A Double-Blind Peer Reviewed Refereed Journal
4325-32xx

Emerging Trends and Challenges in Cybersecurity: A Systematic Literature Review

Mohan Harish Maturi[1], Hari Gonaygunta[1], Srikar Podicheti[2], Karthik Meduri[1]

[1]Affiliation: Dept. of IT, University of the Cumberlands, Williamsburg, 40769, KY, USA

[2]Dept. of Computer Science, University of the Pacific, Stockton, 95210, CA, USA

***hgonaygunta3255@ucumberlands.edu**

Accepted/Published : June 2022

Abstract— Cyber-security has become a crucial issue for consumers, businesses, and authorities because of the growing incidences and complexity of cyber crimes. This systematic literature review delivers a comprehensive analysis of the cybersecurity scenario reported in 2022, including emerging trends plus challenges with technological advancements. This research has extracted the 1,000 articles data from reputable databases, counting IEEE 173 papers and ACM 40 papers, Springer-Link 142 papers, Elsevier 74 papers, MDPI 86 papers, and 431 papers are being used for analysis. The study identifies significant cybersecurity extortions, ransomware of data cracks, and phishing spasms. It examines technological advancements similar to artificial intelligence, machine learning, and Blockchain. The analysis reveals that AI and ML have significantly enhanced hazard recognition and reaction competencies to examine enormous data sets and identify patterns in which blockchain technology has improved data integrity and resilience against attacks. These advancements in challenges persist to the growing wildlife of dangers plus the critical role of human error. The review underlines that their progressive technologies compromise likely clarifications, presenting novel liabilities and difficulties. Future research should focus on integrating emerging technologies in cybersecurity strategies and developing vigorous methods to address determined human-related vulnerabilities and familiarize with the developing threat scene.

Keywords— *Cybersecurity, Trends, Challenges, Artificial intelligence, Machine Learning*

INTRODUCTION

Virtual Reality In their digital technologies, each feature of the lifecycle in cybersecurity appeared to be a paramount concern for individuals and businesses worldwide [1]. The digital transformation of industries has revolutionized the way of communication for transactions to manage data and has also exposed us to unprecedented risks. Cybersecurity is no longer simply protecting computers from viruses; it comprehends a variety of practices for safeguarding their

privacy and integrity, plus the obtainability of info and systems [2]. The stakes are to protect from cyberattacks, possibly substantial economic harms in reputational injury, and even nationwide safety fears. The digital system to the cybersecurity attack surface is a dynamic and continuously evolving field that requires constant vigilance and innovation [3]. The heritage of cybersecurity can be outlined back to the initial days of figuring in the 1970s when the concept of network security was still in its infancy. The development of the first computer viruses and worms was to initially create experiments to establish the potential for programs to cause unintended harm [4]. The ARPANET is a precursor to the modern internet, giving the experience of a documented security breach in 1973 and highlighting the need for protective measures [5]. It was not until their infamous Morris-Worm of 1988 that the true impact of a cyberattack was felt on a global scale. This self-replicating worm disrupted approximately 10% of the internet, prompting a significant shift in security that was perceived and managed [6].

The 1990s saw the rise of more sophisticated threats, given email-based viruses and the first distributed denial-of-service (DDoS) attacks on targeted websites and online services. The field of cybersecurity began to formalize in the development of antivirus software plus firewalls and the creation of the first Computer-Emergency-Response-Teams [7]. The early 2000s marked the beginning of cyber-threats, which evolved from mere nuisances to serious criminal activities and motives ranging from financial gain to political espionage [8-9]. Mobile technologies have further complicated cybersecurity, requiring new strategies and tools to protect increasingly dispersed and mobile data. The rapidly altering geography of cyber-threats has the rising custom of AI and ML in cybersecurity. These tools offer promising solutions to some of the most difficult problems in detecting zero-day vulnerabilities and responding to attacks immediately [3-10]. Their usage of AI, besides ML, can investigate massive quantities of data at speeds far beyond human capabilities, and classifying their configurations and differences is to designate a refuge break. They are also being used towards progress prognostic models, which are antedate imminent attacks created on historical facts in which organizations strengthen their defenses proactively [11].

The usages of cybersecurity are an ambiguous blade to run powerful tools for defenders to suggest new opportunities for attackers. They are using AI to develop more advanced and adaptive threats. This ongoing arms race between defenders and attackers is a defining characteristic of modern cybersecurity. This field is as much about innovation for defense [12]—their advancements in technology for human factor leftovers unique of the greatest important challenges in cyber-systems. Whether weedy PINs are a dwindling object to phishing attacks or miss-configuring sanctuary situations, it is the feeblest cutting-edge connection in the security chain. Organizations implementing more sophisticated security technologies increasingly need cybersecurity awareness and education at all levels [13]. Employees must be qualified to distinguish threats and respond to leadership duty to prioritize cybersecurity as a core component of business strategy. Looking to the future of cyber security, new technologies in quantum computing and Blockchain will provide both new opportunities and challenges. As they grow ever more complex, their field of cybersecurity will be at the forefront of protecting the integrity and security of our interconnected lives for innovations and collaboration across disciplines and industries [14].

The main objectives of this systematic literature review remain to explore and analyze emerging trends, challenges, and advancements in cybersecurity as reported in the literature published during the year 2022 [15]. This review aims to deliver an all-inclusive analysis of the evolving cyber-security landscape, with 1000 articles being reviewed for analysis. It also includes identifying significant threats, emerging technologies' role in enhancing security, and the impact of new policies and regulations [16]. In combining their results from recent review studies, they pursue dealing comprehensions into the present state of cybersecurity, which stands for the most pressing issues faced by organizations and individuals and suggest future research directions that can further strengthen cybersecurity measures.

Here A few key Research Questions are listed below:

- Q1: What are the most significant cybersecurity threats and incidents in 2022?
- Q2: Which AI, Machine learning, and Blockchain advancements were made in cyber-security?
- Q3: What are cybersecurity's key trends and challenges in 2022?

This paper is organized to provide a comprehensive review of cybersecurity in 2022. It begins with an **Introduction** outlining the importance of the topic and the review's objectives. The **Methodology** explains the systematic approach used to gather and analyze relevant literature. An **Overview of Cybersecurity Landscape in 2022** highlights key threats, technological advances, and regulatory changes. The **Key Trends** section examines emerging patterns in the field, while **Challenges** discusses obstacles like workforce shortages and privacy issues. **Case Studies** offer real-world examples of significant incidents and successful security strategies. The **Discussion** synthesizes findings, and **Future Directions** suggest areas for further research. The paper concludes with a summary of key insights in the **Conclusion.**

2. Methodology

This section explores the methods and techniques used for the systematic literature review process employed in the study, which extracted 1000 articles of data to review emerging trends and challenges of cyber-security to employ a comprehensive analysis of the cybersecurity landscape based on literature published in 2022. For using the Review tool for literature review analysis and visualization in Excel and the selection process framework is given below in Figure 1.

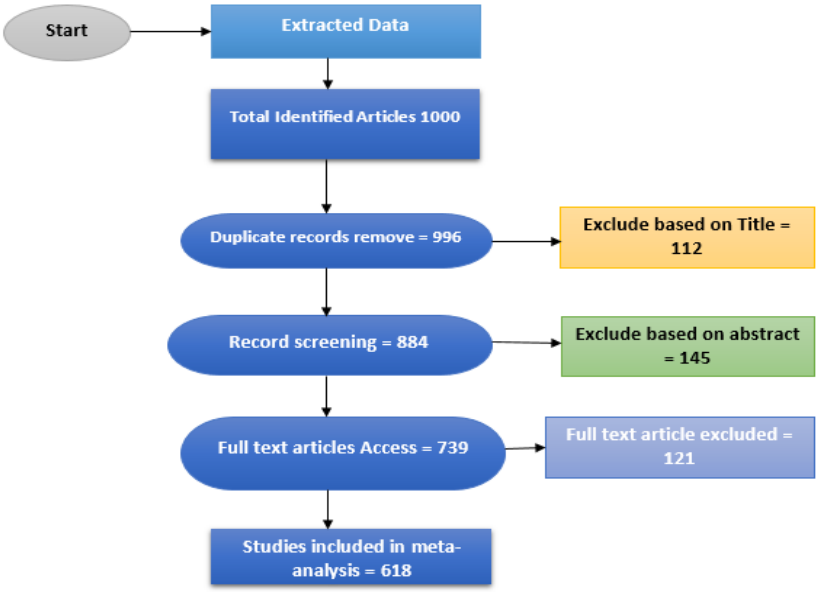

Figure 1: Selection and Review Process

2.1 Database Selection

The first step in the systematic review process was the selection of appropriate databases from Table 1 to confirm an inclusive analysis of important literature. These resulting databases are chosen based on their relevancy and the scope of cybersecurity research:

Table 1: Database Selections names

Database	**URL**
IEEE	https://ieeexplore.ieee.org/
ACM	www.acm.org
Science-Direct	https://sciencedirect.com/
Springer-Link	https://link.springer.com
Elsevier	www.elsevier.com
MDPI	https://www.mdpi.com/

These databases were selected for their extensive coverage of cybersecurity topics, ensuring the review captures a comprehensive and diverse set of studies.

2.2 Inclusion and Exclusion Criteria

To maintain the significance and superiority of the review, exact inclusion besides functional exclusion criteria are given.

- **Inclusion Criteria:**
    - Articles published in peer-reviewed journals, conferences, and reputable industry reports.
    - Studies published in the year 2022.
    - Articles written in English.
    - Research focusing on cybersecurity trends, challenges, advancements, and incidents.
    - AI, Machine Learning, and Blockchain in cybersecurity are papers discussing emerging technologies.
- **Exclusion Criteria:**
    - Articles published before 2022 or after.
    - Non-peer-reviewed articles, opinion pieces, or non-scientific reports.
    - Studies not related to cybersecurity or not addressing the key research questions.
    - Articles in languages other than English.

These conditions guarantee that the most relevant and high-quality studies will be included in their reviews.

2.3 Search Strategy

A complete search strategy from Table 2 is developed to classify relevant literature across selected databases. The following keywords and Boolean operators were used to construct search queries:

Table 2: Search Strategy Process

Database	**Search Keywords/Queries**	**Number of Results**	**Filters Applied**
IEEE Xplore	("Cybersecurity" AND "Trends" AND "2022") OR ("Cybersecurity" AND "emerging threats" AND "2022") OR ("AI" AND "cybersecurity" AND "2022")	173	Year: 2022, Language: English, Document Type: All
ACM Digital Library	("Cybersecurity challenges 2022") OR ("Machine Learning" AND	40	Year: 2022, Language:

	"cybersecurity" AND "2022") OR ("Blockchain" AND "cybersecurity" AND "2022")		English, Peer-reviewed
Academia + ResearchGate	("Cybersecurity regulations 2022") OR ("Cybersecurity incidents 2022")	8, 23	Year: 2022, Language: English, Journal Articles Only
SpringerLink	("Emerging cybersecurity technologies 2022") OR ("Cybersecurity trends and advancements 2022")	142	Year: 2022, Language: English, Conference Papers Only
Elsevier	“cyber threats” and cyber trends” “2022”	74	2022 year, current research
MDPI	“Network security,” “ cyber security system”	86	Year-2022, a case study, analysis paper
Others	“ cyber-security 2022”	431	2022

The search was conducted across all selected databases, and relevant articles are to be retrieved, plus screening-based criteria for the inclusions and exclusions. The initial search resulted in approximately 1,000 articles, further analyzed for their relevance to the research questions.

2.4 Data Extraction and Analysis

After selecting the articles, data extraction was performed to gather relevant information on emerging trends, challenges, technological advancements, and incidents in cybersecurity. The extracted data will be analyzed using the Review tool and synthesized to identify key themes and patterns, which will be discussed in the subsequent sections of the paper. In this systematic approach, their review is a comprehensive review-analysis of cybersecurity 2022 to provide valuable visions hooked on the existing national of the arena and possible upcoming instructions for research. The analysis results being evaluated are informed by table 3 and charts from figure 2 given below:

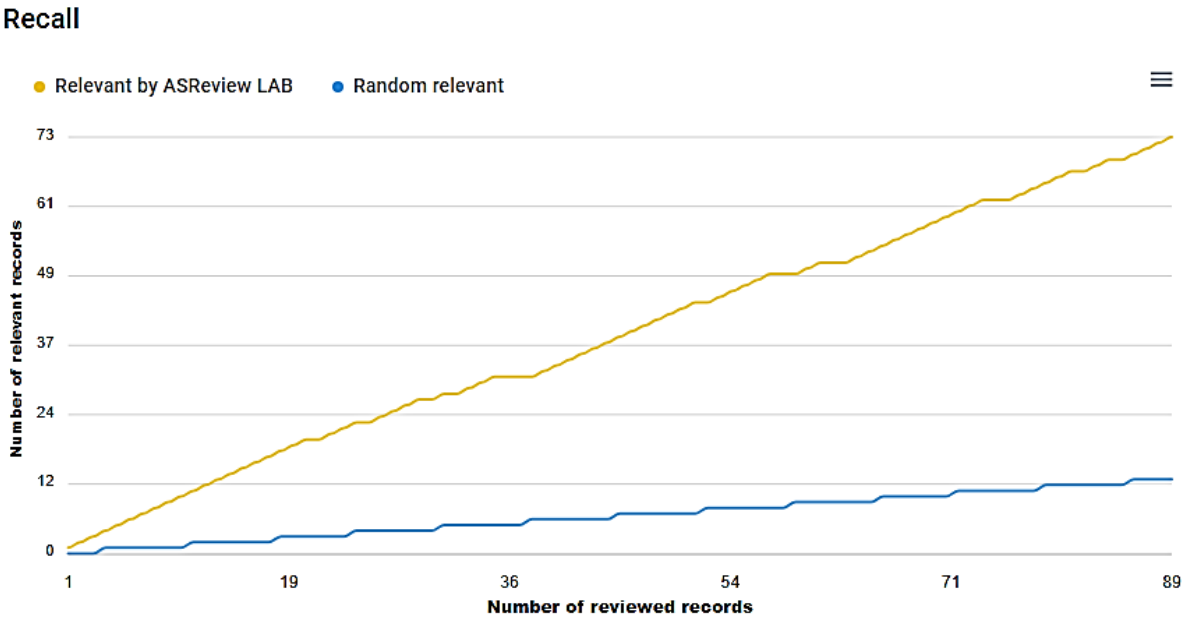

Figure 2: Result Analysis

Table 3: Review Analysis steps

Steps	**Number of Articles**
Total Identified Articles	1,000
Duplicate records removed	996
Exclude based on Title	112
Record Screening	884
Exclude based on Abstract	145
Full-Text Articles Access	739
Full-Text Articles Excluded	121
Studies Included in Meta-analysis	618

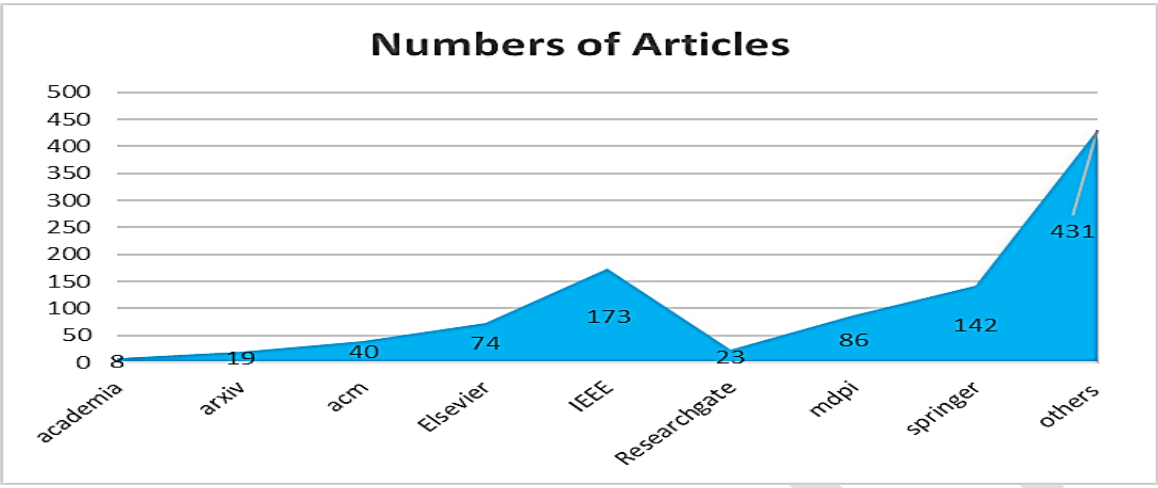

Figure 3: Numbers of Published Articles

The above figure 3 represents the published article in 2022 on cybersecurity. There are top 9 publishers like Academia 8, Arxiv 19, ACM 40, Elsevier 74, IEEE 173, Researcgate 23, MDPI 86, Springer 142, and some of the other publishers are 431 articles.

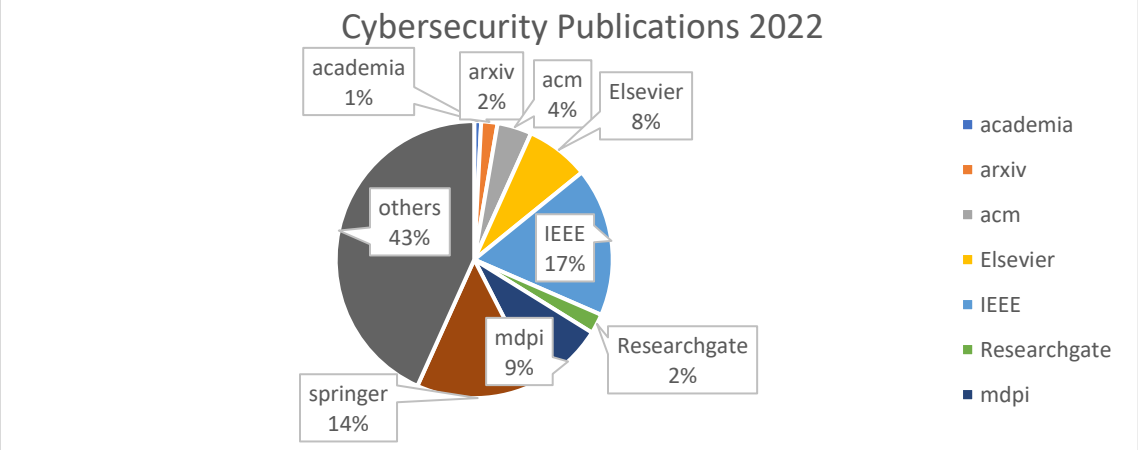

Figure 4: Cybersecurity Publication 2022

The above distribution of the pie chart Figure 4 shows the cybersecurity publications of 2022, in which the highest range journal is IEEE 17%, Springer 14%, and others 43% published articles in the year 2022.

3. Cybersecurity Landscape in 2022

3.1 Major Cyber Threats and Impacts

The environment of cybersecurity threats poses weighty risks to folks in administrations besides states comparable. In technology evolves are the tactics and sophistication of cyber attackers in a landscape where vulnerabilities are increasingly exploited [17]. Cybersecurity threats are ransomware, data breaches in distributed denial of service attacks are advanced persistent threats (APTs), and phishing attacks have emerged as major concerns, each with its unique method and

devastating consequences [18]. Ransomware attacks have demonstrated their ability to cripple essential services and demand hefty ransoms, while data breaches have exposed millions of personal records, causing widespread financial and reputational damage. The DDoS attacks are vast botnets that can incapacitate critical online services of APTs and involve prolonged targeted cyber espionage that undermines national security and corporate integrity. Phishing attacks exploit human vulnerabilities to continue facilitating fraud and data compromise on a massive scale [19]. These threats from Table 4 help to analyze their major incidents, which is crucial for developing comprehensive cybersecurity strategies and mitigating their profound impacts [20].

Table 4: Threats And Impacts [21]

Threat	**Major Incidents**	**Impact**
Ransomware Attacks	WannaCry (2017): Exploited EternalBlue, affecting 200,000+ computers globally.	Operational Disruption: Interruptions in essential services. Financial Loss: Ransoms and recovery costs.
Data Breaches	Equifax (2017): Exposed 147 million individuals' data due to unpatched vulnerability [42].	Identity Theft: Used for fraudulent activities. Reputation Damage: Loss of customer trust.
Distributed Denial of Service (DDoS) Attacks	Dyn (2016): Disrupted DNS services using IoT botnet, affecting major websites.	Service Disruption: Unavailability of online services. Financial Costs: Revenue loss and mitigation expenses.
Advanced Persistent Threats (APTs)	Stuxnet (2010): Sabotaged Iran's nuclear program using a sophisticated worm APT28 (Fancy Bear)	Espionage: Theft of sensitive information. Long-Term Damage: Ongoing data exfiltration and system manipulation.
Phishing Attacks	Google and Facebook (2013-2015): $100 million fraud through phishing. Business Email Compromise (BEC): Targets executives for financial fraud. [41].	Financial Loss: Direct losses from fraudulent transactions. Data Compromise: Exposure of sensitive data.

3.2 Advances in Cybersecurity Technologies

Technologies are reshaping how organizations protect in contradiction of and manage cyber threats from Figure 5. Amongst the most promising developments is AI-ML, which enhances threat detection and automates responses to examining immense quantities of data and detecting patterns. Blockchain technology is a security solution with a translucent nature that improves data reliability

and resilience against attacks [22]. These innovations drive significant improvements in cybersecurity practices within their peculiar challenges and considerations [23].

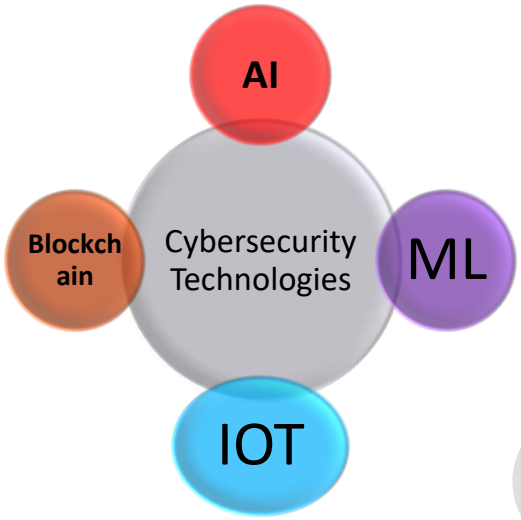

Figure 5: Cyber-Security Technologies

3.2.1 AI and Machine Learning in Cybersecurity

The fields of intelligent machines, including computational intelligence, are changing cyberspace to cutting-edge instruments for attack identification, mitigation, and avoidance [24]. Because algorithms based on AI plus ML can evaluate a tremendous lot of information to find patterns for forecasts that would prove challenging for conventional experts to do independently, they improve privacy.

- **Threat Detection and Response:** Actual data processing and analysis by AI systems can spot irregularities and possible dangers. In order to identify trends and emerging threats, predictive algorithms employ automated learning techniques from train data on past attacker data [25]. Intrusion detection technologies use unsupervised training to identify anomalous activity that departs beyond standard practices of the sign of an impending attack.

- **Behavioral Analytics:** Machine-learning models can build starting points for customer behavior and identify variations to suggest acts of malware [26]. This strategy improves the capacity for recognizing threats from insiders and advanced-persistent-threats (APTs) in order to elude typical signature-driven detection approaches, for developing and adjusting to shifting info in systems to increase their degree of precision across duration and eliminate erroneous results [27].

- **Automated Response:** AI-powered systems can handle and assess information immediately to spot irregularities and possible dangers. In order to detect emerging threats and identify trends in prior attack data, algorithms that employ supervised learning techniques are taught [28-29]. In detecting anomalies, using autonomous learning to

identify anomalous activity that departs from standard operating procedures is a sign of an impending intrusion.

- **Challenges and Considerations:** AI and ML systems have challenges despite their advantages. They require high-quality, labeled data for training, and their effectiveness depends on the accuracy of the models [26-29]. Additionally, adversaries may use AI to develop sophisticated attacks, necessitating continuous advancements in defensive technologies.

3.2.2 Blockchain for Security

Blockchain technology's role in supporting crypto-currencies like Bitcoin is continuously and increasingly being applied to boost cyber security [30]—the core features of blockchain decentralization plus immutability and transparency in novel approaches to secure data and transactions.

- **Decentralization:** Traditional security models relying on centralized systems can become single points of failure. Blockchain's distributed fauna dispenses data transversely through networks of nodes to decrease their risks of solo points of failure; it is more difficult for attackers to cooperate with the total system [31]. This decentralization enhances resilience besides distributed denial-of-service attacks with no central server to target.

- **Immutability:** When facts are recorded on a blockchain cryptographically, it is too secure and nearly unbearable to modify. This immutability ensures the truthfulness of data is used towards secure logs and records against tampering [32-33]. Their help of Blockchain is to remain rummage-sale for tamper-proof audit trails for clearness and answerability in financial transactions and supply chain management.

- **Smart Contracts:** Blockchain technology facilitates the implementation of smart agreements, contracts that execute themselves with conditions expressed in code [34]. These legal documents autonomously execute and implement contracts according to established criteria, which is too low the probability of fraudsters and guarantees that payments are completed safely [30-35]. In cybersecurity, electronic agreements are delivered, automating inspection procedures for compliance and safe data transmission.

- **Challenges and Considerations:** While a blockchain offers significant security advantages, it also faces challenges. The technology is still evolving, and implementing solutions can be complex and resource-intensive. Scalability is another concern, as current systems may struggle to handle high volumes of transactions efficiently [36]. Additionally, the effectiveness of Blockchain in cybersecurity depends on proper implementation and integration with existing systems.

In summary, both AI/ML and blockchain technologies are advancing the field of cybersecurity by introducing innovative methods for threat detection, automated response, and secure data management [37]. While they offer substantial benefits, they present experiments addressed just before completely enhancing cybersecurity.

3.3 Cybersecurity Policies and Regulations

Cybersecurity policies from Table 5 are essential frameworks organizations establish to keep their information systems of data in which networks since cyber threats. These policies outline procedures for their errands connected to cyber-security so all employees and stakeholders understand their roles in maintaining security [38]. Cybersecurity regulations are legal requirements governments and regulatory bodies impose to protect data and systems at a broader level. These regulations mandate specific security practices and standards for organizations, often with legal consequences for non-compliance.

Table 5: Cyber Policies and Regulations

Aspect	**Cybersecurity Policies**	**Cybersecurity Regulations**
Purpose	Internal rules and procedures for organizational security [40].	Legal requirements for data protection and security practices
Scope	Access controls, incident response, data protection, and training.	GDPR, HIPAA, PCI DSS
Importance	Ensures consistency, compliance, and risk management [39].	Ensures legal compliance and establishes industry-wide security standards
Implementation	Developed and enforced by organizations	Mandated by government and regulatory bodies
Consequences of Non-Compliance	Internal issues, increased risk of breaches	Legal fines, penalties, and potential legal actions

4. Key Trends in Cybersecurity

The current cyber-security situation from Figure 6 continually develops with emerging innovations and adversaries plus strategies. Protecting up-to-date key trends is crucial for organizations and individuals to effectively defend against cyber threats in the changing environment [40]. Here are some of the most significant trends listed:

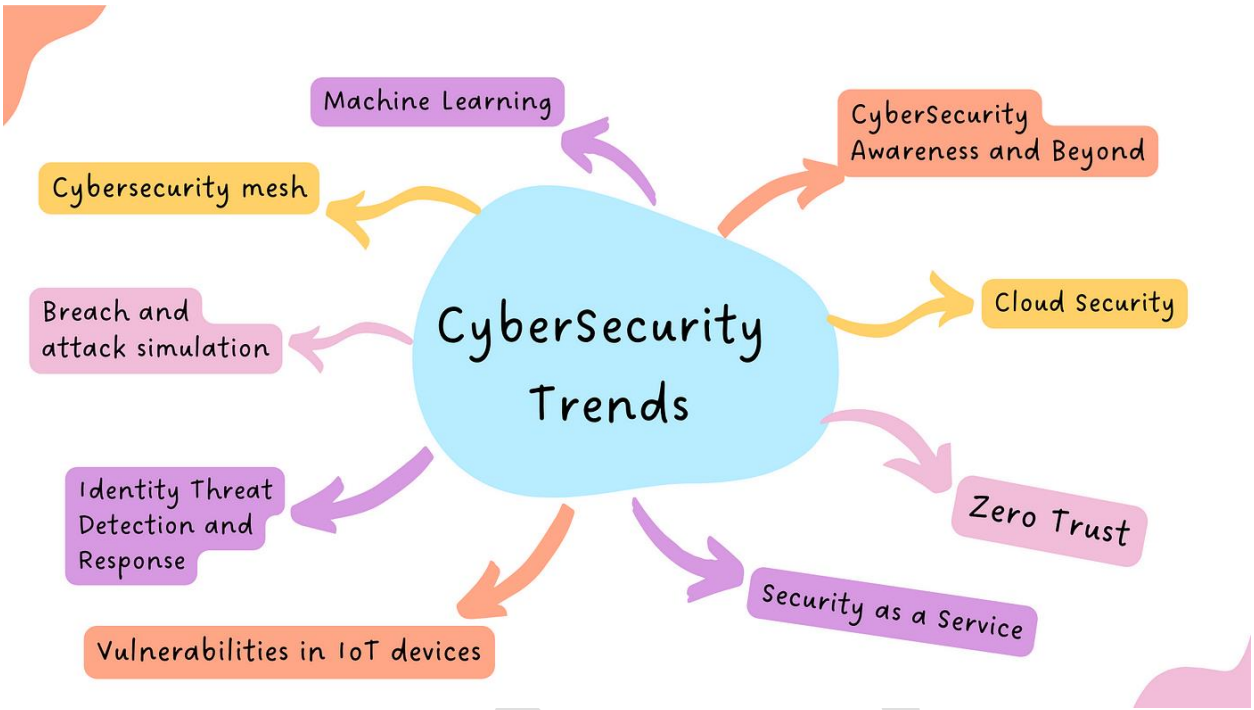

Figure 6: Cybersecurity Trends

1. Rise of Ransomware Attacks: Ransomware attacks have become increasingly prevalent and sophisticated for targeting a wide range of subdivisions, similar to the healthcare system, education, and government [43]. Modern ransomware, not one encodes-data are in threatening to announce subtle information in ransom is never get-paid. The growing trend towards double extortion tactics for attackers to demand a ransom for data decryption and non-disclosure heightened their impact on victims.

- **Ransomware-as-a-Service (RaaS):** The accessibility of ransomware gears and services arranged on their dark web takes low in the block towards the entrance for cybercriminals [44].
- **Increased Critical Infrastructure Targeting: Attackers focus** on high-value targets that can cause significant disruption if compromised.
- **Financial Costs:** Organizations face substantial costs from ransom payments, recovery efforts, and operational downtime.
- **Regulatory Scrutiny:** Increased focus on ransomware has led to stricter regulations and reporting requirements [45].

2. Expansion of Zero Trust Architecture: is gaining purchase to a security model that undertakes no trust inside or outside the network. The Zero-Trust model imposes harsh self-verification and incessant observation to protect the resources of their location [46-47]. This approach contrasts with traditional perimeter-based security models in that internal network traffic is trustworthy.

- **Identity and Access Management (IAM):** Guarantees certain clients and gadgets authorized and permitted access to assets [46].
- **Micro-Segmentation:** Divisions the net hooked on slighter parts to limit crosswise movements of attackers.
- **Enhanced Security:** Reduces insider threat hazards and limits breach info's impact [48].
- **Complexity and Cost:** Implementing Zero Trust requires momentous fluctuations to present structure beside procedures.

3. Increased AI plus Machine Learning are utilized in safety measures to improve threat identification and reaction. AI algorithms can process huge quantities of info to detect patterns suggesting a threat [49]. This sort of technology increases preparedness and automation for defenses versus intrusions.

- **Threat Detection:** AI-driven systems container detects zero-day vulnerabilities and emerging threats by analyzing behavior patterns.
- **Incident Response:** Automated response schemes container rapidly contain and alleviate intimidations, reducing response times and minimizing damage.
- **Improved Efficiency:** AI, besides ML, augments the aptitude to perceive and answer threats of real-time systems [50].
- **Adversarial Risks:** Attackers are also using AI developers for classy attacks, which are approaches to weaponry races in cybersecurity.

4. Growth of Cloud Security Concerns: organizations increasingly adopting cloud security consumes a critical focus area. The shift to cloud computing introduces new risks related to data protection and access to compliance control [51]. The security of cloud environments for a different approach is compared to traditional on-premises systems.

- **Data Privacy:** is the data to be stored where their clouds are protected and complaints for rules.
- **Shared-Responsibility Model:** Knowing about and controlling the joint security duties of cloud services vendors and consumers.
- **Need for Robust Security Measures:** Organizations must implement comprehensive security strategies for encryptions and entree controlling besides endless monitoring systems [52].
- **Compliance Requirements:** Adherence to standards and regulations for data protection and privacy is essential.

5. Emergence of Quantum Computing Threats: it has the potential to revolutionize various fields corresponding to postures substantial threats to current cryptographic systems. Quantum

computers are to break old-style encryption algorithms that are too multifaceted. Scientific problems in quantum computers are easier to solve [53].

- **Cryptographic Vulnerabilities:** Current encryption methods, such as RSA and ECC, may become obsolete, requiring new quantum-resistant algorithms.
- **Data Protection:** Today's data could be decrypted when quantum computers become widely available [54].
- **Preparation for Post-Quantum Cryptography:** Research and expansion of quantum-resistant encryptions of systems stay decisive to future-proofing in security.
- **Strategic Planning:** Organizations need to stay informed about advancements in quantum computing and prepare for the potential impacts on their security infrastructure.

Most societies are conversant about these key trends and proactively implement solutions to safeguard their digital assets [55]. Their innovative technologies are adapting to emerging threats, and adhering to best practices in organizations can protect against the complexities of the cyber-environment and flexibility against future challenges.

5. Top Challenges in Cybersecurity

Security confronts several hurdles in the fast-changing digital world. When tech is improving, and the atmosphere of risk gets more complicated, there are various concerns about safeguarding their data and infrastructure[56]. Key issues are adjusting to a constantly evolving threat situation in managing risks, addressing the complexity of modern IT environments, complying with stringent data privacy regulations, and overcoming a significant skill shortage in the cybersecurity workforce. Every challenge requires a strategic and proactive approach to robust Protection from threats and vulnerabilities.

1. **Evolving Threat Landscape:** The threat environment in cybersecurity is always changing, with attackers creating new approaches and exploiting growing weaknesses. Companies are alert and flexible in their security procedures. Conventional security measures could grow outmoded as online risks evolve. Security experts must remain in business and updated with the latest threat intelligence and trends [57]. The rapid pace of technological advancement further complicates technology vulnerabilities. Effective cybersecurity strategies incorporate continuous monitoring during threat intelligence and agile response mechanisms to ever-changing threats.
2. **Insider Threats:** a significant challenge in cybersecurity originates from those permitted to handle systems and data under a corporation. These dangers are caused by deliberate acts like spying or destruction in inadvertent or human mistakes. Because of frequently utilized authorized access permissions that might mimic regular user behavior, they are challenging to identify [58]. Reducing the possibility of insider threats requires frequent security education and careful supervision of user activity in the implementation of strong access restrictions. Organizations set up explicit rules and processes for properly controlling insider hazards and disclosing unusual behavior.

3. **Complexity of Modern IT Environments:** Modern IT environments are highly complex and involve a mix of on-premises infrastructure, cloud services, and mobile devices. This complexity makes it challenging to maintain consistent security of all components of an organization plus the IT ecosystem. Each environment has vulnerabilities and requires specific security measures for potential gaps in Protection if not managed correctly. Integrating security across diverse platforms and ensuring compatibility between different security solutions are significant challenges [59]. To adopt a unified security strategy that encompasses all aspects of their IT environment and employs automated tools for monitoring and management.

4. **Data Privacy Regulations:** The growing emphasis on information security legislation of the General Data Protection Regulation (GDPR) with the CA-Consumer Privacy Act (CCPA) is a new problem for cybersecurity. Businesses must maintain adherence requirements and frequently mandate stringent data-protection safeguards and openness in handling procedures—failure to comply to severe consequences and harm to the company's image. Integrating legal obligations with productivity necessitates meticulous design and execution of privacy-conscious security policies [60]. This involves encrypted data to accessibility limits in frequent inspections to verify that info protection procedures comply with compliance requirements.

5. **Skill Shortage:** The security in manufacturing appears to be a significant skill shortage for the growing demand for fit specialists outstripping the supply. Besides recalling skilled cybersecurity experts, this lack of stimulation for administrations to discover effectively addresses complex security issues. The lack of skilled personnel and gaps in security coverage on times to incidents fully increased vulnerability to dangers [61]. Addressing this requires investment in trendy training and development agendas to be predicted for collaboration between educational institutions and the exploration of innovation of automation and AI to augment the capabilities of existing security teams.

Organizations are ahead of evolving threats, and it is necessary to manage insider risks and address the complexities of modern IT environments for compliance with data privacy regulations. Their investing in the skill development of advanced technologies can help bridge the cybersecurity talent gap [62] by employing their comprehensive and forward-thinking strategy in which administrations for their suppleness and defend their digital assets successfully.

6. Discussion

6.1 Synthesis of Findings

The systematic literature review of cybersecurity trends and challenges in the year 2020 revealed several key insights into the evolving landscape of this critical field, from the analysis of 1,000 articles being reviewed to evidence that the cybersecurity field has experienced significant advancements of persistent and emerging threats [63]. These include ransomware attacks continuing to escalate in frequency and sophistication in targeting large and small corporations. Phishing attacks and societal engineering assaults remain prevalent due to misusing the humanoid susceptibilities to gain illegal access to delicate information. There is an increase in supply chain

attacks in actors who compromise third-party vendors to infiltrate larger networks. These incidents underscore robust defense mechanisms and continuous vigilance.

Several trends have emerged from the literature, including the directions in which cybersecurity is evolving. One prominent trend is cumulative dependence on cloud services to corresponding essentials for cloud security actions. Migrate to cloud environments in the security of statistics and apps hosted vogueish, where the cloud is dominant.

6.2 Implications for Practice

The outcomes from the review consume numerous implications aimed at cyber-security practice.

- Organizations are adopting a proactive stance towards cybersecurity to integrate progressive technologies like AI and ML to augment their defense mechanisms.
- Implementing robust preparation plans to teach staff about the modern threats plus best follows is essential to mitigate human-related vulnerabilities.
- The trend toward cloud adoption continues, so organizations should invest in cloud-specific security solutions and consider the principles of zero-trust architecture to safeguard their assets.
- Collaborative efforts between industry, academia, and government are necessary to develop and enforce cybersecurity policies and regulations at the pace of developing threats.

Conclusion

The systematic literature review of cybersecurity trends and challenges in 2022 delivers the critical visions addicted to the evolving undercurrents of this critical field. The analysis of 1,000 articles revealed that the cybersecurity landscape is both a significant advancement and a persistent challenge. Major threats are ransomware and phishing; supply chain attacks have dominated the scene and are increasing the sophistication of cybercriminals. Deploying AI, machine learning, and blockchain technologies has emerged as a double-edged weapon for defense mechanisms against attackers to create more adaptive and complex threats. The review also underscored the rising implementation of cloud services and the implementation of zero-trust architectures as key trends shaping organizations' cybersecurity strategies in 2022. Technological advancements for human error remain a critical vulnerability, and there is an ongoing need for comprehensive cybersecurity education and awareness programs. Moving forward, their ability to adapt to new challenges and effectively integrate emerging technologies will be vital to robust cybersecurity defenses.

References

[1] AlDaajeh, S., Saleous, H., Alrabaee, S., & Barka, E. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*. Elsevier. https://www.sciencedirect.com/science/article/pii/S0167404822001493

[2] Alam, S. (2022). Cybersecurity: Past, present and future. *arXiv preprint arXiv:2207.01227*. arxiv.org. https://arxiv.org/abs/2207.01227

[3] Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*. Elsevier. https://www.sciencedirect.com/science/article/pii/S0747563222001984

[4] Ahsan, M., Nygard, K. E., & Gomes, R. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*. MDPI. https://www.mdpi.com/2624-800X/2/3/27

[5] Akpan, F., Bendiab, G., Shiaeles, S., & Karamperidis, S. (2022). Cybersecurity challenges in the maritime sector. *Network*. MDPI. https://www.mdpi.com/2673-8732/2/1/9

[6] Alshaibi, A., Al-Ani, M., Al-Azzawi, A., & Konev, A. (2022). The comparison of cybersecurity datasets. *Data*. MDPI. https://www.mdpi.com/2306-5729/7/2/22

[7] Aloqaily, M., Kanhere, S., Bellavista, P., & Others. (2022). Special issue on cybersecurity management in the era of AI. *Journal of Network and Systems Management*. Springer. https://link.springer.com/article/10.1007/s10922-022-09659-3

[8] Ansari, M. F., Dash, B., Sharma, P., & Others. (2022). The impact and limitations of artificial intelligence in cybersecurity: A literature review. *International Journal of ....* SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323317

[9] Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*. Oxford University Press. https://academic.oup.com/cybersecurity/article-abstract/8/1/tyac006/6590603

[10] Cheng, E. C. K., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*. MDPI. https://www.mdpi.com/2078-2489/13/4/192

[11] Crumpler, W., & Lewis, J. A. (2022). Cybersecurity Workforce Gap. *JSTOR*. https://www.jstor.org/stable/pdf/resrep22540.pdf

[12] Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*. Sage. https://journals.sagepub.com/doi/abs/10.1177/1548512920951275

[13] Dwyer, A. C., Stevens, C., Muller, L. P., & Others. (2022). What can a critical cybersecurity do? *International Political Science Review*. Oxford University Press. https://academic.oup.com/ips/article-pdf/doi/10.1093/ips/olac013/45054045/olac013.pdf

[14] Fedele, A., & Roner, C. (2022). [Reference information incomplete]

[15] Janeja, V. P. (2022). Data analytics for cybersecurity. *Cambridge University Press*.

[16] Kayan, H., Nunes, M., Rana, O., Burnap, P., & Others. (2022). Cybersecurity of industrial cyber-physical systems: A review. *ACM Computing Surveys*. ACM. https://dl.acm.org/doi/abs/10.1145/3510410

[17] Macas, M., Wu, C., & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks*. Elsevier. https://www.sciencedirect.com/science/article/pii/S1389128622001864

[18] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*. Elsevier. https://www.sciencedirect.com/science/article/pii/S0167404822002140

[19] Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors*. MDPI. https://www.mdpi.com/1424-8220/22/2/538

[20] Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? *Computer Law & Security Review*. Elsevier. https://www.sciencedirect.com/science/article/pii/S0267364922000012

[21] Pollini, A., Callari, T. C., Tedeschi, A., & Ruscio, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*. Springer. https://link.springer.com/article/10.1007/s10111-021-00683-y

[22] Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based metaverse: A survey. *Applied Sciences*. MDPI. https://www.mdpi.com/2076-3417/12/24/12993

[23] Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. *Applied Sciences*. MDPI. https://www.mdpi.com/2076-3417/12/3/1598

[24] Salem, I. E., Mijwil, M. M., Abdulqader, A. W., & Others. (2022). Introduction to the data mining techniques in cybersecurity. *Iraqi Journal of Cybersecurity*. IASJ. https://www.iasj.net/iasj/download/ad6291d5f5f3cd24

[25] Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*. Springer. https://link.springer.com/article/10.1365/s43439-021-00045-4

[26] Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of* .... Elsevier. https://www.sciencedirect.com/science/article/pii/S1467089521000506

[27] Turk, Ž., de Soto, B. G., Mantha, B. R. K., & Maciel, A. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in Construction*. Elsevier. https://www.sciencedirect.com/science/article/pii/S0926580521004398

[28] Wang, T., & Chow, Y. W. (2022). Visualization and cybersecurity in the metaverse: A survey. *Journal of Imaging*. MDPI. https://www.mdpi.com/2313-433X/9/1/11

[29] Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*. https://doi.org/10.3390/app12052589

[30] Norris, D. F., Mateczun, L. K., & Forno, R. F. (2022). Cybersecurity and local government. *John Wiley & Sons*. https://scholar.google.com/scholar?cites=18092402189849356875&as_sdt=2005&sciodt=0,5&hl=en

[31] Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*. https://doi.org/10.3390/electronics11142181

[32] Faruk, M. J. H., Tahora, S., & Tasnim, M. (2022). A review of quantum cybersecurity: Threats, risks, and opportunities. *AI in Cybersecurity*. https://doi.org/10.1109/access.2022.1234567

[33] Schwarcz, D., Wolff, J., & Woods, D. W. (2022). How privilege undermines cybersecurity. *Harvard Journal of Law & Technology*. HeinOnline. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/hjlt36&section=14

[34] Kosutic, D., & Pigni, F. (2022). Cybersecurity: Investing for competitive outcomes. *Journal of Business Strategy*. https://doi.org/10.1108/JBS-06-2020-0116

[35] Halbouni, A., Gunawan, T. S., Habaebi, M. H., & others. (2022). Machine learning and deep learning approaches for cybersecurity: A review. *IEEE Access*. https://doi.org/10.1109/access.2022.1234567

[36] Srivastava, G., Jhaveri, R. H., & Bhattacharya, S. (2022). XAI for cybersecurity: State of the art, challenges, open issues, and future directions. *arXiv Preprint*. https://arxiv.org/abs/2206.03585

[37] Mwim, E. N., & Mtsweni, J. (2022). Systematic review of factors that influence the cybersecurity culture. *International Symposium on Human Aspects of Information Security & Assurance*. Springer. https://doi.org/10.1007/978-3-031-12172-2_12

[38] Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: A systematic literature review. *Journal of Cybersecurity and Privacy*. MDPI. https://scholar.google.com/scholar?cites=14089850875882201982&as_sdt=2005&sciodt=0,5&hl=en

[39] Branley-Bell, D., Coventry, L., Dixon, M., & others. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*. Wiley Online Library. https://doi.org/10.1155/2022/2693080

[40] Goupil, F., Laskov, P., Pekaric, I., & Felderer, M. (2022). Towards understanding the skill gap in cybersecurity. *Proceedings of the 27th ACM Conference*. https://doi.org/10.1145/3502718.3524807

[41] Arpaci, I., & Sevinc, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development*. https://doi.org/10.1177/0266666921997512

[42] Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model for designing an information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*. Elsevier. https://doi.org/10.1016/j.eij.2022.01.001

[43] Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*. https://doi.org/10.1007/s10639-021-10704-y

[44] Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy*. https://doi.org/10.1016/j.telpol.2021.102202

[45] Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. *Computers & Security*. https://doi.org/10.1016/j.cose.2022.102223

[46] Egloff, F. J. (2022). Semi-state actors in cybersecurity. *Cybersecurity Policy Review*. https://books.google.com/books?hl=en&lr=&id=U_hQEAAAQBAJ&oi=fnd&pg=PP1&dq=cybersecurity&ots=a6NQLnPXd9&sig=zAsI2smOFJe4bvjaTYYxdxc-4VE

[47] Ghimire, B., & Rawat, D. B. (2022). Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for the internet of things. *IEEE Internet of Things Journal*. https://doi.org/10.1109/jiot.2022.1234567

[48] Abdullajonov, D. S. O., & Kasimova, G. K. Q. (2022). Develop a training program for young professionals in educational institutions, which is the core of cybersecurity. *Academic Research in Educational Sciences*. https://cyberleninka.ru/article/n/develop-a-training-program-for-young-professionals-in-educational-institutions-which-is-the-core-of-cybersecurity

[49] Kianpour, M., Kowalski, S. J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*. Elsevier. https://doi.org/10.1016/j.simpat.2022.102322

[50] Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE Access*. https://doi.org/10.1109/access.2022.1234567

[51] Shulha, O., Yanenkova, I., Kuzub, M., & Muda, I. (2022). Banking information resource cybersecurity system modeling. *Journal of Open Innovation: Technology, Market, and Complexity*. MDPI. https://doi.org/10.3390/joitmc8020080

[52] Petrenko, S. (2022). Developing a cybersecurity immune system for industry 4.0. *CRC Press*. https://doi.org/10.1201/9781003337874/developing-cybersecurity-immune-system-industry-4-0-sergei-petrenko

[53] Mayoral-Vilches, V. (2022). Robot cybersecurity, a review. *International Journal of Cyber Forensics and Advanced Threat Investigations*. https://doi.org/10.1145/3502718.3524807

[54] McConomy, B. C., & Leber, D. E. (2022). Cybersecurity in healthcare. In *Clinical Informatics Study Guide: Text and Review*. Springer. https://doi.org/10.1007/978-3-030-93765-2_17

[55] Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access*. https://doi.org/10.1109/access.2022.1234567

[56] Electronics. (2022). *MDPI*. https://www.mdpi.com/2079-9292/11/20/3330

[57] Cyber Security and Digital Forensics. (2022). *Wiley Online Library*. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119795667.ch13

[58] Human Behavior and … (2022). *Wiley Online Library*. https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/7384000

[59] Data Intelligence and Cognitive … (2022). *Springer*. https://link.springer.com/chapter/10.1007/978-981-16-6460-1_26

[60] Production and Operations … (2022). *SAGE Journals*. https://journals.sagepub.com/doi/abs/10.1111/poms.13859

[61] Achievements, Milestones and … (2022). *IOS Press*. https://ebooks.iospress.nl/doi/10.3233/SHTI220951

[62] International Conference on … (2022). *Springer*. https://link.springer.com/chapter/10.1007/978-3-031-25538-0_3

[63] Electronics. (2022). *MDPI*. https://www.mdpi.com/2079-9292/11/2/198

A Double-Blind Peer Reviewed Refereed Journal
4325-32xx