ISSN 2712-0562
Review Article

Sustainable Engineering and Innovation
Vol. 6, No. 1, April 2024, pp.57-86
https://doi.org/10.37868/sei.v6i1.id207

Cybersecurity challenges across sustainable development goals: A comprehensive review

Nur Nabila Mohamed[1*], Bassam Hossam Hassan Abuobied[2]
[1] School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, Selangor, Malaysia
[2] Department of Mechanical Engineering, Istanbul Aydin University, Istanbul, Turkey

*Corresponding author E-mail: nurnabilamohamed@uitm.edu.my

Received Oct. 30, 2023
Revised Apr. 3, 2024
Accepted Apr. 14, 2024

Abstract

In an era where society becomes increasingly reliant on digital technology and interconnected systems, the significance of cybersecurity for upholding sustainable development has become paramount. The Sustainable Development Goals (SDGs) were adopted by the United Nations in 2015 as a universal call to action to end poverty, protect the planet, and ensure that by 2030, people enjoy peace and prosperity. As we draw closer to the critical year of 2030, the insights of this paper gain urgency in light of ongoing efforts to achieve the SDGs. This review paper takes an innovative stance by examining how cybersecurity challenges align with each SDG. The novelty of this study is that, it not only highlights the interconnected nature of cybersecurity within each goal but also identifies and categorizes the top five emerging threats that could impact the 17 goals. By pinpointing potential risks, it calls for further research and strategies to counter these cyber threats that might hinder the progress towards the SDGs. This research work serves as valuable guidance for researchers, policymakers, and practitioners, offering a comprehensive understanding of the intricate relationship between cybersecurity and sustainable development.

Keywords: Cybersecurity, Cyberattacks, Sustainable Development Goal, Information System, Industry Revolution 4.0

1. Introduction

The 2030 agenda for Sustainable Development lays out a comprehensive framework comprising 17 interconnected Sustainable Development Goals (SDGs) aimed at addressing pressing global challenges [1]. These goals encompass a number of significant objectives including reducing the poverty, ensuring quality education, promoting gender equality and combating climate change among others. While the pursuit of these SDGs is critical for the well-being of both current and future generations, the increasingly digitalized nature of modern society introduces new complexities and vulnerabilities [2]. The rapid proliferation of digital technologies, the Internet of Things (IoT), machine learning, big data, cloud computing and the integration of cyber-physical systems have undeniably revolutionized various sectors and transforming the ways we live and work. However, this digital evolution has fostered a setting vulnerable to exploitation malicious actors. Cyberattacks ranging from data breaches and ransomware attacks to sophisticated state-sponsored cyber operations pose significant threats to the stability and progress of the global community's pursuit of the SDGs.

Cybersecurity vulnerabilities have the potential to disrupt critical infrastructure, compromise personal data and diminish trust in technological advancements. Therefore, acknowledging and addressing these cybersecurity challenges within the context of each SDG is important to ensure a comprehensive and resilient approach for sustainable development. This review paper aims to explore the cybersecurity challenges within the framework of the SDGs. By exploring into the specific threats and vulnerabilities that intersect with each goal, it seeks to provide a comprehensive overview of the potential risks that could compromise the progress. Moreover, this paper aims to serve as a catalyst for further research, encouraging scholars, researchers and practitioners to collaborate in formulating effective strategies to mitigate cyber threats and defend the pursuit of sustainable development. In doing so, this paper contributes to a depth understanding of the challenges associated with the SDGs and emphasizes the need for a multidisciplinary and integrated approach to address the complex interplay between cybersecurity and sustainability.

2. Research methodology

The aim of this study is to explore the relationship between cybersecurity challenges and the attainment of the SDGs. There are two research questions in this study:

1. What potential disruptions do the security threats pose to the progress of each SDG?
2. How do the evolving cybersecurity threats intersect within the 17 SDGs?

Based on these research questions, two objectives have been formulated. The first objective of this study is to identify and categorize emerging cybersecurity threats that intersect with each SDG. The second objective is to categorize and analyze the top five evolving threats within the context of the SDGs, aiming to raise awareness and promote proactive strategies for mitigating their impact. To achieve the first objective of this study, the articles on cybersecurity issue in each SDG from year 2016 to 2023 were reviewed. Keywords of cybersecurity issue/challenges and each of the goals were searched in the electronic databases in the Web of Science, Scopus and Google Scholar. After locating approximately 296 papers related to the approaches, a deep topic filtering was conducted. Consequently, 199 publication articles that satisfied the requirements were selected. The second objective was achieved by identifying how the top five evolving threats could affect the 17 SDG areas. The keywords of the evolving threats and the SDG area were searched within the Web of Science, Scopus and Google Scholar. From this, the goals which were vulnerable to the five attacks could be identified.

3. Results and discussion

Cybersecurity is the practice of safeguarding digital systems, networks, and data from malicious activities which has emerged as an imperative shield against cyberattacks that range from the theft of sensitive information to large-scale cybercrimes. As technology becomes increasingly and rapidly expanding, the protection of digital assets and the assurance of online privacy have risen to the forefront of global concerns. The interconnectedness of our digital lives, spanning from personal devices to critical infrastructure, underscores the pressing need for robust cybersecurity measures [3]. This study identified several cybersecurity challenges on each of the SDGs to deliver a clear understanding of how digital security connects to sustainable development as can be seen in Table 1. It discovers where vulnerabilities might exist in reaching each SDG, showing areas that could be at risk from cyber threats. Recognizing how cybersecurity interacts with the SDGs is crucial for an all-encompassing approach that considers both digital safety and overall development. Table 1 summarizes the findings of cybersecurity challenges across each SDG, offering a comprehensive overview of potential vulnerabilities and risks that could hinder the attainment of these goals.

Table 1. Cybersecurity Concern on Each SDG

SDG	Key Challenge	Cybersecurity Concern
SDG 1: No poverty	Digital exclusion	No proper access on digital technologies face exclusion from opportunities and resources [4]. The study in [5] highlights a significant digital gap among urban residents, particularly those with low incomes. Moreover, low digital literacy persists due to minimal interaction with digital resources, resulting in low internet and social media usage within this demographic [6].
	Digital identification system	Many poverty alleviation programs rely on this system to target beneficiaries and deliver services efficiently [7].The adoption of Aadhaar, India's biometric population database, within the national food security program showed that datafication can enhance the effectiveness of anti-poverty schemes but also resulted in data injustice and exclusion of entitled households [8]. A large-scale experiment in India's subsidized food program found that requiring biometric authentication did not reduce leakage but increased transaction costs and reduced benefits for beneficiaries who had not previously registered an ID [9].
	Digital Platform -	Governments use digital platforms to distribute social assistance and safety net benefits [10]. Aid agencies, governments, and donors are investing in the digitization of beneficiary identification and registration systems to facilitate the delivery of shock-responsive social protection and move towards government provision of assistance as discussed in [11].
SDG 2: Zero hunger	Supply Chain Vulnerabilities	The supply chains [12] are increasingly digitized and connected, making them vulnerable to cyberattacks that could disrupt the flow of agricultural products, leading to food shortages and increased food insecurity. The study in [13] discusses that the food industry is experiencing an increase in cyber-security threats, which might result in business interruptions. The COVID-19 lockdown in India highlighted the vulnerability of food supply chains, both rural and urban, and the negative impact on farm-to-market arrivals [14].
	Data Privacy and AgTech	Ensuring the privacy and security of this data is essential to prevent unauthorized access, data breaches, and potential misuse that could affect the overall agricultural sector and contribute to food insecurity [15]. Technical architectures and sharing design patterns, like the Open Ag Data Alliance framework, can also support different sharing models while ensuring data privacy [16].
	Agri-Financing	Ensuring the cybersecurity of these systems is crucial to prevent financial losses and protect the economic livelihoods of farmers who rely on these platforms [17]. The adoption of mobile banking technology has been found to influence the level of agricultural credit demand, highlighting the importance of technology adoption in accessing financial services for farmers [18]. Furthermore, the development of digital finance has been shown to significantly promote agricultural green total factor productivity (AGTFP), which is crucial for sustainable agricultural development [19]

SDG	Key Challenge	Cybersecurity Concern
SDG 3: Good health and well being	Digital Health Data Security	The integration of electronic health records and telemedicine introduces a wealth of sensitive patient data, making it crucial to secure health information from unauthorized access, data breaches, and identity theft [20]. The blockchain implementation by the healthcare companies [21] to gather comprehensive patient records, including sensitive data like social security numbers, making it crucial to secure health information from unauthorized access and data breaches.
	IoT Medical Devices and patient safety concern	Medical devices such as wearable health trackers and remote monitoring devices, are vulnerable to cyberattacks which compromise patient safety, privacy, and data integrity [22]. The paper [23] mentions that wearable medical devices connected to the IoT can improve the quality of care for patients, but they also pose threats and vulnerabilities that require attention and mitigative actions. [24] discusses the inadequate security and privacy precautions in IoMT devices, which can lead to patient health data leakage and cyberattacks on medical devices, compromising patient safety and data integrity.
	Data Integrity	Ensuring the accuracy and integrity of medical data is essential to make informed medical decisions [25]. The criticalness of data integrity issues in healthcare and the need for research in this field was highlighted in [26]
	Ransomware Threats	Hospitals and healthcare organizations are increasingly targeted by ransomware attacks [27], which disrupt critical medical services and compromise patient care until ransoms are paid. Ransomware attacks have a significant impact on emergency department workflow, acute patient care, and the personal wellbeing of healthcare providers [28]
	Lack of Cyber Awareness	Healthcare professionals might lack awareness of cybersecurity practices, leading to unintentional vulnerabilities, like falling victim to phishing attacks or inadvertently exposing patient data [29]. The paper [30] states that levels of awareness and education on cybersecurity were universally poor among the healthcare organizations surveyed, indicating a lack of cyber awareness among healthcare professionals.
	Regulatory Compliance	Adhering to privacy and healthcare regulations in a digital health environment is complex and demands effective cybersecurity measures to avoid legal and financial consequences [31].The importance of governing and understanding digitally stored healthcare information [32]
	Securing Telemedicine	As telemedicine becomes more prevalent, securing online patient-doctor interactions and medical consultations is vital to protect patient privacy and confidentiality [33]. The paper discusses the importance of security and privacy in telecare medicine information systems [34]. [35] discusses the need for regulations to provide legal protection for patients who use telemedicine services to prevent data misuse and cybercriminal attacks.

SDG	Key Challenge	Cybersecurity Concern
	Long-term Data Protection	Medical records contain sensitive information that might be relevant for a patient's lifetime; ensuring the security of this data over the long term is a significant challenge [36]. The challenge of long-term data protection and the need for protection schemes that can ensure the integrity and confidentiality of sensitive information, such as medical records, over extended periods of time [37]
SDG 4: Quality education	Digital Learning Platforms	The integration of digital technologies in education introduces vulnerabilities in online learning platforms, requiring robust security to protect student data and prevent disruptions [38]. According to [39], e-learning platforms collect and store large amounts of sensitive information, making them attractive targets for cybercriminals. Additionally, [40] found that the use of security and cyber security countermeasures had a significant effect on students' frequent use and participation in the e-learning system.
	Secure Online Assessments -	Conducting secure online exams and assessments is challenging due to the potential for cheating and the need to prevent unauthorized access to exam content [41]. Studies have highlighted the common challenges faced in online assessments, including cheating and plagiarism, issues faced by teachers in making and conducting online assessments, concerns raised by students, and technical and financial issues faced by institutions [42]. The integrity of online university assessments has been examined, revealing concerns such as students cheating and resource unavailability, hesitancy to adopt online assessment systems, and fear of losing examination integrity [43]
	Remote Learning Security	Ensuring the security of remote learning environments, including video conferencing and collaboration tools, is crucial to prevent unauthorized access and protect students' online safety [44]. The paper discusses the adoption of emergency remote learning during the COVID-19 pandemic and the security risks associated with it. It emphasizes the need for proactive measures to mitigate these risks and presents a security framework for remote learning environments [45]
	Educational Content Protection	Online educational content, including textbooks and proprietary resources, needs cybersecurity measures to prevent unauthorized distribution and piracy [46]. Content protection techniques, including encoding, scrambling, and authentication, are essential for ensuring the security and integrity of digital content [47]
SDG 5: Gender equality	Online Harassment and Cyberbullying	The digital landscape can amplify online harassment and cyberbullying, disproportionately affecting women and discouraging them from participating in online spaces [48]. The digital landscape amplifies these issues, disproportionately affecting women and discouraging their participation in online spaces [49]. Studies have shown that cyber violence and harassment in cyberspace have detrimental effects on women's social, economic, and psychological well-being [50]

SDG	Key Challenge	Cybersecurity Concern
	Data Privacy and Consent	Women's data privacy and consent can be compromised due to inadequate awareness, lack of control over personal data, and potential misuse of their information [51]. The existing techniques of consent processing are not transparent and may lead to data fiduciaries misusing the collected data for purposes other than specified in the consent [52]. Human-centric IoT-based systems often lack mechanisms for managing resources and data in the user domain, which can lead to problems related to transparency [53]. Data openness can generate significant social and economic benefits, but it also comes with risks to privacy and data protection, including risks to individuals and organizations [54].
	Online Recruitment and Trafficking	Cybercriminals can exploit digital platforms for recruitment into human trafficking networks, particularly targeting vulnerable women and girls [55]. Cyberbullying against women and girls, facilitated by the internet and mobile technologies, negatively affects their well-being and hinders gender equality [56]. Additionally, the internet-enabled platform economy has led to an increase in online mediated gig work opportunities, which can create human rights and sustainability concerns, particularly for gig workers who lack job security and employment benefits [57]. Furthermore, indicators of labor trafficking are prevalent in online job advertisements, highlighting the potential for exploitation in the labor market [58].
SDG 6: Clean water and sanitation	Data Integrity for Water Quality Monitoring	Ensuring the accuracy and reliability of data from sensors that monitor water quality is crucial to making informed decisions about water treatment and distribution [59]. The importance of accurate sensors in measuring water quality to ensure safe water [60].
	Water Infrastructure Disruption	Cyberattacks targeting water treatment facilities or distribution networks could disrupt water supply, potentially compromising public health and sanitation [61]. Deliberate contamination of water sources as part of a terrorist attack can have serious medical, public health, and economic consequences [62]. While no immediate correlation was found between disruptions to water, sanitation, and hygiene (WASH) and waterborne diseases in northeast Syria, further research is needed to explore the impact of conflict-associated damage to WASH infrastructure [63].
	Cross-border Water Management	Shared water resources require international cooperation; ensuring the cybersecurity of data exchanged between countries is essential for equitable water management [64]. Sustainable water management solutions have been found to have a significant impact on local communities and contribute to the fulfillment of SDG 6 [65]. The approach applied in stakeholder management within the Adriatic region also highlights the importance of stakeholders' contribution in addressing relevant issues and options for sustainable cross-border drinking water resources management, reinforcing SDG 6 targets [66].
	Emergency Response Systems	Securing communication and data systems used for emergency response in water-related disasters (floods, droughts, etc.) is crucial to

SDG	Key Challenge	Cybersecurity Concern
		effective crisis management [67]. The use of substitute communications solutions, such as analog two-way radio or unsecured internet access, during disasters can pose risks to NGOs and individuals due to reduced or unknown security properties [68][69]. These substitute solutions are often used when existing communications infrastructure is impaired or overwhelmed [70].
SDG 7: Affordable and clean energy	Energy Infrastructure Attacks	Cyberattacks targeting power plants, renewable energy installations, and distribution networks could lead to power outages and disruptions, impacting both energy availability and affordability [71]. The attacks result in power outages and disruptions, impacting the availability and affordability of energy [72]. Recent high-profile cyberattacks on energy infrastructures, such as the security breach of the Colonial Pipeline and attacks on Ukraine's power grid, have highlighted the vulnerability of energy grids to cyber threats [73].
	Data Privacy in Energy Usage	Smart meters and IoT devices collect data on energy consumption patterns; protecting this data is crucial to maintaining user privacy and preventing unauthorized access [74]. The paper [75] discusses the privacy concerns in smart metering and proposes a mechanism called UPriv-AC to protect customer privacy. It mentions that the interception of a third malicious entity or the data misuse by the utility could expose customer privacy.
	Renewable Energy Facility Security	Cybersecurity measures must be in place to safeguard renewable energy facilities like solar farms and wind turbines, which are digitally controlled and could be targeted by attackers [76]. A study demonstrated the impact of cybersecurity technologies on a virtualized wind energy site, showing that encryption and intrusion detection systems can effectively detect and quarantine adversaries, preventing physical impacts to the power system [77]. Another research proposed a cyber-attack detection model using synchrosqueezed wavelet transforms and convolutional neural networks to safeguard roof-PV generation systems from cyber threats [78].
	Critical Infrastructure Protection	Ensuring the security of critical energy infrastructure, such as power substations and transmission lines, is essential to prevent large-scale disruptions to energy supply [79]. The power sector in India is at risk due to increasing cyber incidences, and vulnerabilities in centralized systems can have a wide impact on the operation of the entire power system [80]. The failure of security systems in protecting power grids can lead to blackouts and other disruptions, as seen in the case of Ukraine [81].
SDG 8: Decent work and economic growth	Automation and Job Disruption	The rise of automation and AI-driven technologies could lead to job displacement, impacting economic growth and requiring strategies to retrain and reskill the workforce [82]. [83] highlights how automation can result in unemployment and underemployment, as well as deskilling of workers. [84]emphasizes that while job loss may occur, automation also creates new jobs and expands demand for existing ones.

SDG	Key Challenge	Cybersecurity Concern
	Cyber Threats to Economic Infrastructure	Attacks on critical economic infrastructure, such as financial systems and digital payment networks, could disrupt economic activities and stability [85]. The integration of digital technology in economic transformation introduces new risks and threats, necessitating governments to identify and minimize these risks to ensure the security of the national economy during the digital economic transformation [86]. The efficiency of measures developed to minimize risks and eliminate threats to national economic security depends on the quality and precision of the policies implemented [87].
	Digital Supply Chain Vulnerabilities	The digitalization of supply chains can introduce vulnerabilities that cyber attackers might exploit to disrupt production, affecting economic growth and stability [88]. The use of digital and electronic technologies in the supply chain has opened up various security threats and risks, widening the attack surface on the entire end-to-end supply chain [89]. Recent cybersecurity breaches have highlighted the economic, political, and social effects of such attacks, emphasizing that cybersecurity is now a supply chain issue [90]
	Small Business Cybersecurity	Small and medium-sized enterprises (SMEs) might lack the resources to implement robust cybersecurity measures, leaving them susceptible to cyberattacks that could hinder economic growth [91].The literature highlights that SMEs may struggle to comply with cybersecurity regulations and lack the expertise to ensure regulatory compliance [92]. Moreover, SMEs working together as part of a supply chain may be reluctant to share cybersecurity information, hindering their ability to address cybersecurity challenges collectively [93]. The specific threat of malware is emphasized, as non-compliance with adequate cybersecurity infrastructure leaves SMEs more vulnerable to malware attacks.
SDG 9: Industry, innovation and infrastructure	Critical Infrastructure Vulnerabilities	The integration of digital technologies in critical infrastructure, such as transportation and energy systems, introduces new points of vulnerability that cyber attackers could exploit [94]. The interconnected and interdependent nature of critical infrastructure systems, along with the lack of specialized mechanisms for knowledge-sharing in the field of industrial control systems (ICS) vulnerability management, further exacerbates the problem [95].
	IoT Security	The proliferation of IoT devices in industrial settings introduces potential entry points for cyber attackers seeking to compromise operational technology (OT) systems [96]. These devices, which are often small and have limited security mechanisms, can be vulnerable to attacks, putting the entire network at risk [97]. Implementing IoT solutions in industrial environments requires a comprehensive threat model and the application of information security controls and risk management frameworks to mitigate associated risks [98].
	Intellectual Property Theft	Industries reliant on innovation are vulnerable to cyberattacks that aim to steal trade secrets and intellectual property, hindering competitiveness and growth [99]. The theft of intellectual property has

SDG	Key Challenge	Cybersecurity Concern
		been a devastating challenge for the United States, with foreign countries targeting critical intangible assets [100].
	Ransomware Impact on Industry	Ransomware attacks targeting industries can halt production processes and disrupt supply chains, leading to financial losses and economic consequences [101]. These attacks can halt operations, disrupt critical infrastructure, and cause downtime, resulting in decreased productivity and revenue [102] [103] [104]
	Smart Manufacturing Vulnerabilities	The adoption of smart manufacturing and digital twins could lead to data breaches that impact the integrity of production processes and product quality [105]. The interconnected systems rely on accurate and trustworthy data from various parties, and any errors or inaccuracies in the data can have significant consequences [106]. Additionally, the increasing security threats, such as advanced persistent threats (APTs), pose a risk to the normal operations of smart manufacturing systems [107].
	Lack of Cybersecurity Standards	A lack of consistent cybersecurity standards in industrial environments can lead to fragmented security measures, making it easier for attackers to exploit weaknesses [108]. The increasing incidents of high-level damage caused by attackers using prepared and targeted methods, despite compliance with international information security standards and statutory requirements [109]. Industrial vulnerability assessment reports have highlighted these vulnerabilities, which occur due to limited or ill-defined security policies [110].
	Human-Machine Interface Security	Ensuring the security of interfaces between humans and machines, especially in industries like healthcare and transportation, is crucial to prevent unauthorized control and manipulation [111]. In collaborative automation systems, security and safety assessments are increasingly important, as improperly deployed systems can hide security threats and raise safety issues [112]. Additionally, in the telehealth system, machine learning can provide reliable protection against potential threats by continuously authenticating IoT devices and detecting insider attacks [113].
SDG 10: Reduced inequalities	Cyber Threats to Social Services	Vulnerabilities in digital platforms used for social assistance and support programs can disproportionately affect vulnerable populations, disrupting their access to essential services [114]. Cyberattacks targeting civil society groups can disrupt their activities and steal private information, which can hinder their ability to provide social services [115]. Additionally, the rise of online platforms has led to an increase in cyber social threats, including hate speech, misinformation, and gender-based stereotyping, which can further perpetuate inequalities and marginalize certain communities [116].
	Online Discrimination and Bias	The use of AI and algorithms can perpetuate biases and discrimination, deepening social inequalities in areas like job recruitment, lending, and resource allocation [117]. Examples of biases and discrimination in AI applications to healthcare have been identified based on race, ethnicity,

SDG	Key Challenge	Cybersecurity Concern
		gender, disability, and other factors [118]. In online two-sided markets, such as ride-sharing and freelance labor platforms, biases and discrimination against certain social groups have been observed, leading to unequal hiring opportunities and lower expected payoffs for minority workers [119].
SDG 11: Sustainable cities and communities	Smart City Vulnerabilities	The integration of IoT devices and digital technologies in smart cities introduces new attack vectors that could be exploited by cybercriminals to disrupt critical services and compromise citizen safety [120]. The use of Information and Communication Technology (ICT) in smart cities has contributed to a rise in safety threats, criminal use of information, and security and privacy challenges [121]. The increased deployment and use of digital infrastructure and processes in the name of sustainability and optimization is the focus of critical literature on smart cities [122].
	Data Privacy in Urban Systems	The collection and utilization of data for smart city operations can raise concerns about citizen privacy, requiring strong data protection measures [123]. Empirical evidence supports this, as studies have highlighted the need for privacy-preserving access control systems in smart city environments [124]. The development of sensor technologies and the Internet of Things (IoT) in smart cities has led to the generation of large amounts of data, making cybersecurity and privacy crucial issues [125].
	Cyber Attacks on Infrastructure	Critical urban infrastructure, such as transportation systems and utilities, could be targeted by cyberattacks, leading to disruptions in services and affecting the quality of life for residents [126]. The integration of emerging technologies in smart cities, such as connected and automated vehicles (CAVs), increases the risk of cyberattacks on the transportation domain [127]. These cyberattacks can compromise the decision-making capabilities of autonomous systems, leading to complicated CAV accidents.
	Safety of Autonomous Vehicles	As cities integrate autonomous vehicles, securing their communication and control systems becomes critical to prevent accidents and disruptions [128]. Studies have identified the security vulnerabilities and recommended mitigation techniques associated with different sensors, controllers, and connection mechanisms in autonomous and connected vehicles [129]. Cyber-attacks pose a significant risk to the performance and operations of autonomous vehicles, impacting both intra-vehicle systems and inter-vehicle systems [130].
	Protection of Public Wi-Fi	Public Wi-Fi networks are common in cities, and securing them is essential to prevent unauthorized access, data breaches, and potential cyber threats to users. [131] Empirical evidence has demonstrated that people who access public Wi-Fi networks are more likely to engage in risky behavior and expose their personal accounts to potential threats [132].

SDG	Key Challenge	Cybersecurity Concern
SDG 12: Responsible Consumption and Production	E-Waste and Data Security	The proliferation of electronic devices raises concerns about the disposal of electronic waste (e-waste) and the need to ensure data security when disposing of digital devices [133]. Improper disposal of e-waste result in the loss of resources and adverse impacts on health and the environment [134]
	Sustainable Manufacturing Vulnerabilities	Smart manufacturing and automation introduce cybersecurity risks that could impact the quality and sustainability of products [135]. The integration of digital systems with critical industries and their accessibility from the internet creates opportunities for cyber attacks [136]. The lack of a recognized methodology for cybersecurity decision-making in Industry 4.0 is a significant barrier to the development of sustainable manufacturing [137]. Additionally, the slow introduction of sustainable machine tools hampers the smart sustainability transition in the machine tools industry [138].
	Digital Greenwashing	Misleading claims about environmentally friendly products can undermine responsible consumption efforts; verifying the accuracy of such claims requires reliable data protection [139]. Zhang et al. found that digital transformation (DIT) can curb greenwashing behavior by enterprises, and government subsidies, resource slack, and public pressure positively moderate the relationship [140]. Ramtiyal et al. studied the impact of greenwashing by corporations on consumers' sustainable purchase behavior and found that corporate greenwashing has a negative effect on sustainable consumer behavior [141]. Another study by Ho and Forster showed that greenwashing perceptions significantly negatively affect green purchasing intentions, highlighting the detrimental effects of greenwashing in advertising on product sales [142].
	Energy-efficient Tech and Data Privacy	Using energy-efficient technologies can improve sustainability, but data privacy concerns must be addressed in connected devices and systems [143]. In the context of the Internet of Things (IoT), a framework has been developed to examine the energy cost of privatizing data while still ensuring utility and privacy for users [144]. Similarly, in the case of demand response implemented with blockchain, a system has been devised to preserve privacy using Secure Multiparty Computation (SMC) algorithms and a blockchain-based architecture [145]. Furthermore, in the medical and healthcare systems, a privacy-aware energy-efficient framework has been proposed to secure patient information and minimize communication costs [146].
SDG 13: Climate action	Cyber Threats to Environmental Monitoring	Attacks on systems that monitor climate and environmental data could compromise our ability to track and respond to climate change effectively [147]. In the paper by Abhijith et al., they discuss the importance of water quality monitoring sensors in water distribution systems (WDS) [148]. These sensors communicate over a cyberinfrastructure layer and are exposed to cyber-attacks. Similarly, Yang et al. propose a data sharing scheme for environmental monitoring using attribute-based encryption and cloud computing

SDG	Key Challenge	Cybersecurity Concern
		technology [149]. This scheme ensures the confidentiality, integrity, and verifiability of monitoring data, protecting it from malicious attacks. Furthermore, in the paper [150], it is mentioned that cyber-related hazards, including attacks on environmental monitoring systems, can be affected by mental formations such as the Finite Pool of Worry, which may lead to inaction.
	Renewable Energy Facility Security	Securing renewable energy facilities such as solar farms and wind turbines is essential to preventing disruptions in clean energy generation [151]. Empirical evidence from a study on a cyber-physical wind energy site demonstrated the effectiveness of cybersecurity technologies in preventing physical impacts and disruptions to the power system [152]
	Smart Transportation Resilience	As transportation becomes more connected and automated, ensuring the cybersecurity of smart transportation systems is vital for reducing carbon emissions [153]. As studies have shown the vulnerabilities and potential cyber-attack incidents in the transportation sector [154] [155]. The deployment of Internet of Things (IoT) in transportation applications has also highlighted the importance of cybersecurity measures such as secure data code, two-factor authentication, and end-to-end encryption [156]. Additionally, the presence of connectivity and complex interactions in connected transportation systems necessitates the resilience against cyber-attacks, which can be achieved through the fusion of physical and social signals for cyber-attack detection [157].
SDG 14: Life Below Water	Marine IoT Vulnerabilities	The deployment of IoT devices for marine monitoring introduces vulnerabilities that could be exploited to compromise marine ecosystem data and disrupt conservation efforts [158]. Empirical evidence supporting this includes the fact that the main consequences of unprotected connected devices in seaports are unauthorized access, theft of important information, and loss of information control [159]. Additionally, the implementation of Greengrass IoT at maritime environments involves running machine learning models at the edge, which requires the devices to make their own decisions and withstand intermittent network connectivity, posing potential security risks [160]. Furthermore, reliable and low latency communication techniques are crucial for reconstructing monitored phenomena in a timely manner, and the proposed architecture for underwater IoT includes analog biodegradable sensors and a correlation-aware Hybrid Automatic Repeat Request technique, both of which address security and energy efficiency concerns [161].
	Data Integrity for Ocean Monitoring	Ensuring the accuracy of data collected from sensors and devices used to monitor marine ecosystems is vital to make informed decisions for ocean conservation [162]. Karandikar et al. propose a solution called DataSafe, which utilizes docker and blockchain technology to enhance data standardization and integrity [163]. Subramanian et al. highlight the importance of automated mechanisms, such as the ADvanced Data REception and AnalysiS System (ADDRESS), for reliable data

SDG	Key Challenge	Cybersecurity Concern
		reception, analysis, and dissemination in ocean observation programs [164].
	Illegal Fishing and Cybercrime	Cybercriminals could exploit vulnerabilities in maritime tracking and enforcement systems, contributing to illegal fishing and damaging marine life [165]. Empirical evidence suggests that illegal fishing is prevalent globally and impacts the health of oceans, the sustainability and profitability of fisheries, and even acts to destabilize geopolitical relations [166]. While there is minimal evidence of organized crimes being directly linked to illegal fishing, violations of worker's rights, forced labor, and modern slavery are commonly associated with illegal fishing activities [167].
	Cyber Threats to Aquaculture	The aquaculture industry's adoption of digital technologies introduces new attack vectors that could affect fish farming operations and environmental sustainability [168]. These threats arise from the increasing reliance on computers and internet access in fish farming, making the industry vulnerable to cyber-attacks [169]. The use of IoT and smart technologies in farming environments has also exposed the industry to cybersecurity vulnerabilities and potential attacks [170].
	Pollution Monitoring Security	Systems that monitor marine pollution and plastic waste must be protected from cyberattacks that could compromise their accuracy and integrity [171]. The Internet of Things (IoT) has transformed traditional monitoring systems into high-tech solutions, but it also introduces vulnerabilities that can be exploited by attackers [172]. To address this challenge, researchers have developed secure IoT-WSN architectures for environmental monitoring, such as the proposed SIAEM system, which includes a Dynamic Security Scheme Manager (DSSM) to increase security [160].
SDG 15: Life on Land	Environmental Monitoring Vulnerabilities	The use of digital technologies and sensors for land ecosystem monitoring introduces vulnerabilities that could be exploited to compromise data accuracy and integrity [173].Pricope et al. discuss the challenges of operationalizing the integration of biophysical indicators of land degradation with climatic and socio-economic indicators, which can impact the accuracy and integrity of monitoring data [174].
	Data Protection for Biodiversity Tracking	Ensuring the security of data collected from biodiversity tracking systems is crucial to making informed decisions for land ecosystem conservation [175]. The increasing accessibility of large-scale biodiversity genomic datasets and the need for comprehensive data management practices highlight the importance of data security [176]. Additionally, the detection of species of concern in molecular biodiversity data requires stringent quality control standards to ensure the suitability of the data for decision-making [177].
	Wildlife Trafficking and Cybercrime	Cybercriminals could exploit weaknesses in systems tracking wildlife populations and conservation efforts, contributing to illegal wildlife trafficking [178]. Haas proposes a cybersecurity-based solution

SDG	Key Challenge	Cybersecurity Concern
		involving a confederation of criminal investigators to collect intelligence on wildlife cybercriminals and recommend actions to law enforcement [178]. Smart et al. discuss the potential of DNA marker systems and emerging molecular technologies to aid in the rapid identification of species and individuals involved in wildlife trafficking [179]
SDG 16: Peace, Justice and Strong Institutions	Cyber Attacks on Governance Systems	The increasing reliance on digital technologies in governance systems introduces vulnerabilities that could be exploited to disrupt public services and compromise democratic processes [180]. Empirical evidence supports this, as studies have shown that cyber-attacks have a significant impact on e-governance and can damage public trust [180]. These attacks pose a threat to the security and integrity of data, with the potential to manipulate information and undermine the governance system [181]. Organizations globally, including Nigeria, have been found to have inadequate data governance strategies in place, leaving them vulnerable to cybercrime incidents [182].
	Data Privacy and Human Rights	Ensuring data privacy in government systems is essential to prevent unauthorized access that could infringe upon citizens' human rights and civil liberties [183]. Martirosyan et al. [184] discuss the use of nontraditional data sources, such as social media, by national statistical offices to fill data gaps and involve citizens in the production of statistics. They highlight the challenges of representativity and quality assurance based on statistical standards used by NSOs. Similarly, the authors [54] explore the use of citizen reports on social media platforms to complete official records on human rights violations in Mexico. They emphasize the challenges and opportunities of migrating local knowledge from online communities to address institutional failures. Furthermore, [185] emphasize the need for privacy, data rights, and cybersecurity in the deployment of new technologies to achieve sustainable development goals.
	Cyber Threats to Legal Processes	Attacks targeting legal institutions and processes could compromise access to justice, impact fair trials, and undermine the rule of law [186]. The escalation of cyberattacks on critical infrastructure, such as the 2021 Colonial Pipeline ransomware attack, highlights the vulnerability of critical systems and the potential cascading consequences on national security and the economy [187]. Additionally, the increasing frequency and sophistication of cybercrimes necessitate strong international cooperation and harmonization of laws to effectively address the challenges [188]. The interconnectedness of critical infrastructure and the transnational nature of cyberattacks further emphasize the need for collaborative efforts in cybersecurity [189].

SDG	Key Challenge	Cybersecurity Concern
	Election Security	Ensuring the cybersecurity of election processes is vital to prevent manipulation, disinformation, and foreign interference that could undermine democratic institutions [190]. Election systems in the United States are diverse, making it challenging to develop a national picture of cybersecurity risk. Each state and jurisdiction needs to evaluate and prioritize risk in the systems it oversees [191]. Spreading false information about elections has the potential to undermine confidence in the electoral process and suppress voter turnout, particularly among marginalized communities [192]. Election misinformation poses a threat to democratic processes in the United States, with 64% of election officials reporting that spreading false information had made their jobs more dangerous [193]
	Secure Digital ID Systems	Developing secure digital identity systems is crucial for citizen access to government services while protecting against identity theft and misuse [194]. The implementation of digital identity programs without thorough consideration of cybersecurity and privacy increases the risk of cyberattacks and security vulnerabilities [195].
SDG 17: Partnerships for the goals	Global Data Sharing Security	Collaborative efforts among nations require secure data sharing to achieve the SDGs, while addressing concerns about data privacy, ownership, and misuse [196]. Empirical evidence shows that the need for secure and integrity-preserved data sharing has become increasingly important in the emerging era of changed demands on healthcare and increased awareness of the potential of data [197]. Within the context of the big data age, data sharing is gradually rising with the embodiment of data value. However, security problems such as centralized deployment, malicious theft, and tampering greatly affect the security of data [198]. Significant empirical evidence reveals that about 2.7 zettabytes of data in the digital universe are being threatened by cybercrime incidents that are on the rise globally. Only 67% of organizations globally deployed data governance or data intelligence solutions, highlighting the importance of leveraging good security measures for Sustainable Data Governance (SDG) [181].
	International Development Project Security	Digital platforms used for international development projects must be secure to prevent disruptions that could hinder progress towards the SDGs [199]. A study by Humayun et al. [200] identified secure software development (SSD) practices critical for global software development (GSD) projects. The study found that 16 out of 36 security practices were critical for GSD projects, highlighting the importance of incorporating security in the different phases of the GSD life cycle.

SDG	Key Challenge	Cybersecurity Concern
	Innovation Ecosystem Security	Promoting innovation for sustainable development demands secure environments for collaborative research and development [201]. Multi-stakeholder partnerships, managed by non-profit organizations, play a crucial role in facilitating sustainable development and collaborative innovation processes [202]. The Water Joint Programming Initiatives (JPIs) address water challenges in the context of the UN Sustainable Development Goals (SDGs), emphasizing the importance of research, innovation, and implementation of sustainable solutions [203].

From the review, a number of challenges on each SDG have been identified which was illustrated in Figure 1. From the analysis, SDG 3 (Good Health and Well-being) and SDG 9 (Industry, Innovation, and Infrastructure) face significant security challenges. SDG 3 deals with healthcare, where the increasing use of digital health technologies and medical devices can expose sensitive patient data and medical systems to cyber threats [204]. Therefore, ensuring patient privacy, data integrity, and reliable healthcare services becomes crucial. Meanwhile, SDG 9 encompasses various industries and technological advancements in IR 4.0, introducing vulnerabilities in critical infrastructure, supply chains and innovation processes. As industries become more interconnected, the potential for cyberattacks on manufacturing processes, transportation systems and energy networks also rises [205]. Apart from that, SDG 10 which focused on Reduced Inequalities appeared to have less number of security challenges compared to some other goals. However, the security challenges on this area are possibly not much explored; it is important to recognize that while the number might be fewer, but the underlying issues related to inequality and its intersection with technology and cybersecurity are still important. Above all, balancing innovation with cybersecurity measures becomes imperative to prevent disruptions and promote sustainable development.

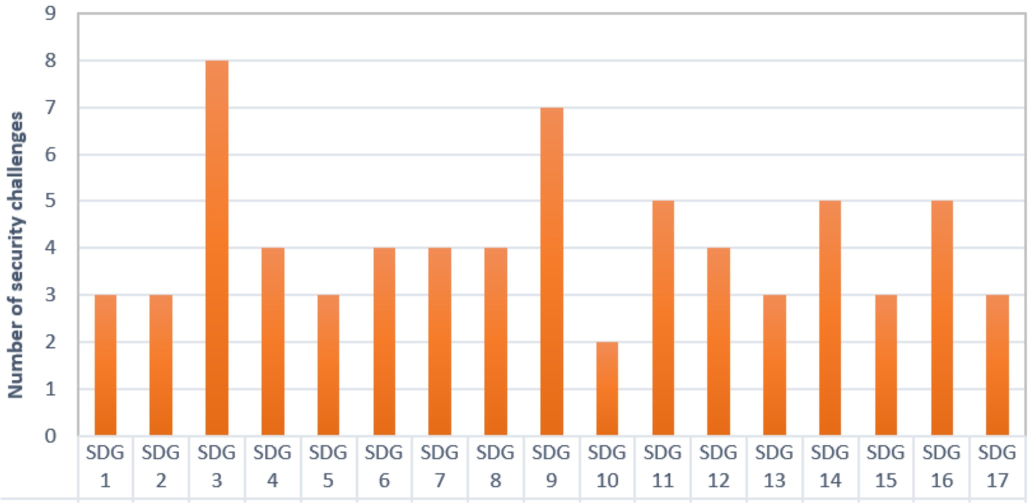

Figure 1. Security Challenges on Each SDG

4. Cyberattacks in SDGs

Cyberattacks not only pose immediate threats to individuals' digital identities and financial well-being but also extend their influence to the stability of nations and the integrity of democratic processes. The significance of cybersecurity is growing, impacting individuals, entities and entire countries. Malicious online activities including cyberattacks have the potential to jeopardize confidential data, interrupt public services and inflict economic damage. The work in [206] has identified five evolving threats in cybersecurity, which are ransomware attacks, IoT attacks, cloud attacks, phishing attacks and cryptocurrency and blockchain attacks.

These attacks are indeed vulnerable to the SDGs; each of these threats has the potential to impact various aspects of the 17 goals, depending on their scope and consequences. Taking motivation from this work [206], our aim is to discover the vulnerabilities associated with these five threats within the framework of the SDGs. An overview of how each threat could be vulnerable to the SDGs are explained as followed:

1. Ransomware Attack: This attack can disrupt critical services and organizations, impacting SDGs related to infrastructure, healthcare, and economic stability. For instance, if a healthcare facility is targeted and its operations are disrupted, this could affect SDG 3 (Good Health and Well-being) by hindering access to medical services [207]. Additionally, these attacks could also impact SDG 9 (Industry, Innovation, and Infrastructure) by disrupting critical industrial systems, hindering manufacturing processes and supply chains, thus impeding economic growth and innovation [208]. Moreover, SDG 11 (Sustainable Cities and Communities) could be affected through attacks on smart city infrastructure, potentially disrupting essential services and diminishing residents' quality of life as mentioned in [209].
2. IoT Attack: Attacks targeting IoT devices can compromise data privacy and security, potentially affecting SDGs related to innovation and industry. As IoT devices are increasingly used in sectors like agriculture (SDG 2)[210], energy (SDG 7)[211] and infrastructure (SDG 9)[212], their compromised security could hinder progress in these areas. In addition, SDG 6 (Clean Water and Sanitation) might be impacted due to compromised IoT sensors monitoring water quality [213], leading to inaccurate data and affecting decisions on water treatment and sanitation. Similarly, SDG 11 (Sustainable Cities and Communities) could suffer from vulnerable IoT devices in smart cities, compromising urban services and overall resilience in creating sustainable and inclusive cities [214].
3. Cloud Attack: This threat can lead to data breaches and service disruptions, impacting SDGs related to data privacy, information access, and industry innovation. Loss of valuable data could affect SDG 8 (Decent Work and Economic Growth), especially in industries relying heavily on cloud services [215]. Moreover, in the context of SDG 4 (Quality Education), cloud service disruptions could hinder access to online education platforms and digital learning materials, thereby affecting educational quality and inclusiveness [216]. Additionally, SDG 13 (Climate Action) could be impacted by data loss or breaches in cloud-stored environmental monitoring data, hindering accurate tracking of climate change progress [150].
4. Phishing Attack: It can compromise personal information, leading to identity theft and fraud, which could impact several SDGs. For instance, these attacks might affect SDG 16 (Peace, Justice, and Strong Institutions) by enabling fraud and facilitating illegal activities [217]. Moreover, SDG 5 (Gender Equality) could be influenced by these attacks, as cyberbullying and online harassment resulting from phishing attacks could disproportionately affect women and discourage their full participation in online spaces [218].
5. Blockchain Attack: Attacks on blockchain technology can disrupt secure transactions and data integrity, affecting SDGs related to financial inclusion, innovation, and information security. Blockchain's role in enhancing peace, justice and strong institutions (SDG 16) could be compromised if blockchain systems are attacked [219]. In addition, SDG 10 (Reduced Inequalities) might encounter challenges, as attacks on blockchain systems supporting transparent and secure transactions could undermine efforts to reduce inequalities by compromising trust and accountability [220].

Figure 2 depicts these vulnerabilities within the context of SDG. From the figure, it can be seen that each threat intersects with multiple SDGs, highlighting which goals are vulnerable to the five attacks. This visualization emphasizes the urgency of addressing cybersecurity issues as an integral part of achieving the SDGs. By recognizing the potential vulnerabilities that these threats pose to various aspects of sustainable development, researchers can be able to develop robust strategies to protect the critical systems and ensure the continued progress towards achieving the SDGs by year 2030.

In reflecting upon the cybersecurity challenges identified across the various SDGs, it becomes evident that the diversity and complexity inherent in these goals necessitate a nuanced approach to cybersecurity. Each SDG, with its unique challenges and objectives, requires a cybersecurity strategy that is as specialized and multifaceted as the goal itself. For example, the cybersecurity measures suited to SDG 3 (Good Health and Well-being), which must safeguard sensitive health data against breaches, differ significantly from those needed for SDG 9 (Industry, Innovation, and Infrastructure), where the focus is on protecting industrial control systems and innovation ecosystems from cyber threats. This diversity underscores the imperative for tailored cybersecurity solutions that not only address the specific vulnerabilities and threats facing each SDG but also support the overarching aim of sustainable development. It is clear that a one-size-fits-all approach to cybersecurity falls short when confronted with the broad spectrum of objectives covered by the SDGs.

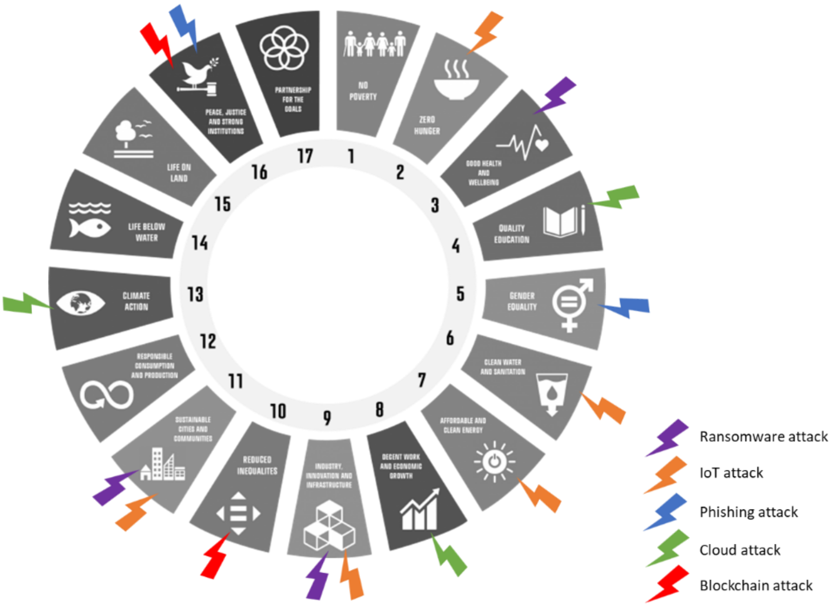
17
PARTNERSHIP FOR THE GOALS
1
NO POVERTY
2
ZERO HUNGER
3
GOOD HEALTH AND WELLBEING
4
QUALITY EDUCATION
5
GENDER EQUALITY
6
CLEAN WATER AND SANITATION
7
AFFORDABLE AND CLEAN ENERGY
8
DECENT WORK AND ECONOMIC GROWTH
9
INDUSTRY, INNOVATION AND INFRASTRUCTURE
10
REDUCED INEQUALITES
11
SUSTAINABLE CITIES AND COMMUNITIES
12
RESPONSIBLE CONSUMPTION AND PRODUCTION
13
CLIMATE ACTION
14
LIFE BELOW WATER
15
LIFE ON LAND
16
PEACE, JUSTICE AND STRONG INSTITUTIONS
Ransomware attack
IoT attack
Phishing attack
Cloud attack
Blockchain attack

Figure 2. Security Vulnerabilities within SDG

5. Conclusions

As a conclusion, this review paper has provided an insightful analysis of the alignment between cybersecurity challenges and the 17 Sustainable Development Goals (SDGs). By identifying and categorizing emerging threats such as ransomware attacks, IoT vulnerabilities, cloud breaches, phishing exploits and blockchain compromises, the paper sheds light on potential risks that could hinder progress towards the SDGs. This comprehensive review underscores the significant relationships between cybersecurity and each SDG, highlighting the need for proactive measures to counter these threats. The novel findings of this study emphasize the urgency of addressing cybersecurity concerns to ensure the successful achievement of the SDGs by 2030. It is evident that no aspect of sustainable development is immune to cyber threats, and neglecting cybersecurity could compromise the progress. The interconnected nature of these challenges demonstrates the need for a multidisciplinary and integrated approach that considers both digital security and broader development objectives. Cybersecurity is a global issue that requires international cooperation. Future efforts should focus on strengthening global frameworks and treaties on cybersecurity, promoting cross-border collaboration in cyber threat intelligence, and establishing international norms and standards for cybersecurity that support the SDGs. Apart from that, while the analysis has centered on the cybersecurity threats that pose risks to achieving the SDGs, the dual nature of cybersecurity as both a challenge and an opportunity for sustainable development is also recognized. Future research could fruitfully explore how proactive cybersecurity measures not only mitigate risks but also actively contribute to the realization of the SDGs by safeguarding digital innovations that support economic, social, and environmental progress. This broader perspective underscores the multifaceted role of cybersecurity in shaping a sustainable future.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Acknowledgements

The authors would like to thank the Universiti Teknologi MARA, 40450 Selangor, Malaysia for the support in publishing this paper.

Author contribution

The contribution to the paper is as follows: N. N. Mohamed, B. H. H. Abuobied: literature review study; N. N. Mohamed: analysis and interpretation of results; B. H. H. Abuobied: draft preparation. All authors approved the final version of the manuscript.

References and citations

[1] N. K. Arora and I. Mishra, "United Nations Sustainable Development Goals 2030 and environmental sustainability: race against time," *Environ. Sustain.*, vol. 2, no. 4, pp. 339–342, 2019, doi: 10.1007/s42398-019-00092-y.

[2] P. Seele and I. Lock, "The game-changing potential of digitalization for sustainability: possibilities, perils, and pathways," *Sustain. Sci.*, vol. 12, no. 2, pp. 183–185, 2017, doi: 10.1007/s11625-017-0426-4.

[3] E. Avdibasic, A. S. Toksanovna, and B. Durakovic, "Cybersecurity Challenges in Industry 4.0: A State of The Art Review," *Def. Secur. Stud.*, vol. 3, no. 8, pp. 32–49, 2022, doi: 10.37868/dss.v3.id188.

[4] M. Madden, M. Gilman, K. Levy, and A. Marwick, "Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans," *Wash. Univ. Law Q.*, vol. 95, no. 1, pp. 053–125, 2017.

[5] T. Mulyaningsih, R. Wahyunengseh, and S. Hastjarjo, "Poverty and digital divide: A study in urban poor neighborhoods," *J. Ilmu Sos. dan Ilmu Polit.*, vol. 24, no. 2, pp. 189–203, 2020, doi: 10.22146/JSP.52325.

[6] S. R. Sheikh Dawood, S. Ghazali, and N. Samat, "Digital divide and poverty eradication in the rural region of the northern Peninsular Malaysia," *Indones. J. Geogr.*, vol. 51, no. 2, pp. 172–182, 2019, doi: 10.22146/ijg.37758.

[7] A. D. M. Alan Gelb, *Identification Revolution: Can Digital ID be Harnessed for Development?* Brookings Institution Press, 2018.

[8] D. Gibson and C. Harfield, "Amplifying victim vulnerability: Unanticipated harm and consequence in data breach notification policy," *Int. Rev. Vict.*, vol. 29, no. 3, pp. 341–365, 2022.

[9] S. Das and S. Masiero, "The datafication of anti-poverty programmes: Evidence from the public distribution system in Karnataka," in *ACM International Conference Proceeding Series*, 2019, no. January 2019, doi: 10.1145/3287098.3287135.

[10] E. K. Clemons, R. V. Waran, S. Hermes, M. Schreieck, and H. Krcmar, "Computing and Social Welfare: Minimizing societal harm from digital transformation while preserving the benefits of innovation in online businesses," *Electron. Mark.*, vol. 32, no. 2, pp. 417–436, 2022, doi: 10.1007/s12525-021-00512-0.

[11] B. Faith, T. Roberts, and K. Hernandez, "Risks, Accountability and Technology Thematic Working Paper," 2022. doi: DOI: 10.19088/BASIC.2022.003.

[12] J. Clapp and W. G. Moseley, "This food crisis is different: COVID-19 and the fragility of the neoliberal food security order," *J. Peasant Stud.*, vol. 47, no. 7, pp. 1393–1417, 2020, doi: 10.1080/03066150.2020.1823838.

[13] H. C. Verma, S. Srivastava, T. Ahmed, and N. A. Usmani, *Cyber Threats in Agriculture and the Food Industry: An Indian Perspective*. 2023.

[14] S. Deng, J. Zhang, D. Wu, Y. He, X. Xie, and X. Wu, "A Quantitative Risk Assessment Model for Distribution Cyber-Physical System Under Cyberattack," *IEEE Trans. Ind. Informatics*, vol. 19, no. 3, pp. 2899–2908, 2023, doi: 10.1109/TII.2022.3169456.

[15] J. L. Ferris, *Data privacy and protection in the agriculture industry: is federal regulation necessary*, vol. 18, no. 1. 2017.

[16] A. Bergstrom *et al.*, "Protecting farm privacy while researching large-scale unmanned aircraft systems platforms for agricultural applications," *Agron. J.*, no. July 2021, pp. 2700–2714, 2022, doi: 10.1002/agj2.21054.

[17] K. E. Ajambo Susan, Ogutu Sylvester, Birachi Eliud, *Digital agriculture platforms: Understanding innovations in rural finance and logistics in Uganda's agrifood sector*. Intl Food Policy Res Inst, 2023.

[18] G. Kariuki-Njogu, A. Njeru, and T. Olweny, "Influence of Technology Adoption on Credit Access among Small Holder Farmers: A Double-Hurdle Analysis," *Africa Int. J. Manag. Educ. Gov. Africa Int. J. Manag. Educ. Gov. © Oasis Int. Consult. Journals*, vol. 2, no. 3, pp. 60–74, 2017, [Online]. Available: www.oasiseduconsulting.com.

[19] L. N. KÜÇÜKARPACI and S. ÜLEV, "Developed Agricultural Fintech (Agri-Fintech) Solutions for Financing Problems of Farmers: A Critical Evaluation from the Perspective of Islamic Finance," *Int. J. Islam. Econ. Financ. Stud.*, vol. 9, no. 1, pp. 33–60, 2023, doi: 10.54427/ijisef.1218516.

[20] S. Zeadally, J. T. Isaac, and Z. Baig, "Security Attacks and Solutions in Electronic Health (E-health) Systems," *J. Med. Syst.*, vol. 40, no. 12, 2016, doi: 10.1007/s10916-016-0597-z.

[21] K. Ramar, P. V. Gopirajan, H. Shanmugasundaram, B. P. Andraju, and S. Baskar, "Digital Healthcare using Blockchain," in *2022 1st International Conference on Computational Science and Technology, ICCST 2022 - Proceedings*, 2022, pp. 651–655, doi: 10.1109/ICCST55948.2022.10040411.

[22] M. Papaioannou *et al.*, "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, pp. 1–15, 2022, doi: 10.1002/ett.4049.

[23] R. M. Czekster, P. Grace, C. Marcon, F. Hessel, and S. C. Cazella, "Challenges and Opportunities for Conducting Dynamic Risk Assessments in Medical IoT," *Appl. Sci.*, vol. 13, no. 13, 2023, doi: 10.3390/app13137406.

[24] F. K. Shaikh, S. Zeadally, and E. Exposito, "Enabling Technologies for Green Internet of Things," *IEEE Syst. J.*, pp. 1–12, 2015.

[25] F. Leal *et al.*, "Smart Pharmaceutical Manufacturing: Ensuring End-to-End Traceability and Data Integrity in Medicine Production," *Big Data Res.*, vol. 24, p. 100172, 2021, doi: 10.1016/j.bdr.2020.100172.

[26] A. K. Pandey *et al.*, "Key Issues in Healthcare Data Integrity: Analysis and Recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020, doi: 10.1109/ACCESS.2020.2976687.

[27] H. T. Neprash *et al.*, "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," *JAMA Heal. Forum*, vol. 3, no. 12, p. E224873, 2022, doi: 10.1001/jamahealthforum.2022.4873.

[28] L. S. van Boven *et al.*, "Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals," *Ann. Emerg. Med.*, vol. 83, no. 1, pp. 46–56, 2024, doi: 10.1016/j.annemergmed.2023.04.025.

[29] I. Singh and Y. Singh, "Cyber-Security Knowledge and Practice of Nurses in Private Hospitals in Northern Durban, Kwazulu-Natal," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 1, pp. 246–267, 2022.

[30] N. O. Brien, M. Durkin, and A. Darzi, "Cybersecurity in healthcare: Comparing cybersecurity maturity and experiences across global healthcare organizations," 2020. doi: 10.2196/preprints.24203.

[31] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity Enterprises Policies: A Comparative Study," *Sensors*, vol. 22, no. 2, pp. 1–35, 2022, doi: 10.3390/s22020538.

[32] A. Castanheira, H. Peixoto, and J. Machado, "Overcoming Challenges in Healthcare Interoperability Regulatory Compliance," 2020.

[33] N. AlOsail, D., Amino, N., Mohammad, "Security Issues and Solutions in E-Health and Telemedicine," *Lect. Notes Data Eng. Commun. Technol.*, vol. 66, pp. 305–318, 2021.

[34] K. Chatterjee, "A Secure Three Factor-Based Authentication Scheme for Telecare Medicine Information Systems With Privacy Preservation," *Int. J. Inf. Secur. Priv.*, vol. 16, no. 1, p. 24, 2022.

[35] S. P. Yuninda, S. Aga Pasma, and T. Mantoro, "Patient Data Security in Telemedicine Services from Data Misuse in Health Practice," in *IEEE 8th International Conference on Computing, Engineering and*

Design, *ICCED 2022*, 2022, pp. 1–4, doi: 10.1109/ICCED56140.2022.10010685.

[36] A. Esther Omolara, A. Jantan, O. I. Abiodun, H. Arshad, K. V. Dada, and E. Emmanuel, "HoneyDetails: A prototype for ensuring patient's information privacy and thwarting electronic health record threats based on decoys," *Health Informatics J.*, vol. 26, no. 3, pp. 2083–2104, 2020, doi: 10.1177/1460458219894479.

[37] M. Geihs, "Long-Term Protection of Integrity and Confidentiality," 2018.

[38] A. Oke and F. A. P. Fernandes, "Innovations in teaching and learning: Exploring the perceptions of the education sector on the 4th industrial revolution (4IR)," *J. Open Innov. Technol. Mark. Complex.*, vol. 6, no. 2, p. 31, 2020, doi: 10.3390/JOITMC6020031.

[39] R. Vivek, "Sustainable Strategic Management for Online Platforms in Higher Education: Practices and Challenges," *Malaysian E Commer. J.*, vol. 6, no. 1, pp. 29–35, 2022, doi: 10.26480/mecj.01.2022.29.35.

[40] S. Ghanem, "E-learning in Higher Education to Achieve SDG 4: Benefits and Challenges," 2020, doi: 10.1109/IEEECONF51154.2020.9319981.

[41] T. Susnjak, "ChatGPT: The End of Online Exam Integrity?," pp. 1–21, 2022, [Online]. Available: http://arxiv.org/abs/2212.09292.

[42] C. C. Glava, "Mechanisms for Objectivity Ensuring and Fraud Prevention in the Online Academic Assessment," *Educ. 21*, no. 23, pp. 136–142, 2022, doi: 10.24193/ed21.2022.23.13.

[43] I. Hilliger, J. A. Ruipérez-Valiente, G. Alexandron, and D. Gašević, "Trustworthy remote assessments: A typology of pedagogical and technological strategies," *J. Comput. Assist. Learn.*, vol. 38, no. 6, pp. 1507–1520, 2022, doi: 10.1111/jcal.12755.

[44] S. F. Huang, R.H., Liu, D.J., Zhu, L.X., Chen, H.Y., Yang, J.F., Tlili, A., Fang, H.G., Wang, *Personal Data and Privacy Protection in Online Learning : Guidance for Students, Teachers and Parents*, vol. 10. Beijing: Smart Learning Institute of Beijing Normal University, 2020.

[45] A. Asante, V. Amankona, M. Opoku, C. Srekumah, and A. K. Peprah, "Securing Remote Learning Environments," in *ACM International Conference Proceeding Series*, 2021, pp. 84–88, doi: 10.1145/3473465.3473480.

[46] M. A. Rahman, "Designing Copyright Laws to Combat Digital Piracy and Effectively Balance Proprietary and Public Interests in Bangladesh," Law School Macquarie University, 2019.

[47] N. Memon and P. W. Wong, "Protecting Digital Media Content," *Commun. ACM*, vol. 41, no. 7, pp. 35–43, 1998, doi: 10.1145/278476.278485.

[48] J. Vitak, K. Chadha, L. Steiner, and Z. Ashktorab, "Identifying women's experiences with and strategies for mitigating negative effects of online harassment," in *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*, 2017, pp. 1231–1245, doi: 10.1145/2998181.2998337.

[49] H. Khan, D. T. Basharat, and D. I. Hayat, "An Analytical Study of Unveiling Gender-Based Harassment in Cyberspace: An Exploration of Realities and Experiences," *Eur. PMC*, 2023, doi: 10.20944/preprints202306.0813.v1.

[50] F. Kurasawa, E. Rondinelli, and G. Kilicaslan, "Evidentiary activism in the digital age: On the rise of feminist struggles against gender-based online violence," *Information, Commun. Soc.*, vol. 24, no. 14, pp. 2174–2194, 2021.

[51] D. Almeida, K. Shmarko, and E. Lomas, "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 Ethics*, vol. 2, no. 3, pp. 377–387, 2022, doi: 10.1007/s43681-021-00077-w.

[52] R. G. Singh and S. Ruj, "Encoding of security properties for transparent consent data processing," in *2023 IEEE Guwahati Subsection Conference, GCON 2023*, 2023, pp. 1–8, doi: 10.1109/GCON58516.2023.10183463.

[53] J. E. Rivadeneira, M. B. Jiménez, R. Marculescu, A. Rodrigues, F. Boavida, and J. S. Silva, "A Blockchain-Based Privacy-Preserving Model for Consent and Transparency in Human-Centered Internet of Things," in *IoTDI '23: Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation*, 2023, pp. 301–314, doi: 10.1145/3576842.3582379.

[54] C. Biesmans *et al.*, "Responding to Societal Challenges with Data Access, Sharing, Stewardship Control OECD Digital and Control," OECD Publishing, Paris, 2022. doi: https://doi.org/10.1787/2182ce9f-en.

[55] A. T. Vivrette, “Approach to the Global Human Trafficking Crisis: Analyzing Applications of Social Network Analysis,” Graduate School of Vanderbilt University, 2022.

[56] C. Y. Luk, *The Human Rights-Based Approach to Combat Cyberbullying Against Women and Girls*. 2022.

[57] F. Lari-Williams and W. Verheyen, “Combating Slavery at the Doorstep: Implementing SDGs in the Gig Economy,” in *Young Universities for the Future of Europe (YUFE) Law Conference Proceedings No. 01/2022*, 2023, vol. 9, no. 1, pp. 157–162, doi: 10.1017/iop.2015.129.

[58] A. Volodko, E. Cockbain, and B. Kleinberg, “‘Spotting the signs’ of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers,” *Trends Organ. Crime*, vol. 23, no. 1, pp. 7–35, 2020, doi: 10.1007/s12117-019-09376-5.

[59] K. Nova, “AI-Enabled Water Management Systems : An Analysis of System Components and Interdependencies for Water Conservation,” *Eig. Rev. Sci. Technol.*, vol. 8, no. 1, pp. 106–124, 2023.

[60] M. Lamrini, Q. A. Quevy, M. Yassin Chkouri, and A. Touhafi, “Data Integrity Analysis of Water Quality Sensors and Water Quality Assessment,” in *IECON Proceedings (Industrial Electronics Conference)*, 2022, pp. 1–6, doi: 10.1109/IECON49645.2022.9968643.

[61] H. H. Addeen, Y. Xiao, J. Li, and M. Guizani, “A survey of cyber-physical attacks and detection methods in smart water distribution systems,” *IEEE Access*, vol. 9, pp. 99905–99921, 2021, doi: 10.1109/ACCESS.2021.3095713.

[62] R. Sharma and O. R. Katoch, “Analysis of the Targets and Progress toward Meeting the 2030 Sustainable Development Goal - 6 on Clean Water and Sanitation: Evidence from India,” *South Asian J. Soc. Stud. Econ.*, vol. 15, no. 3, pp. 16–26, 2022, doi: 10.9734/sajsse/2022/v15i330407.

[63] R. Bhattacharya, A. Kumari, and D. Bose, “Impact of Covid-19 on SDG 6 and Integrated Approaches for Clean Water Access and Sanitation,” *Sustain. Clim. Chang.*, vol. 15, no. 5, 2022.

[64] R. Moorthy and S. Bibi, “Water Security and Cross-Border Water Management in the Kabul River Basin,” *Sustain.*, vol. 15, no. 792, pp. 1–14, 2023, doi: 10.3390/su15010792.

[65] F. Lara-Valencia *et al.*, “Water Management on the U.S.-Mexico Border: Achieving Water Sustainability and Resilience through Cross-Border Cooperation,” *J. Borderl. Stud.*, vol. 38, no. 2, pp. 323–334, 2023, doi: 10.1080/08865655.2023.2168294.

[66] I. Franco, T. Ellennderbyshire, and J. Editors, “SDG 6 Clean Water and Sanitation: Sustainable Use of Energy and Water Resources in the Mining Sector: A Comparative Case Study of Open-Pit and Alluvial Mining Technology,” in *Actioning the Global Goals for Local Impact*, no. January, 2020, pp. 173–185.

[67] P. J. Ward *et al.*, “The need to integrate flood and drought disaster risk reduction strategies,” *Water Secur.*, vol. 11, no. 2020, pp. 1–14, 2020, doi: 10.1016/j.wasec.2020.100070.

[68] J. Korhonen, W. Otieno, and D. Berod, “Hydrological Data Sharing is a key for Sustainable Development and building Early Warning Systems,” 2024.

[69] E. Shittu, G. Parker, and N. Mock, “Improving communication resilience for effective disaster relief operations,” *Environ. Syst. Decis.*, vol. 38, no. 3, pp. 379–397, 2018, doi: 10.1007/s10669-018-9694-5.

[70] F. Alvarez, M. Hollick, and P. Gardner-Stephen, “Maintaining both availability and integrity of communications: Challenges and guidelines for data security and privacy during disasters and crises,” in *GHTC 2016 - IEEE Global Humanitarian Technology Conference: Technology for the Benefit of Humanity, Conference Proceedings*, 2016, pp. 62–69, doi: 10.1109/GHTC.2016.7857261.

[71] Z. Li, M. Shahidehpour, and X. Liu, “Cyber-secure decentralized energy management for IoT-enabled active distribution networks,” *J. Mod. Power Syst. Clean Energy*, vol. 6, no. 5, pp. 900–917, 2018, doi: 10.1007/s40565-018-0425-1.

[72] O. R. Katoch, S. Sehgal, R. Sharma, and A. Nawaz, “Analysis of the Targets and Progress toward Meeting the 2030 Agenda for SDG 7 on Affordable and Clean Energy: Evidence from India,” *J. Energy Res. Rev.*, vol. 12, no. 4, pp. 92–102, 2022, doi: 10.9734/jenrr/2022/v12i4251.

[73] M. Kalinin, D. Zegzhda, and E. Zavadskii, “Protection of Energy Network Infrastructures Applying a Dynamic Topology Virtualization,” *Energies*, vol. 15, no. 11, 2022, doi: 10.3390/en15114123.

[74] F. Dalipi and S. Y. Yayilgan, “Security and privacy considerations for IoT application on smart grids: Survey and research challenges,” in *4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud*, 2016, pp. 63–68, doi: 10.1109/W-FiCloud.2016.28.

[75] T. B. De Castro and N. C. Fernandes, "UPriv-AC: A Privacy-Preserving Mechanism for Smart Metering Against Curious Utility," in *2022 IEEE Latin-American Conference on Communications, LATINCOM 2022*, 2022, pp. 1–6, doi: 10.1109/LATINCOM56090.2022.10000456.

[76] S. N. G. Gourisetti *et al.*, "Standardization of the Distributed Ledger Technology cybersecurity stack for power and energy applications," *Sustain. Energy, Grids Networks*, vol. 28, no. 100553, pp. 1–23, 2021, doi: 10.1016/j.segan.2021.100553.

[77] L. Haghnegahdar and Y. Wang, "Cyber security and risk analysis in power systems," in *IISE Annual Conference and Expo 2018*, 2018, no. May 2018, pp. 1450–1455.

[78] W. Qiu, K. Sun, K. J. Li, Y. Li, J. Duan, and K. Zhu, "Cyber-Attack Detection: Modeling and Roof-PV Generation System Defending," *IEEE Trans. Ind. Appl.*, vol. 59, no. 1, pp. 160–168, 2023, doi: 10.1109/TIA.2022.3213629.

[79] C. Medina, C. R. M. Ana, and G. González, "Transmission Grids to Foster High Penetration of Large-Scale Variable Renewable Energy Sources -A Review of Challenges, Problems, and Solutions," *Int. J. Renew. Energy Res.*, vol. 12, no. 1, pp. 146–169, 2022, doi: 10.20508/ijrer.v12i1.12738.g8400.

[80] "Cyber-Physical Security and Critical Infrastructures," *International Security Ligue*, no. February, 2022.

[81] Nurfarah Nidatya, Muhammad Kamil Ghiffary Abdurrahman, Dini Putri Saraswati, "Securitisation of Ukrainian Critical Infrastructures: The Case of the Failure of SCADA System in Protecting the Power Grids," *J. Mandala J. Ilmu Hub. Int.*, vol. 5, no. 2, pp. 152–172, 2022, doi: 10.33822/mjihi.v5i2.4878.

[82] L. Li, "Reskilling and Upskilling the Future-ready Workforce for Industry 4.0 and Beyond," *Inf. Syst. Front.*, p. 1016, 2022, doi: 10.1007/s10796-022-10308-y.

[83] M. K. Bisht, "Automatization as a Challenge for Employment of Skilled Manpower: An Empirical Investigation from HRM perspective," *Psychol. Educ.*, vol. 55, no. 1, pp. 470–477, 2023, doi: 10.48047/pne.2018.55.1.58.

[84] A. Brown, H. Safford, and D. Sperling, *Historical perspectives on managing automation and other disruptions in transportation*. 2019.

[85] C. Adelmann, F., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, M.T., Morozova, A., Schwarz, N. and Wilson, *Cyber risk and financial stability: It's a small world after all*. International Monetary Fund, 2020.

[86] H. Kreinin and E. Aigner, *From "Decent work and economic growth" to "Sustainable work and economic degrowth": a new framework for SDG 8*, vol. 49, no. 2. Springer US, 2022.

[87] M. Maphiri, M. A. Matasane, and G. Mudimu, "Challenges to the Effective Implementation of SDG 8 in Creating Decent Work and Economic Growth in the Southern African Hemisphere: Perspectives from South Africa, Lesotho and Zimbabwe," in *Global Challenges to CSR and Sustainable Development*, Springer, 2021, pp. 39–63.

[88] Y. Li, K. Chen, S. Collignon, and D. Ivanov, "Ripple effect in the supply chain network: Forward and backward disruption propagation, network health and firm vulnerability," *Eur. J. Oper. Res.*, vol. 291, no. 3, pp. 1117–1131, 2021, doi: 10.1016/j.ejor.2020.09.053.

[89] B. Hammi, S. Zeadally, and J. Nebhen, "Security Threats, Countermeasures, and Challenges of Digital Supply Chains," *ACM Comput. Surv.*, vol. 55, no. 1, 2023, doi: 10.1145/3588999.

[90] S. A. Melnyk, T. Schoenherr, C. Speier-Pero, C. Peters, J. F. Chang, and D. Friday, "New challenges in supply chain management: cybersecurity across the supply chain," *Int. J. Prod. Res.*, vol. 60, no. 1, pp. 162–183, 2022.

[91] A. Chidukwani, S. Zander, and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," *IEEE Access*, vol. 10, no. July, pp. 85701–85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[92] A. B. A. Ali, R. K. Ayyasamy, R. Akbar, V. A. Ponnusamy, and L. E. Heng, "Cybersecurity Infrastructure adoption Model for Malware Mitigation in Small Medium Enterprises (SME)," in *2022 IEEE 5th International Symposium in Robotics and Manufacturing Automation*, 2022, no. August, pp. 1–6, doi: 10.1109/ROMA55875.2022.9915696.

[93] E. B. Cahyono, S. B. M. Sam, N. H. B. Hassan, N. Mohamed, N. Ahmad, and Y. Yusuf, "A Review on Cyber Resilience Model in Small and Medium Enterprises," in *4th International Conference on Smart Sensors and Application: Digitalization for Societal Well-Being, ICSSA 2022*, 2022, pp. 114–119, doi: 10.1109/ICSSA54161.2022.9870952.

[94] L. Marti, “Cyber-attacks against critical infrastructure,” in *Cyber Security: Critical Infrastructure Protection*, Springer International Publishing, 2022, pp. 3–42.

[95] S. Adepu, E. Kang, and A. P. Mathur, “Challenges in secure engineering of critical infrastructure systems,” in *34th IEEE/ACM International Conference on Automated Software Engineering Workshops*, 2019, no. 1, pp. 61–64, doi: 10.1109/ASEW.2019.00030.

[96] S. Akailvi, U. Gautam, P. Bhandari, H. Rashid, P. D. Huff, and J. P. Springer, “HELOT-Hunting Evil Life in Operational Technology,” *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3058–3071, 2022, doi: 10.1109/TSG.2022.3222261.

[97] J. McNett, J. McNett, and X. Su, “IoT Security in Industry: A Threat Model of Existing and Future Network Infrastructure,” *J. Appl. Secur. Res.*, vol. 19, no. 1, pp. 1–19, 2022.

[98] R. J. Raimundo and A. T. Rosário, “Cybersecurity in the Internet of Things in Industrial Management,” *Appl. Sci.*, vol. 12, no. 3, 2022, doi: 10.3390/app12031598.

[99] D. Halbert, “Intellectual property theft and national security: Agendas and assumptions,” *Inf. Soc.*, vol. 32, no. 4, pp. 256–268, 2016, doi: 10.1080/01972243.2016.1177762.

[100] K. L. McLaughlin, “SECURING CORPORATE IoT DEVICES: CHALLENGES, STRATEGIES, AND THE ROLE OF AI AND ML IN CYBERSECURITY,” *EDP Audit. Control. Secur. Newsl.*, vol. 67, no. 4, 2023.

[101] M. Crosignani, M. Macchiavelli, and A. F. Silva, “Pirates without borders: The propagation of cyberattacks through firms’ supply chains,” *J. financ. econ.*, vol. 147, no. 2, pp. 432–448, 2023, doi: 10.1016/j.jfineco.2022.12.002.

[102] D. P. F. Möller, “Ransomware Attacks and Scenarios: Cost Factors and Loss of Reputation,” in *Guide to Cybersecurity in Digital Transformation*, Springer, Cham, 2023.

[103] C. Lamers, E. Spoerl, G. Levey, N. Choudhury, and M. Ahmed, “Ransomware: A Threat to Cyber Smart Cities,” in *Cybersecurity for Smart Cities. Advanced Sciences and Technologies for Security Applications.*, Springer, Cham, 2023.

[104] U. Javed Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, “Ransomware Threat and its Impact on SCADA,” 2019, doi: 10.1109/ICGS3.2019.8688327.

[105] E. Karaarslan and M. Babiker, “Digital Twin Security Threats and Countermeasures: An Introduction,” in *International Conference on Information Security and Cryptology*, 2021, pp. 7–11, doi: 10.1109/ISCTURKEY53027.2021.9654360.

[106] J. Wu, M. Dong, K. Ota, J. Li, and W. Yang, “Sustainable Secure Management against APT Attacks for Intelligent Embedded-Enabled Smart Manufacturing,” *IEEE Trans. Sustain. Comput.*, vol. 5, no. 3, pp. 341–352, 2020, doi: 10.1109/TSUSC.2019.2913317.

[107] E. O’Connell, W. O’Brien, M. Bhattacharya, D. Moore, and M. Penica, “Digital Twins: Enabling Interoperability in Smart Manufacturing Networks,” *Telecom*, vol. 4, no. 2, pp. 265–278, 2023, doi: 10.3390/telecom4020016.

[108] I. Tasheva, “Cybersecurity post-COVID-19: Lessons learned and policy recommendations,” *Eur. View*, vol. 20, no. 2, pp. 140–149, 2021, doi: 10.1177/17816858211059250.

[109] B. Babu, T. Ijyas, P. Muneer, and J. Varghese, “Security issues in SCADA based industrial control systems,” in *2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017*, 2017, pp. 47–51, doi: 10.1109/Anti-Cybercrime.2017.7905261.

[110] T. Gasiba, U. Lechner, and M. Pinto-Albuquerque, “CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments,” *Lect. Notes Inf. Syst. Organ.*, vol. 47, pp. 370–387, 2021, doi: 10.1007/978-3-030-86797-3_25.

[111] T. K. Sung, “Industry 4.0: A Korea perspective,” *Technol. Forecast. Soc. Change*, vol. 132, no. November 2017, pp. 40–45, 2018, doi: 10.1016/j.techfore.2017.11.005.

[112] S. Plósz, C. Schmittner, and P. Varga, “Combining Safety and Security Analysis for Industrial Collaborative Automation Systems,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10489, doi: 10.1007/978-3-319-66284-8.

[113] B. Gebru *et al.*, “A Review on Human-Machine Trust Evaluation: Human-Centric and Machine-Centric Perspectives,” *IEEE Trans. Human-Machine Syst.*, vol. 52, no. 5, pp. 952–962, 2022, doi:

10.1109/THMS.2022.3144956.

[114] K. Karos *et al.*, "The social threats of COVID-19 for people with chronic pain," *Pain*, vol. 161, no. 10, pp. 2229–2235, 2020, doi: 10.1097/j.pain.0000000000002004.

[115] D. R. A. Schallmo and J. Tidd, *Digitalization Approaches, Case Studies, and Tools for Strategy, Transformation and Implementation Management for Professionals*. 2021.

[116] N. Žganec, "Developing Smart Social Services for Mending the Gap in Development Inequalities," *Eur. Soc. Work Educ. Pract. Pract. Soc. Work Deprived Communities*, pp. 177–190, 2021.

[117] M. L. Smith and S. Neupane, *Artificial intelligence and human development Toward a research agenda*. 2018.

[118] F. Monachou and I. Ashlagi, "Discrimination in online markets: Effects of social bias on learning from reviews and policy design," *Adv. Neural Inf. Process. Syst.*, vol. 32, no. NeurIPS, 2019.

[119] A. Kelly-Lyth, "Challenging Biased Hiring Algorithms," *Oxf. J. Leg. Stud.*, vol. 41, no. 4, pp. 899–928, 2021.

[120] K. Nova, "Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence Kannan Nova," *Int. J. Inf. Cybersecurity*, vol. 6, no. 1, pp. 21–42, 2022.

[121] M. Houichi, F. Jaidi, and A. Bouhoula, "Analysis of Smart Cities Security: Challenges and Advancements," *Proc. 2022 15th IEEE Int. Conf. Secur. Inf. Networks, SIN 2022*, pp. 1–5, 2022, doi: 10.1109/SIN56466.2022.9970494.

[122] B. J. R. Figueiredo, R. L. de C. Costa, L. Santos, and C. Rabadão, "Cybersecurity and Privacy in Smart Cities for Citizen Welfare," in *Smart Cities, Citizen Welfare, and the Implementation of Sustainable Development Goals*, 2022, p. 25.

[123] R. Kitchin, "The ethics of smart cities and urban science," *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.*, vol. 374, no. 2083, 2016, doi: 10.1098/rsta.2016.0115.

[124] C. Chakraborty, J. C. W. Lin, and M. Alazab, "Privacy Issues of Smart Cities: Legal Outlook," in *Data-Driven Mining, Learning and Analytics for Secured Smart Cities*, no. May, 2021.

[125] P. M. Kumar, B. Rawal, and J. Gao, "Blockchain-enabled Privacy Preserving of IoT Data for Sustainable Smart Cities using Machine Learning," in *14th International Conference on COMmunication Systems and NETworkS, COMSNETS*, 2022, pp. 1–6, doi: 10.1109/COMSNETS53615.2022.9668530.

[126] M. Z. Serdar, M. Koç, and S. G. Al-Ghamdi, "Urban Transportation Networks Resilience: Indicators, Disturbances, and Assessment Methods," *Sustain. Cities Soc.*, vol. 76, no. 2022, pp. 1–16, 2022, doi: 10.1016/j.scs.2021.103452.

[127] A. Pundir, S. Singh, M. Kumar, A. Bafila, and G. J. Saxena, "Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the New Mobility Era," *IEEE Access*, vol. 10, pp. 16350–16364, 2022, doi: 10.1109/ACCESS.2022.3147323.

[128] F. Al-Turjman and J. P. Lemayian, "Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview," *Comput. Electr. Eng.*, vol. 87, p. 106776, 2020, doi: 10.1016/j.compeleceng.2020.106776.

[129] A. Pauwels, N. Pourmohammad-Zia, and F. Schulte, "Safety and Sustainable Development of Automated Driving in Mixed-Traffic Urban Areas—Considering Vulnerable Road Users and Network Efficiency," *Sustain.*, vol. 14, no. 20, 2022, doi: 10.3390/su142013486.

[130] Z. Wang, H. Wei, J. Wang, X. Zeng, and Y. Chang, "Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey," *Sustain.*, vol. 14, no. 19, 2022, doi: 10.3390/su141912409.

[131] Cosmas Eko Suharyanto, Pastima Simanjuntak, "Potential Threat Analysis Hypertext Transfer Protocol and Secure Hypertext Transfer Protocol of Public WiFi Users (Batam Case)," *Int. J. Sci. Eng. Res.*, vol. 8, no. 3, pp. 320–326, 2017.

[132] A. Karaymeh, M. Ababneh, M. Qasaimeh, and M. Al-Fayoumi, "Enhancing data protection provided by VPN connections over open wifi networks," in *2nd International Conference on New Trends in Computing Sciences, ICTCS*, 2019, no. January 2022, pp. 1–6, doi: 10.1109/ICTCS.2019.8923104.

[133] P. Roychowdhury, J. M. Alghazo, B. Debnath, S. Chatterjee, and O. K. M. Ouda, "Security Threat Analysis and Prevention Techniques in Electronic Waste," in *Waste Management and Resource Efficiency*, 2019, pp. 853–866, doi: 10.1007/978-981-10-7290-1.

[134] V. Bhat, "E-waste management and Achieving SDG-Challenges in Indian Context," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 1161, no. 1, 2023, doi: 10.1088/1755-1315/1161/1/012008.

[135] A. Zarreh, H. Da Wan, Y. Lee, C. Saygin, and R. Al Janahi, "Cybersecurity concerns for total productive maintenance in smart manufacturing systems," *Procedia Manuf.*, vol. 38, no. 2019, pp. 532–539, 2019, doi: 10.1016/j.promfg.2020.01.067.

[136] W. Torbacki, "A hybrid mcdm model combining danp and promethee ii methods for the assessment of cybersecurity in industry 4.0," *Sustain.*, vol. 13, no. 16, 2021, doi: 10.3390/su13168833.

[137] M. Despeisse and E. T. Bekar, "Challenges in Data Life Cycle Management for Sustainable Cyber-Physical Production Systems," in *IFIP International Conference on Advances in Production Management Systems (APMS)*, 2020, pp. 57–65, doi: 10.1007/978-3-030-57997-5_7.

[138] K. Śledziewska and R. Włoch, "Cybersecurity and Control Sustainability in Digital Economy and Advanced Production," in *The Economics of Digital Transformation*, 2021, pp. 173–185.

[139] M. Gabriella, "Green claims, green washing and consumer protection in the European Union," *J. Financ. Crime*, vol. 30, no. 1, pp. 143–153, 2021.

[140] K. Zhang, Z. Pan, K. Zhang, and F. Ji, "The effect of digitalization transformation on greenwashing of Chinese listed companies: an analysis from the dual perspectives of resource-based view and legitimacy," *Front. Environ. Sci.*, vol. 11, no. June, pp. 1–21, 2023, doi: 10.3389/fenvs.2023.1179419.

[141] B. Ramtiyal, P. Garg, S. Johari, A. P. S. Rathore, and A. Thakrey, "Investigating the effects of corporate social responsibility on sustainable consumer purchase behavior," *J. Glob. Oper. Strateg. Sourc.*, vol. 17, no. 1, pp. 1–27, 2023.

[142] S. Fella and E. Bausa, "Green or Greenwashed? Examining Whether and When Consumers Are Able to Identify Greenwashing," *Bus. Res. Proc.*, vol. 1, no. 1, pp. 1–1, 2023, doi: 10.51300/brp-2023-95.

[143] S. Bharany *et al.*, "Energy efficient fault tolerance techniques in green cloud computing: A systematic survey and taxonomy," *Sustain. Energy Technol. Assessments*, vol. 53, no. PB, p. 102613, 2022, doi: 10.1016/j.seta.2022.102613.

[144] L. Bracciale, P. Loreti, E. Raso, G. Bianchi, P. Gallo, and E. R. Sanseverino, "A Privacy-Preserving Blockchain Solution to Support Demand Response in Energy Trading," in *MELECON 2022 - IEEE Mediterranean Electrotechnical Conference, Proceedings*, 2022, pp. 677–682, doi: 10.1109/MELECON53508.2022.9843108.

[145] F. Al-Turjman and B. Deebak, "Privacy-Aware Energy-Efficient Framework Using the Internet of Medical Things for COVID-19," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 64–68, 2020, doi: 10.1109/iotm.0001.2000123.

[146] A. Scaglione, "The Use of Differential Privacy for Energy Data," in *CPSS '22: Proceedings of the 8th ACM on Cyber-Physical System Security Workshop*, 2022, p. 1, doi: 10.1145/3494107.3522780.

[147] Michael Assante; Tim Conway; Robert Lee, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, vol. 388. 2016, pp. 1–26.

[148] G. R. Abhijith, E. Salomons, and A. Ostfeld, "Enhancing the Reliability of a Contamination Detection Sensors' Network in Water Distribution Systems during a Cyber-Attack," pp. 1–12, 2023, doi: 10.1061/9780784484852.fm.

[149] S. Fujii *et al.*, "Continuous and Multiregional Monitoring of Malicious Hosts," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2020, pp. 2101–2103, doi: 10.1145/3372297.3420018.

[150] X. Yang, W. Xi, A. Chen, and C. Wang, "An environmental monitoring data sharing scheme based on attribute encryption in cloud-fog computing," *PLoS One*, vol. 16, no. 9, pp. 1–21, 2021, doi: 10.1371/journal.pone.0258062.

[151] G. Aquila, E. de O. Pamplona, A. R. de Queiroz, P. Rotela Junior, and M. N. Fonseca, "An overview of incentive policies for the expansion of renewable energy generation in electricity power systems and the Brazilian experience," *Renew. Sustain. Energy Rev.*, vol. 70, pp. 1090–1098, 2017, doi: 10.1016/j.rser.2016.12.013.

[152] M. McCarty *et al.*, "Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment," *IEEE Access*, vol. 11, no. February, pp. 15297–15313, 2023, doi: 10.1109/ACCESS.2023.3244778.

[153] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam, and O. M. Elkomy, “Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2523–2537, 2022, doi: 10.1109/TITS.2021.3119968.

[154] S. Sarowa, B. Bhanot, V. Kumar, and M. Kumar, “Review of Smart Transportation and Challenges: Cyber Security Perspective,” in *International Conference on Advancement in Computation and Computer Technologies, InCACCT*, 2023, pp. 327–332, doi: 10.1109/InCACCT57535.2023.10141708.

[155] S. Paiva, M. A. Ahad, S. Zafar, G. Tripathi, A. Khalique, and I. Hussain, “Privacy and security challenges in smart and sustainable mobility,” *SN Appl. Sci.*, vol. 2, no. 7, pp. 1–10, 2020, doi: 10.1007/s42452-020-2984-9.

[156] A. Chowdhury, R. Naha, S. Kaisar, M. A. Khoshkholghi, K. Ali, and A. Galletta, “Information Fusion-based Cybersecurity Threat Detection for Intelligent Transportation System,” in *23rd IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing Workshops, CCGridW*, 2023, pp. 96–103, doi: 10.1109/CCGridW59191.2023.00029.

[157] T. Roy, A. Tariq, and S. Dey, “A Socio-Technical Approach for Resilient Connected Transportation Systems in Smart Cities,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 6, pp. 5019–5028, 2022, doi: 10.1109/TITS.2020.3045854.

[158] I. Ahmad *et al.*, “Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks,” *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/1444024.

[159] M. Jovic, E. Tijan, S. Aksentijevic, and D. Cišic, “An overview of security challenges of seaport IoT systems,” *2019 42nd Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2019 - Proc.*, no. May, pp. 1037–1042, 2019, doi: 10.23919/MIPRO.2019.8757206.

[160] S. Battula, M. Kumar, S. K. Panda, U. M. Rao, G. Laveti, and B. Mouli, “Online Ocean Monitoring using Edge IoT,” in *2020 Global Oceans 2020: Singapore - U.S. Gulf Coast*, 2020, pp. 3–9, doi: 10.1109/IEEECONF38699.2020.9389430.

[161] V. Sadhu, Z. Li, Z. Qi, and D. Pompili, “High-Resolution Data Acquisition and Joint Source-Channel Coding in Underwater IoT,” *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14003–14013, 2023, doi: 10.1109/JIOT.2023.3239580.

[162] L. Hang, I. Ullah, and D. H. Kim, “A secure fish farm platform based on blockchain for agriculture data integrity,” *Comput. Electron. Agric.*, vol. 170, no. October 2019, p. 105251, 2020, doi: 10.1016/j.compag.2020.105251.

[163] S. Wang, N. Karandikar, K. E. Knutsen, X. G. Tony Tong, T. Edseth, and Z. X. Zile, “Enhancing Maritime Data Standardization and Integrity using Docker and Blockchain,” in *Proceedings - International Conference on Software Engineering*, 2023, pp. 370–374, doi: 10.1109/ICSE-Companion58688.2023.00105.

[164] R. Subramanian, S. Ranganathan, and V. Ramasamy, “Gateway to Ocean Data Management: Ocean Best Practices, Information and Visualisation for moored ocean observation network,” in *Oceans Conference Record (IEEE)*, 2022, pp. 1–9, doi: 10.1109/OCEANSChennai45887.2022.9775375.

[165] B. Sullivan, “A Tale of Two Treaties: A Maritime Model to Stop the Scourge of Cybercrime,” *Boston Univ. Int. Law J.*, vol. 39, no. 143, pp. 143–180, 2021.

[166] J. R. Watson and A. J. Woodill, “Detecting illegal maritime activities from anomalous multiscale fleet behaviours,” *Fish Fish.*, vol. 23, no. 5, pp. 1055–1069, 2022.

[167] C. E. Nauen and S. T. Boschetti, “Fisheries Crimes, Poverty and Food Insecurity,” in *Routledge Handbook of Maritime Security*, 2022, p. 11.

[168] F. During, “Agriculture, Forestry, and Aquaculture,” *Va. J. Sci.*, vol. 70, no. 1, pp. 15–85, 2019, doi: 10.25778/hf6v-xd41.

[169] S. Mustafa, A. Estim, R. Shapawi, M. J. Shalehand, and S. R. M. Sidik, “Technological applications and adaptations in aquaculture for progress towards sustainable development and seafood security,” *IOP Conf. Ser. Earth Environ. Sci.*, vol. 718, no. 1, 2021, doi: 10.1088/1755-1315/718/1/012041.

[170] S. Sarowa, V. Kumar, B. Bhanot, and M. Kumar, “Enhancement of Security Posture in Smart Farming: Challenges and Proposed Solution,” in *Proceedings - IEEE International Conference on Device Intelligence, Computing and Communication Technologies, DICCT 2023*, 2023, pp. 155–159, doi: 10.1109/DICCT56244.2023.10110208.

[171] M. C. de Francesco, M. L. Carranza, M. Varricchione, F. P. Tozzi, and A. Stanisci, “Natural protected

areas as special sentinels of littering on coastal dune vegetation," *Sustain.*, vol. 11, no. 19, 2019, doi: 10.3390/su11195446.

[172] L. S. Talluru, S. Kapuganti, Y. B. Jonnala, and J. Joshi, "Secured Environmental Monitoring System," in *3rd International Conference on Intelligent Communication and Computational Techniques*, 2023, pp. 1–5, doi: 10.1109/ICCT56969.2023.10075967.

[173] D. Suhendi and E. Asmadi, "Cyber laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia," *Int. J. Cyber Criminol.*, vol. 15, no. 2, pp. 135–143, 2021, doi: 10.5281/zenodo.4766552.

[174] N. G. Pricope, G. A. Daldegan, A. Zvoleff, K. M. Mwenda, M. Noon, and D. Lopez-Carr, "Operationalizing an integrative socio-ecological framework in support of global monitoring of land degradation," *L. Degrad. Dev.*, vol. 34, no. 1, pp. 109–124, 2023, doi: 10.1002/ldr.4447.

[175] V. Dabkiene, T. Balezentis, and D. Streimikiene, "Development of agri-environmental footprint indicator using the FADN data: Tracking development of sustainable agricultural development in Eastern Europe," *Sustain. Prod. Consum.*, vol. 27, pp. 2121–2133, 2021, doi: 10.1016/j.spc.2021.05.017.

[176] N. J. Forsdick *et al.*, "Journeying towards best practice data management in biodiversity genomics," in *Molecular Ecology Resources*, 2023, no. November, doi: 10.1111/1755-0998.13880.

[177] K. Despot-Belmonte *et al.*, "Biodiversity data provision and decision-making - addressing the challenges," 2017. doi: 10.3897/rio.3.e12165.

[178] T. C. Haas, "Adapting cybersecurity practice to reduce wildlife cybercrime," *J. Cybersecurity*, vol. 9, no. 1, pp. 1–20, 2023, doi: 10.1093/cybsec/tyad004.

[179] U. Smart, J. C. Cihlar, and B. Budowle, "International Wildlife Trafficking: A perspective on the challenges and potential forensic genetics solutions," *Forensic Sci. Int. Genet.*, vol. 54, no. March, p. 102551, 2021, doi: 10.1016/j.fsigen.2021.102551.

[180] S. I. Ali, R. Ahamed, A. Habeeb, S. Rajper, and A. Laraib, *The Influence of Cybersecurity Attacks on E-Governance." pp. 77-95. IGI Global, 2022.* 2022.

[181] Felix C Aguboshim, Ifeyinwa N Obiokafor, and Anastasia O Emenike, "Sustainable data governance in the era of global data security challenges in Nigeria: A narrative review," *World J. Adv. Res. Rev.*, vol. 17, no. 2, pp. 378–385, 2023, doi: 10.30574/wjarr.2023.17.2.0154.

[182] C. K. Bhagat, "Study of Current Cybersecurity Threats to Information & Operational Technology (IOT) and their Effect on e-Governance in Nepal," *J. UTEC Eng. Manag.*, vol. 1, no. 01, pp. 41–50, 2023, doi: 10.36344/utecem.2023.v01i01.005.

[183] Y. N. Zulfiani, "Prevention of personal data privacy leakage in e-government, as the government's responsibility," *Ann. Justice Humanit.*, vol. 1, no. 1, pp. 29–37, 2021.

[184] V. A. Cabra, G. T. Pineda, K. C. Quintero, J. S. Villa, A. D. Pérez, and V. Martirosyan, "Civil Society Data for Sustainable Development Goal 16 Monitoring: A Case Study of the Use of Social Networks for Measuring Perception of Discrimination," *Citiz. Sci. Theory Pract.*, vol. 8, no. 1, pp. 1–16, 2023, doi: 10.5334/cstp.590.

[185] A. Alvarado Garcia, M. J. Britton, D. M. Doshi, M. De Choudhury, and C. A. Le Dantec, "Data Migrations: Exploring the Use of Social Media Data as Evidence for Human Rights Advocacy," *Proc. ACM Human-Computer Interact.*, vol. 4, no. CSCW3, 2021, doi: 10.1145/3434177.

[186] I. Journal and C. Law, "Cyber Law: Safeguarding Digital Spaces in Uzbekistan," *Int. J. Cyber Law*, vol. 1, no. 5, pp. 1–15, 2023.

[187] WIDYA SETIABUDI SUMADINATA, "Cybercrime and Global Security Threats: a Challenge in International Law," *Russ. Law J.*, vol. 11, no. 3, pp. 438–444, 2023, doi: 10.52783/rlj.v11i3.1112.

[188] M. Watney, "Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: A Legal Perspective," *Eur. Conf. Inf. Warf. Secur. ECCWS*, vol. 2022-June, pp. 319–327, 2022, doi: 10.34190/eccws.21.1.196.

[189] L. Kello, "Cyber legalism: Why it fails and what to do about it," *J. Cybersecurity*, vol. 7, no. 1, pp. 1–15, 2021, doi: 10.1093/cybsec/tyab014.

[190] A. Zuiderwijk, Y. C. Chen, and F. Salem, "Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda," *Gov. Inf. Q.*, vol. 38, no. 3, p. 101577, 2021, doi: 10.1016/j.giq.2021.101577.

[191] S. R. Muller, D. N. Burrell, C. Nobles, H. C. Mingo, and A. Vassilakos, "Exploring Cybersecurity,

Misinformation, and Interference in Voting and Elections Through Cyberspace," *Eff. Cybersecurity Oper. Enterp. Syst.*, pp. 221–241, 2023, doi: 10.4018/978-1-6684-9018-1.ch011.

[192] S. Baloglu, S. Bursuc, S. Mauw, and J. Pang, "Election Verifiability Revisited: Automated Security Proofs and Attacks on Helios and Belenios," in *Proceedings - IEEE Computer Security Foundations Symposium*, 2021, pp. 1–15, doi: 10.1109/CSF51468.2021.00019.

[193] H. Fjelde and H. M. Smidt, "Protecting the Vote? Peacekeeping Presence and the Risk of Electoral Violence," *Br. J. Polit. Sci.*, vol. 52, no. 3, pp. 1113–1132, 2022, doi: 10.1017/S0007123421000132.

[194] W. Zhang and H. Wu, "Digital Identity, Privacy Security and their Legal Safeguards in the Metaverse," *Secur. Saf.*, vol. 2, no. 2023011, pp. 1–14, 2023, doi: 10.1051/sands/2023011.

[195] B. Okunoye, "Digital identity for development should keep pace with national cybersecurity capacity: Nigeria in focus," *J. Cyber Policy*, vol. 7, no. 1, pp. 24–37, 2022.

[196] B. K. Cheryl and B. K. Ng, "Protecting the Unprotected Consumer Data in Internet of Things: Current Scenario of Data Governance in Malaysia," *Sustain.*, vol. 14, no. 16, pp. 1–25, 2022, doi: 10.3390/su14169893.

[197] H. M. Linge and R. Brännvall, "Secure Sharing of Health-Related Data: Research Description of the VINTER, DELFIN, and HEIDA Projects," *Stud. Health Technol. Inform.*, vol. 302, pp. 143–144, 2023, doi: 10.3233/SHTI230087.

[198] A. Aljumah and T. A. Ahanger, "Blockchain-Based Information Sharing Security for the Internet of Things," *Mathematics*, vol. 11, no. 9, pp. 1–20, 2023, doi: 10.3390/math11092157.

[199] A. F. Aysan, F. Bergigui, and M. Disli, "Using Blockchain-Enabled Solutions as SDG Accelerators in the International Development Space," *Sustain.*, vol. 13, no. 7, pp. 1–24, 2021, doi: 10.3390/su13074025.

[200] M. Humayun, M. Niazi, M. Assiri, and M. Haoues, "Secure Global Software Development : A Practitioners ' Perspective," *Appiled Sci.*, vol. 13, no. 4, 2023.

[201] J. H. Kahle, É. Marcon, A. Ghezzi, and A. G. Frank, "Smart Products value creation in SMEs innovation ecosystems," *Technol. Forecast. Soc. Change*, vol. 156, no. 2020, p. 120024, 2020, doi: 10.1016/j.techfore.2020.120024.

[202] E. Reid, "Human Rights in the Anthropocene, the Sustainable Development Goals and the Significance of SDG 17, 'Partnerships for the Goals,'" in *Human Rights in the Anthropocene: Concepts, Contexts and Challenges*, 2023.

[203] L. Mariani, B. Trivellato, M. Martini, and E. Marafioti, "Achieving Sustainable Development Goals Through Collaborative Innovation: Evidence from Four European Initiatives," *J. Bus. Ethics*, vol. 180, no. 4, pp. 1075–1095, 2022, doi: 10.1007/s10551-022-05193-z.

[204] M. Zarour *et al.*, "Ensuring data integrity of healthcare information in the era of digital health," *Healthc. Technol. Lett.*, vol. 8, no. 3, pp. 66–77, 2021, doi: 10.1049/htl2.12008.

[205] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electr. Power Syst. Res.*, vol. 215, no. PA, p. 108975, 2023, doi: 10.1016/j.epsr.2022.108975.

[206] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," *Mesopotamian J. Cyber Secur.*, vol. 2023, pp. 57–63, 2023, doi: 10.58496/mjcs/2023/010.

[207] S. Kiser and B. Maniam, "Ransomware: Healthcare Industry at Risk," *J. Bus. Account.*, vol. 14, no. 1, pp. 65–81, 2021, [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.654.7646&rep=rep1&type=pdf#page=4.

[208] B. Greenstein and A. Capstone, "The Impact of Ransomware-as-a-Service on Critical Infrastructure," 2022.

[209] M. Lamers, C., Spoerl, E., Levey, G., Choudhury, N., Ahmed, "Ransomware: A Threat to Cyber Smart Cities," in *Cybersecurity for Smart Cities*, Springer, Cham., 2023, pp. 185–204.

[210] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on security threats in agricultural iot and smart farming," *Sensors (Switzerland)*, vol. 20, no. 22, pp. 1–17, 2020, doi: 10.3390/s20226458.

[211] Kamaldeep, M. Malik, and M. Dutta, "Security Challenges in Internet of Things (IoT) Integrated Power

and Energy (PaE) Systems," in *Intelligent Data Analytics for Power and Energy Systems*, 2022, pp. 555–566.

[212] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures," *Internet of Things*, vol. 2, no. 1, pp. 163–186, 2021, doi: 10.3390/iot2010009.

[213] K. Shanmugam, M. E. Rana, and R. S. J. Singh, "IoT-based Smart Water Quality Monitoring System for Malaysia," in *3rd International Sustainability and Resilience Conference: Climate Change*, 2021, pp. 530–538, doi: 10.1109/IEEECONF53624.2021.9668120.

[214] J. Telo, "Smart City Security Threats and Countermeasures in the Context of Emerging Technologies," *Int. J. Intell. Autom. Comput.*, vol. 6, no. 1, pp. 31–45, 2023, [Online]. Available: https://research.tensorgate.org/index.php/IJIAC/article/view/18.

[215] Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 52–59, 2015, doi: 10.1109/MCOM.2015.7081075.

[216] E. Michael Onyema *et al.*, "Cloud Security Challenges:Implication on Education," *Int. J. Comput. Sci. Mob. Comput.*, vol. 9, no. 2, pp. 56–73, 2020, [Online]. Available: www.ijcsmc.com.

[217] B. Kim, D. Y. Lee, and B. Kim, "Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks," *Behav. Inf. Technol.*, vol. 39, no. 11, pp. 1156–1175, 2020, doi: 10.1080/0144929X.2019.1653992.

[218] Z. Ghasem, I. Frommholz, and C. Maple, "Machine Learning Solutions for controlling Cyberbullying and Cyberstalking," *J. Inf. Secur. Res.*, vol. 6, no. 2, pp. 55–64, 2015.

[219] S. Shackelford and S. Myers, "Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace," *SSRN Electron. J.*, vol. 19, pp. 334–388, 2017, doi: 10.2139/ssrn.2874090.

[220] G. Coppi and L. Fast, "Blockchain and distributed ledger technologies in the humanitarian sector," 2019. [Online]. Available: https://www.odi.org/sites/odi.org.uk/files/resource-documents/12605.pdf.