

Hoving, S. (2023. August 30). *5 ways to shield your library from cybercrime — advice from the experts*. Germany: Springer Nature. https://www.springernature.com/gp/librarians/the-link/blog/blogposts-resources/shield-your-library-from-cybercrime-tips-from-the-experts/25946990

IASS (2021, April 7). *The opportunities and risks of digitalization for sustainable development*. Germany: Institute for Advance Sustainability Studies. https://phys.org/news/2021-04-opportunities-digitalization-sustainable.html

Ibrahim, H.O. & Umar, F.A. (2023). Cybersecurity threats and its emerging trends on academic libraries. *International Journal of Academic Library and Information Science*, 8(2), 22-26. https://academicresearchjournals.org/IJALIS/PDF/2020/March/Ibrahim%20and%20Umar.pdf

IFLA (2015). *IFLA statement on privacy in the library environment*. International Federation of Library Associations and Institutions. https://www.ifla.org/wp-content/uploads/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf

Igbinovia, M., & Aiyebelehin, A. J. (2023). Libraries as facilitators of digital inclusion for sustainable development: The Nigerian experience. *Folia Toruniensia*, 23, 53–73. https://doi.org/10.12775/FT.2023.003

Igbinovia, M.O. & Ishola, B.C. (2023). Cyber security in university libraries and implication for library and information science education in Nigeria. *Digital Library Perspectives*, 39(3), 248-266. https://doi.org/10.1108/DLP-11-2022-0089

Jones, C. (2023, November 20). *Rhysida ransomware gang: We attacked the British Library*. The Register, Situation Publishing. https://www.theregister.com/2023/11/20/rhysida_claims_british_library_ransomware/

Jones, C. (2024, March 11). *British Library pushes the cloud button, says legacy IT estate cause of hefty rebuild: Five months in and the mammoth post-ransomware recovery has barely begun*. The Register, Situation Publishing. https://www.theregister.com/2024/03/11/british_library_slaps_the_cloud/

Kala, E.S.M. (2023) Challenges of technology in African countries: A case study of Zambia. *Open Journal of Safety Science and Technology*, 13, 202-230. https://doi.org/10.4236/ojsst.2023.134011

Kumar, N., Sai, K.H., Hordiichuk, V., Menon, R., Aarthy, C.J., Saha, G.C. & Balaji, K. (2023). Harnessing the power of Big Data: Challenges and opportunities in analytics. *Journal of Propulsion*, 44(2), 363-371. http://dx.doi.org/10.52783/tjjpt.v44.i2.193

Kumarasinghe, N., Gerard, J. & Ventimiglia, A. (2022*). Lessons learned on leveraging digital transformations to meet the SDGs: Joint submission by Future Earth Canada & sustainability in the digital age*. United Nations, SDGs. https://sdgs.un.org/sites/default/files/2023-05/B4%20-%20Future%20Earth%20-%20Leveraging%20digital%20transformations%20to%20meet%20the%20SDGs.pdf

Lannucci, L. (2024, April 19). *Media literacy and misinformation: Getting started*. New Jersey: Monmouth University, Guggenheim Memorial Library. https://guides.monmouth.edu/media_literacy

Lee, T. (2023, October 31). *Toronto Public Library faces disruptions due to cyberattack*. Kepler Safe. https://keplersafe.com/toronto-public-library-faces-disruptions-due-to-cyberattack/

Li, Y. & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126.

Lupton, A. (2023, December 15). *2 experts explain why libraries can become cybercrime targets*. Canada: CBC. https://www.cbc.ca/news/canada/london/2-experts-explain-why-libraries-can-become-cybercrime-targets-1.7059002

Malikowski, M. (2022, April 21). *Protecting patron data: What librarians can do*. Massachusetts Libraries. https://masslibsystem.org/blog/2022/04/21/protecting-patron-data-what-librarians-can-do/

Manzoor, M. & Vimarlund, V. (2018). Digital technologies for social inclusion of individuals with disabilities. *Health and Technology*, 8(5), 377–390. https://doi.org/10.1007/s12553-018-0239-1

Martin, A. (2024b, March 18*). British Library hailed by UK cyber agency for its response to ransomware attack*. The Record from Record Future News. https://therecord.media/british-library-incident-response-uk-ncsc-praise

Masferrer A. (2023). The decline of freedom of expression and social vulnerability in Western democracy. *International Journal for the Semiotics of Law = Revue Internationale De Semiotique Juridique*, 1–33. Advance online publication. https://doi.org/10.1007/s11196-023-09990-1

Mendez-Dominguez, P., Munoz, D.C., Diez, E.R. & De-Mesa, J.C. (2023). Digital inclusion for social inclusion. Case study on digital literacy. *Frontier in Communication*, 8, 1191995. https://doi.org/10.3389/fcomm.2023.1191995

Meyer, V. & Zimmermann, F. (2022, December 6). *Fighting mis- and disinformation: 7 steps for development communicators.* The SDG communicator. https://sdg-communicator.org/2022/12/06/fighting-mis-and-disinformation-7-steps-for-development-communicators/

Middleton, C. (2024, March 15). *The British Library looks to the future as it reveals the incalculable damage of its ransomware attack*. Diginomica Limited. https://diginomica.com/british-library-looks-future-it-reveals-incalculable-damage-its-ransomware-attack

Mokhtari, F. (2023). Fostering Digital Literacy in Higher Education: Benefits, Challenges and Implications. *International Journal of Linguistics, Literature and Translation*, 6(10), 160–167. https://doi.org/10.32996/ijllt.2023.6.10.19

Mondejar, M.E., et al. (2021). Digitalization to achieve sustainable development goals: Steps towards a Smart Green Planet. *Science of the Total Environment*, 794, 148539. https://doi.org/10.1016/j.scitotenv.2021.148539

Muhammed T, S., & Mathew, S. K. (2022). The disaster of misinformation: A review of research in social media. *International Journal of Data Science and Analytics*, 13(4), 271–285. https://doi.org/10.1007/s41060-022-00311-6

Munyoka, W. (2022). Inclusive digital innovation in South Africa: Perspectives from disadvantaged and marginalized communities. *Sustainability*, 14(9), 5372. https://doi.org/10.3390/su14095372

Ng, J.Y., Liu, S., Maini, I., Pereira, W., Cramer, H. & Moher, D. (2023). Complementary, alternative, and integrative medicine-specific COVID-19 misinformation on social media: A scoping review. *Integrative Medicine Research*, 12(3), 100975. https://doi.org/10.1016/j.imr.2023.100975.

Oladokun, B., Yemi-Peters, O.E. & Owolabi, K.A. (2021). Utilization of library and information centres in promoting Sustainable Development Goals (SDGs) in Nigeria. *Library Philosophy and Practice (e-journal)*. 6648. https://digitalcommons.unl.edu/libphilprac/6648

Omol, E.J. (2023). Organizational digital transformation: From evolution to future trends. *Digital Transformation and Society*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/DTS-08-2023-0061

Panesi, S., Bocconi, S. & Ferlino, L. (2020). Promoting Students' Well-Being and Inclusion in Schools Through Digital Technologies: Perceptions of Students, Teachers, and School Leaders in Italy Expressed Through SELFIE Piloting Activities. *Frontier in Psychology*, 11, 1563. https://doi.org/10.3389/fpsyg.2020.01563

Paor, S.D. & Heravi, B. (2020). Information literacy and fake news: How the field of librarianship can help combat the epidemic of fake news. *The Journal of Academic Librarianship*, 46(5), 102218. https://doi.org/10.1016/j.acalib.2020.102218.

Petrowicz, D. (2021, August 10). *How libraries can protect themselves from cyberattacks.* Germany: Springer Nature. https://www.springernature.com/gp/librarians/the-link/blog/blogposts-news-initiatives/how-libraries-can-protect-themselves-from-cyberattacks/19556496

Phuong, J., Ordóñez, P., Cao, J., Moukheiber, M., Moukheiber, L., Caspi, A., Swenor, B. K., Naawu, D. K. N., & Mankoff, J. (2023). Telehealth and digital health innovations: A mixed landscape of access. *PLOS Digital Health*, 2(12), e0000401. https://doi.org/10.1371/journal.pdig.0000401

Popkova, E.G. (2023). SDGs risks and digital approach to managing them. In: Popkova, E.G. (eds) *Sustainable Development Risks and Risk Management*. Advances in Science, Technology & Innovation. Springer, Cham. https://doi.org/10.1007/978-3-031-34256-1_1

Pressreader (2023, April 24). *How public libraries are helping bridge the digital divide*. Pressreader Team. https://blog.pressreader.com/libraries-institutions/how-public-libraries-are-helping-bridge-the-digital-divide

Qureshi, S. (2023). Digital transformation for development: A human capital key or system of oppression? *Information Technology for Development*, 29(4), 423–434. https://doi.org/10.1080/02681102.2023.2282269

Renn, O., Beier, G. & Schweizer, P. (2021). The opportunities and risks of digitalisation for sustain able development: a systemic perspective. *GAIA*, 30(1), 23-28. https://publications.iass-potsdam.de/rest/items/item_6000804_5/component/file_6000805/content

Rivers, H. (2024, January 12). *London library almost fully recovered from cyberattack, no ransom paid*. London: The London Free Press. https://lfpress.com/news/local-news/london-library-almost-fully-recovered-from-cyberattack-no-ransom-paid

Santos, L.G. & Dhaou, S.B. (2022). *Open Data and emerging technologies: Connecting SDG performance and digital transformation*. United Nations, SDGs. https://sdgs.un.org/sites/default/files/2023-05/A13%20-%20Magalh%C3%A3es%20-%20Open%20Data%20and%20Emerging%20Technologies%20Connecting%20SDG%20Performance%20and.pdf

Scroxton, A. (2024b, March 13). *British Library opens up over ransomware attack to help others*. Computer Weekly. https://www.computerweekly.com/news/366573453/British-Library-opens-up-over-ransomware-attack-to-help-others

Scroxton, A. (2024a, January 15). British Library cyberattack explained: What you need to know. Computer Weekly. https://www.computerweekly.com/feature/British-Library-cyber-attack-explained-What-you-need-to-know

Sethi, P. (2024, April 22). *What are climate misinformation and disinformation and what is their impact?* London: The London School of Economics and Political Science. https://www.lse.ac.uk/granthaminstitute/explainers/what-are-climate-misinformation-and-disinformation/

Sharma, Y. (2022, December 16). *Pandemic misinformation index: lessons for meeting SDGs*. University World News. https://www.universityworldnews.com/post.php?story=20221216061015666

Shaw, N. M., Hakam, N., Lui, J., Abbasi, B., Sudhakar, A., Leapman, M. S., & Breyer, B. N. (2022). COVID-19 misinformation and social network crowdfunding: Cross-sectional study of alternative treatments and antivaccine mandates. *Journal of Medical Internet Research*, 24(7), e38395. https://doi.org/10.2196/38395

Sullivan, M. C. (2019a). Libraries and Fake News: What's the Problem? What's the Plan?. *Communications in Information Literacy*, 13(1), 91-113. https://doi.org/10.15760/comminfolit.2019.13.1.7

Sullivan, M. C. (2019b). Why librarians can't fight fake news. *Journal of Librarianship and Information Science*, 51(4), 1146-1156. https://doi.org/10.1177/0961000618764258

Tanczer, L.M., Deibert, R.J., Bigo, D., Franklin, M.I., Melgaco, L., Lyon, D., Kazansky, B. & Milan, S. (2020). Online surveillance, censorship, and encryption in academia. *International Studies Perspectives*. 21(1), 1–36. https://doi.org/10.1093/isp/ekz016

Tekisalp, L. (2022, July 14). *Delaying climate action: The challenges of moderating climate misinformation on social media*. Business for Social Responsibility. https://www.bsr.org/en/blog/delaying-climate-action-moderating-climate-misinformation-social-media

The World Bank (2024). *Digital Technologies in Education: The use of information and communication technologies in education can play a crucial role in providing new and innovative forms of support to teachers, students, and the learning process more broadly*. The World Bank Group. https://www.worldbank.org/en/topic/edutech

Trevithick, M. (2024, March 4). *London library 'almost fully recovered' from ransomware attack, CEO says*. Canada: CBC. https://www.cbc.ca/news/canada/london/london-library-ransomware-almost-recovered-1.7131984

Udo, C.S., Ben, E.N., Afaha, I.J. & Yusuf, S. (2022). Media literacy in library and information centres: Practical perspectives. *Library Philosophy and Practice (e-journal)*. 7225. https://digitalcommons.unl.edu/libphilprac/7225

UNDP (2023a, March 22). *Three ways digital transformation accelerates sustainable and inclusive development*. United Nations Development Programme. https://www.undp.org/blog/three-ways-digital-transformation-accelerates-sustainable-and-inclusive-development

UNDP (2023b, September 17). *Digital technologies directly benefit 70 percent of SDG targets, say ITU, UNDP and partners*. United Nations Development Programme. https://www.undp.org/press-releases/digital-technologies-directly-benefit-70-percent-sdg-targets-say-itu-undp-and-partners

United Nation (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*. USA: United Nations. https://sdgs.un.org/2030agenda

United Nations (2021, February 17). *UN/DESA Policy Brief #92: Leveraging digital technologies for social inclusion*. Department of Economic and Social Affairs. https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-92-leveraging-digital-technologies-for-social-inclusion/

United Nations (2023, October 6). *Widening digital gap between developed, developing states threatening to exclude world's poorest from next industrial revolution, speakers tell second committee.* United Nations Meetings Coverage and Press Releases. https://press.un.org/en/2023/gaef3587.doc.htm

Welle, D. (2024, January 25). *What is climate misinformation, and why does it matter?* The Publishing PVT Ltd. https://frontline.thehindu.com/news/what-is-climate-misinformation-and-why-does-it-matter-disinformation-opponents-of-climate-science-greenwashing/article67771776.ece

WhoFi (2023). *Quarterly Analysis of Public Library WiFi Usage: Helping libraries across the country navigate the intersection of data and stories*. https://www.cosla.org/assets/images/Sponsor/Q1%202023%20Public%20Library%20WiFi%20Use.pdf

Young, J. C., Boyd, B., Yefimova, K., Wedlake, S., Coward, C., & Hapel, R. (2021). The role of libraries in misinformation programming: A research agenda. *Journal of Librarianship and Information Science*, 53(4), 539-550. https://doi.org/10.1177/0961000620966650

Youssef, A.B., Boubaker, S., Dedaj, B. & Carabregu-Vokshi, M. (2021). Digitalization of the economy and entrepreneurship intention. *Technological Forecasting and Social Change*, 164, 120043. https://doi.org/10.1016/j.techfore.2020.120043.

Zhang, X., & Saltman, R. (2022). Impact of electronic health record interoperability on telehealth service outcomes. *JMIR Medical Informatics*, 10(1), e31837. https://doi.org/10.2196/31837.