Issues in Information Systems
Volume 26, Issue 1, pp. 79-93, 2025

DOI: https://doi.org/10.48009/1_iis_107

Overview of the challenges and potential solutions in securing digital ecosystem in the US

Saeed Tabar, *University of West Georgia, Richards College of Business, stabar@westga.edu*
Gelareh Towhidi, *University of West Georgia, Richards College of Business, gtowhidi@westga.edu*
Tay Bryant, *University of West Georgia, Richards College of Business, tb00303@my.westga.edu*

Abstract

The U.S. federal government's vision for a fully integrated digital ecosystem by 2033 faces significant obstacles due to escalating cybersecurity threats. This study focuses on a critical challenge within that vision: securing interconnected infrastructures—specifically the digital economy, power grids, Internet of Things (IoT), and Artificial Intelligence (AI)—as outlined in the National Cybersecurity Strategy. Through a targeted literature review, this research identifies key vulnerabilities in these domains and evaluates current mitigation strategies. The paper proposes a structured framework for addressing systemic cybersecurity risks, offering actionable insights to support the secure evolution of the national digital ecosystem. These findings aim to inform both policymakers and researchers working toward resilient digital infrastructure.

Keywords: cybersecurity, cybercrime, digital ecosystem, cybersecurity strategy, DDOS, ransomware

Introduction

Cyberattacks have become increasingly pervasive and sophisticated in recent years, with a notable rise in both frequency and impact. Cybercrime is now often regarded as the world's third-largest economy, following the United States and China, due to its substantial economic influence, surpassing the GDP of many nations. This comparison is based on the estimated global costs of cybercrime, projected to reach $10.5 trillion by 2025 (Vainilavičius, 2023; Nagy, 2024). In 2023, ransomware accounted for 70.13% of all cyberattacks worldwide, with over 317 million attempts (Statistica, 2023). Ransomware incidents have been reported to cost organizations an average of $1.85 million per incident in mitigation, recovery, and legal fees (Pott, 2019). In 2023, ransomware adversaries generated a total of $1.1 billion (Deus, 2023). To address these challenges, the U.S. federal government introduced a five-pillar framework for the national cybersecurity strategy in March 2023 (Whitehouse, 2023). This strategy addresses cybersecurity challenges from individual, organizational, and governmental perspectives, aiming to ensure a secure digital future for both the U.S. and the world.

This research article reviews significant threats identified in past literature from a scientific perspective and highlights areas needing further exploration. The need for robust cybersecurity measures is critical to protect the digital economy, which accounted for $2.41 trillion of the U.S. GDP in 2021 (Bureau of Economic Analysis, 2023). The integration of digital power grids, essential for managing growing power demand and incorporating renewable energy sources, also presents significant cybersecurity risks (Statista, 2024). The proliferation of IoT devices, expected to reach over 17 billion by 2025, further complicates the cybersecurity landscape (Vailshery, 2024). Additionally, the rapid advancement of AI technologies necessitates stringent security protocols to prevent misuse and ensure responsible development (US Department of State, 2024).

This paper condenses these research topics by providing an overview of recent studies and their applications to advance common cybersecurity objectives in light of the cybersecurity strategy. It examines the evolving challenges faced by organizations, explores defense mechanisms, and addresses areas where knowledge may be lacking in protecting digital assets. The significance of this research lies in its potential to provide readers with valuable insights, enabling a comprehensive understanding of key considerations in cybersecurity while creating a framework that contextualizes potential solutions for a digital ecosystem. By understanding the complexities of cyberattacks and their impact on business operations, we can better prepare for and mitigate the risks associated with our interconnected world.

The paper is organized as follows: First, we review the national cybersecurity strategy and its five pillars, along with the main elements of digital ecosystems and the vulnerabilities that threaten these ecosystems. This review relates to the cybersecurity strategy framework, highlighting strengths, weaknesses, and potential solutions. Finally, we discuss the current state of security in the U.S. from various perspectives and address the questions that remain unanswered.

The cybersecurity strategy framework

The Internet has revolutionized global connectivity, enabling individuals, organizations, and states to communicate and collaborate digitally over a shared platform. This digital ecosystem offers numerous benefits: individuals can exercise their rights, such as freedom of speech and online voting; businesses can reach global customers with their products and services; financial organizations can provide services worldwide, transcending physical boundaries; and governments can collaborate on addressing global issues like hunger and climate change.

However, these advantages come with significant challenges. Enhanced connectivity and advanced technologies also introduce vulnerabilities. If these challenges are not addressed, they can negate the benefits and create substantial dilemmas. A cyberattack on one entity within this interconnected grid can have cascading effects on others. For example, the "NotPetya" cyberattack on Ukraine caused extensive damage in numerous countries across Europe, Asia, and America. This ransomware attack compromised Ukraine’s tax accounting software, MeDoc, and quickly spread through a Windows vulnerability, causing approximately $10 billion in damage worldwide (Brumfield, 2022; Sean Steinberg, 2021). To combat the growing threats in cyberspace, the White House released a national cybersecurity strategy framework in March 2023.

This strategy emphasizes a collective effort among individuals, organizations, and governments at state, local, tribal, and territorial levels, as well as international partners and allies. The goal is to distribute responsibility among various actors and achieve comprehensive security for the digital ecosystem by 2033.

Table1. Cybersecurity strategy framework (Whitehouse, 2023)

Cybersecurity pillar	Objectives
1-Defend Critical infrastructure	1.1 Establish cybersecurity requirements to support national security and public safety
	1.2 Scale public-private collaboration
	1.3 Integrate federal cybersecurity centers
	1.4 Update federal incident response plans and processes
	1.5 Modernize federal defenses
2-Disrupt & dismantle threat actors	2.1 Integrate federal disruption activities
	2.2 Enhance public-private operational collaboration to disrupt adversaries
	2.3 Increase the speed and scale of intelligence sharing and victim notification
	2.4 Prevent abuse of US-based infrastructure
	2.5 Counter cybercrime, defeat ransomware
3-Shape market forces to drive security and resilience	3.1 Hold the stewards of the data accountable
	3.2 Drive the development of secure IoT devices
	3.3 Shift liability for insecure software products and services
	3.4 Use federal grants and other incentives to build in security
	3.5 Leverage federal procurement to improve accountability
	3.6 Explore a federal cyber insurance backstop
4-Invest in a resilient future	4.1 Secure the technical foundation of the Internet
	4.2 Reinvigorate Federal research and development for cybersecurity
	4.3 Prepare for the post-quantum future
	4.4 Secure clean energy future
	4.5 Support development of a digital identity ecosystem
	4.6 Develop a national strategy to strengthen the cyber workforce
5-Foreign international partnership to pursue shared goals	5.1 Build coalitions to counter threats to the digital ecosystem
	5.2 Strengthen international partner capacity
	5.3 Expand US ability to assist allies and partners
	5.4 Build coalition to reinforce global norms of responsible state behavior
	5.5 Secure global supply chain for information, communication and operational technology products and service

The cybersecurity strategy, detailed in Table 1, is structured around five pillars and aims to advance the digital ecosystem by leveraging technological advancements and addressing challenges in cyberspace. The strategy's vision is to protect key elements of the digital ecosystem, including the digital economy, digital power grids for energy production, the Internet of Things (IoT) for surveillance and control, and Artificial Intelligence (AI) to accelerate the move toward a secure cyberspace. This vision targets 2033 as the milestone for the full implementation of the digital ecosystem. These four main elements are interconnected and must be addressed collectively.

The five pillars that require protection against threat actors include:

1. Defending critical infrastructure
2. Disrupting and dismantling threat actors
3. Shaping market forces to drive security and resilience
4. Investing in a resilient future
5. Collaborating with international partners and allies

These pillars incorporate both defensive and offensive measures against threat actors and mandate that technology companies produce software and hardware, such as IoT devices, with security standards in mind. The strategy also emphasizes investment in research and development of new technologies and international collaboration to advance toward the post-quantum era and clean renewable energy.

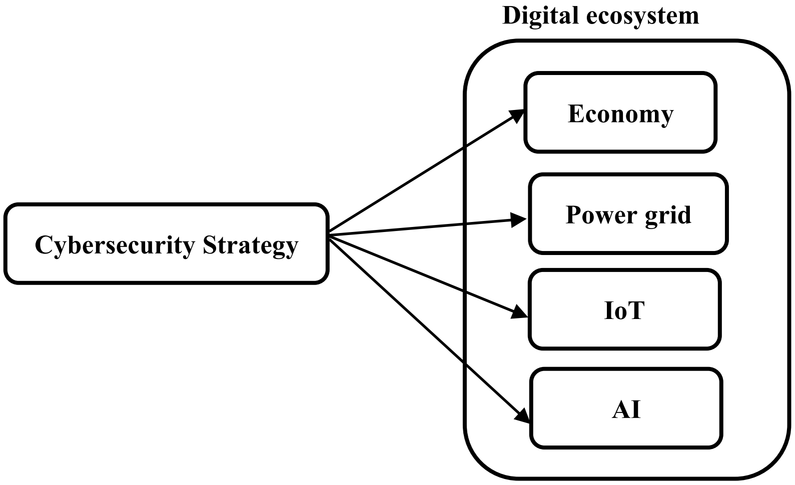

Figure1. Cybersecurity strategy and digital ecosystem

Figure 1 illustrates the main drivers of the digital ecosystem that need to be protected through the cybersecurity strategy. The following sections provide detailed challenges and potential solutions to these challenges by reviewing past literature.

Digital Economy

The term "digital economy" was first coined by Tapscott (1996) to describe the combination of intelligence, knowledge, and creativity to create wealth on the Information and Communication Technology (ICT) platform (Tapscott, 1996). It refers to an economy that encompasses markets, organizations, and their networks, all based on digital technologies, including the internet, digital communication networks, computers, software, and e-commerce (Lubacha, 2023). Later, Kenney and Zysman (2016) introduced the concept of the "Digital Platform Economy" to describe a wide range of digital activities in business, politics, and social interaction (Kenney, 2016). This economy relies on digital information and knowledge as key factors of production. Key aspects of the digital economy include:

1. E-Commerce: Online buying and selling of goods and services, including platforms like Amazon and eBay (Laudon, 2020).

2. Digital Services: Services provided over the internet, such as cloud computing, online banking, and streaming services like Netflix and Spotify (Armbrust, 2010).
3. Digital Platforms Online platforms facilitating interactions between users, such as social media (Facebook, Twitter), search engines (Google), and gig economy platforms (Uber, Airbnb) (Parker, 2016).
4. Digital Payments: Electronic transactions and payment systems, including mobile payments, online banking, and cryptocurrencies (Kokkola, 2010).
5. Data and Analytics: The use of big data and analytics to drive business decisions, improve customer experiences, and create new products and services (Chen, 2012).
6. Digital Infrastructure: The physical and virtual infrastructure supporting digital activities, including broadband networks, data centers, and cybersecurity measures (Von Solms, 2013).

The digital economy, through the use of digital information, lowers the costs of search, replication, transportation, tracking, and verification, thereby reducing the overall costs of economic activities involving these processes (Goldfarb, 2019; Zoltan Acs, 2021). The digital economy relies on ICT for data exchange, with data acting as the lifeblood and ICT infrastructure serving as the skeleton. Consequently, cyberattacks on data and ICT infrastructure pose serious threats to the entire digital economy.

For example, in 2023, three out of four companies in the United States were at risk of a material cyberattack, with 480,000 attacks reported in 2022. Cybercrime is projected to cost U.S. businesses more than $452 billion in 2024 (Petrosyan, 2024). The average annual cost of cyberattacks for U.S. small and medium-sized businesses (SMBs) in 2024 is approximately $25,000, with global costs projected to reach $10.5 trillion by 2025 (Palatty, 2024)**.** The average cost of a data breach globally was $4.88 million in 2024. The average cost of a ransomware attack, including recovery costs, is around $4.54 million (Mariah St. John, 2024)**.**

Significant cyber threats to U.S. businesses include phishing, ransomware, malware, Distributed Denial of Service (DDoS), and Business Email Compromise (BEC). Phishing, in various forms such as email phishing, spear phishing, whaling, and pharming, accounted for 36% of data breaches in 2023, resulting in $10.3 billion in losses (Jo Rushton, 2024). The average cost of a ransomware attack, including recovery costs, was around $4.9 million in 2024, a 10% increase from the previous year.

Organizations using security AI and automation saved an average of $2.22 million (IBM, 2024). The average DDoS attack cost businesses $408,000 in 2023, with the average attack duration increasing from 24 minutes to 121 minutes. Telecommunications companies experienced the most frequent attacks, while retail and healthcare sectors faced the largest attack sizes. Government entities had the longest attack durations, averaging 4 hours in the first half of 2023 and 18 hours in the second half. Educational institutions accounted for 17% of all attacks. Data from 14 industries and regions across North America and Western Europe, covering January 1 to December 31, 2023, showed that business email compromise resulted in $2.95 billion in losses in 2023, making it the costliest cybercrime for businesses (Zayo, 2024; Internet Crime Complaint Center, 2023).

Digital PowerGrid

The G7 countries, including the United States, United Kingdom, Canada, France, Germany, Italy, and Japan, have committed to phasing out unabated coal-fired power plants by 2035 (Thorsberg, 2024). To achieve this, they plan to end most fossil fuel subsidies by 2025 and significantly invest in cleaner energy sources such as solar, wind, water, and hydrogen (United Nations Climate Change, 2016). As renewable energy systems become more integrated with digital networks, addressing cybersecurity risks to protect the energy infrastructure from potential cyberattacks becomes increasingly crucial (Jones, 2024). For instance, the U.S. electric power system comprises over 3,000 utility companies, 200,000 miles of high-voltage transmission lines, 55,000 substations, and 5.5 million miles of distribution lines (Tsafos, 2021). Cyberattacks targeting these systems could disrupt power functions, cause blackouts, and result in significant financial losses. Power grids typically cover large geographical areas spanning multiple countries (He, 2016). Due to the extensive size of the grid and the associated costs of updating the digital infrastructure, the power sector has not kept pace with technological advancements, and many countries still rely on legacy systems for their infrastructure, posing security threats to the entire network (Phuangpornpitak, 2013; Krause, 2021).

Consequently, the magnitude of the network makes it inflexible to update. Additionally, the incorporation of digital technology into legacy power systems opens the door to malicious users, especially state actors, to target power grids and launch various types of attacks. For example, North America relies on DNP3, while the rest of the world predominantly uses IEC 60870-5-104 as the protocol for their process control networks (Segall, 1983; IEC, 2016). These outdated protocols are vulnerable to various attacks, such as Trojan horses and Distributed Denial of Service (DDoS) attacks, due to their age and lack of updates. When these protocols are interlinked with data communication protocols, they pose an even greater threat as the weakest point in the security chain.

A major concern in the power sector is the security of the communication infrastructure that monitors and controls the grid (Krause, 2021). This infrastructure receives critical information from various Internet of Things (IoT) sensors, making it a primary point of entry for malicious users. According to Krause et al. (2021), availability is the most crucial factor in power sector security, surpassing both confidentiality and integrity (Krause, 2021). Consequently, safeguarding against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which target the network's availability, is of paramount importance. Additionally, threat actors might exploit vulnerabilities in the power grid by compromising hardware components supplied to power companies, creating backdoors during the distribution process (Knake, 2017; Macola, 2020). The SolarWinds cyberattack exemplified this type of infiltration, where hackers accessed SolarWinds systems and deployed trojan updates to Orion software, enabling them to install stealthy malware on consumer networks (Center for Internet Security, 2021).

Mitigating threats from state actors with sophisticated technologies is particularly challenging (Department of Homeland Security, 2025). The electric utility sector faces millions of attempted cyber intrusions daily, with significant increases between 2011 and 2017 (Tsafos, 2021). Despite numerous laws aimed at combating these challenges, many organizations recognize that their systems could be exploited to infiltrate technical equipment and extract sensitive data. Companies can detect these events through network monitoring, advanced intrusion detection systems (IDS), anomaly detection, threat intelligence, audits and penetration testing, and endpoint detection and response.

Another source of threat to the power system is the cascading effect, where threat actors gain control of customers' solar panels remotely and start manipulating the frequency (Dabrowski, 2017) causing damage to the control office and consequently to other customers connected to the office. Therefore, the central office of power service providers of power such as wind and solar could impact other customers as well, creating a cascading impact (Cardenas, 2020; Pudjianto, 2007).

To address these challenges, a comprehensive approach encompassing device, application, and network security, as well as upgrading legacy systems, is necessary to achieve an acceptable level of security. In addition to checking firmware for potential bugs and using firewalls, intrusion detection, and protection systems to shield communication networks, approaches such as separating the control side from the operational network through software-defined networking could protect the network and prevent the cascading effect of attacks (Krause, 2021; Wei, 2011).

IoT

The advent of computers, networks, and sensors has ushered in the transformative era of the Internet of Things (IoT). Coined by Kevin Ashton, the term IoT encapsulates the vision of endowing computers with sensory capabilities, extending beyond traditional inputs from keyboards, cameras, or scanners. The IoT paradigm enables computers to autonomously perceive and interact with the world, harnessing a wealth of data far surpassing what human users can manually input. Ashton equates IoT to humans in terms of receiving information through eyes and ears, processing information through the brain, and taking action through hands and legs. Sensors in IoT receive signals from the environment, process information through microprocessors, and take actions through actuators (Ashton, 2009; Gabbai, 2015). Depending on the application, IoT networks may have different architectures. However, they all share basic components such as sensors, processors, actuators, and communication elements (Voas, 2016).

The Internet of Things envisions a networked ecosystem where over 100 billion devices are anticipated to be online by 2025, potentially unleashing an economic impact exceeding $11 trillion globally (Rose, 2015). IoT applications are divided into four main categories: Consumer IoT, Industrial IoT, Infrastructure IoT, and Commercial IoT (Boulaalam, 2019). Consumer IoT includes wearables for health and fitness tracking, home amenities (Kang, 2017), security systems, and shopping aids (Tan, 2024). Industrial IoT, referred to as Industry 4.0 (Ayala, 2019), is primarily utilized in manufacturing to monitor and control production processes, including assembly lines and quality controls. It also encompasses fields such as the Internet of Battlefield Things (Polit, 2018; Said, 2021). The infrastructure IoT (Li, 2015) automates urban infrastructure, including smart cities, environmental monitoring, traffic management, and power infrastructure management.

Commercial IoT applications include healthcare, transportation (Xie, 2017) such as self-driving automobiles, robot, and drone delivery, agriculture (Meola, 2021), maritime (World, 2020) and smart parking management (Zhao, 2020). Given the widespread use of IoT technology, failing to secure IoT networks can pose serious threats, especially to manufacturing companies and power plants. IoT devices are vulnerable to various types of attacks such as DDoS, man-in-the-middle attacks, and malware infections due to their low processing power (Laghari, 2024; Iqbal, 2020). A layered architecture addressing various threats can provide a robust security solution. These layers include the perception or access level, network layer, and application layer. The access layer, where sensors communicate with the external environment, such as inventory sensing, is the most vulnerable due to low processing power, which makes implementing encryption challenging. Solutions such as lightweight encryption and authentication are suggested to protect this layer (Laghari, 2024). Another vulnerability stems from the limited storage capacity of sensors, necessitating the incorporation of cloud-based storage. Consequently, access layer sensors could serve as entry points to the cloud storage of the IoT framework (Rajmohan, 2022).

The most widely cited attack on the network layer is the Distributed Denial of Service (DDoS), which aims to disrupt or terminate the function of the network layer. DDoS attacks involve 96% of IoT devices (Makhdoom, 2019). In IoT, heterogeneous networks comprising both data communication and operation management work together to provide services to end-users. However, linking operations management systems, which use sensors in legacy systems, might expose vulnerabilities in the network layer when connected to the communication network. Therefore, isolating the operation network and communication network through encrypted VPNs could mitigate the vulnerabilities of the sensors in the operation network. Similarly, hardware components within the IoT network are attractive targets for hackers because security

is often not the primary consideration during IoT device production. Standardizing the security of IoT devices to prevent remote exploitation can enhance the protection of sensors
(Iqbal, 2020; Hernandez, 2014; Zonouz, 2014). The application layer of IoT shares the same threats as other applications, such as infection by Trojan horses, viruses, and SQL injection attacks. Application hardening is the most feasible solution for the application layer of IoT (Laghari, 2024; Rajmohan, 2022; Iqbal, 2020).

AI (Artificial Intelligence)

AI is becoming the backbone for many firms, with its use rapidly increasing as organizations adapt to the new technological age (Malatji, 2024). AI applications are being programmed to detect malware, which traditional antivirus applications cannot always identify since they rely on a database of known malware samples (Kshetri, 2021; Kaur, 2023; Ansari, 2022). AI systems are designed to continuously learn and perform repetitive tasks, making them optimal for environments requiring constant supervision to ensure malicious activity is not occurring (Burhanuddin, 2025). Research shows that firms have been successful in preventing various network attacks by utilizing AI to perform automated tasks (Okdem, 2024). For example, in March 2020, the cybersecurity company "Cyber AI Analyst" identified an advanced persistent threat group affiliated with a foreign government (Zhang, 2021). The vulnerability allowed unauthenticated users to launch remote attacks on affected systems without indicators of compromise or log entries to identify malicious activity (Kshetri, 2021; Zhang, 2021).

While there is significant evidence showcasing the effectiveness of AI in cybersecurity, it is equally important to recognize its limitations. Malicious users, especially state actors, can create inputs specifically designed to deceive AI models through SQL injection, which inserts statements into a database server. This can be particularly problematic for systems that rely on databases for storing and retrieving data, as the injection can allow threat actors to alter data and propagate misinformation. Even with proper security measures such as input validation and parameterized queries, malicious AI applications could still be deployed to analyze and exploit mistakes made by developers and administrators, demonstrating the need for continuous monitoring by security personnel. However, this comes with a tradeoff. Substituting AI monitoring with human monitoring may create loopholes that could make an organization more susceptible to attacks, as humans do not possess the intellectual capacity to analyze large amounts of information simultaneously and quickly learn about evolving cyberattacks. This scenario highlights the need for more research into the limitations of AI and how malicious AI can be used to circumvent strong security protocols.

Another field pertinent to AI that poses a threat to the digital economy is quantum computing. Quantum computing has the capacity to solve complex logical issues in technology and foster tremendous advancements in science and other disciplines (Galer, 2023). Quantum computing uses the principles of quantum mechanics to process information, wherein these sophisticated devices apply qubits, allowing for a state of 0, 1, or both simultaneously (Malik, 2025). This ability enables quantum computing to perform many calculations simultaneously, making them more powerful and equipped to solve efficiency issues such as the "traveling salesman problem" (Pazur, 2025).

Quantum computing is therefore a revolutionary development, similar to historical advancements. For example, one estimate states that without the Allies' ability to break Axis communications encrypted by the Enigma machine, 13 million additional lives would have been lost during World War II (Swayne, 2023). One interesting challenge presented by quantum computing is the risk in transitioning to its algorithms while moving away from current, quantum-vulnerable implementations (Computers, 2024). Downgrade attacks, for example, involve an attacker forcing the system to abandon current higher security mechanisms and "fall back" to older models, exploiting vulnerabilities of outdated algorithms to access sensitive information (Priya, 2023).

Moore's Law, which observes that the number of transistors on computer chips doubles approximately every two years, would be significantly surpassed by quantum computing, increasing computing power by a factor of 10,000. However, engineers currently face challenges in building such powerful computers, including error-causing vibrations, electromagnetic waves, and temperature fluctuations. Many scientists predict that these obstacles can be resolved within the next 20 years, resulting in computers powerful enough to decrypt the predominant public key schemes currently in use (Masterson, 2024; Burden, 2025; Vasiliu-Feltes, 2023).

RSA encryption, for example, bases its security on the use of large prime numbers and modular arithmetic. While multiplying 13 by 97 yields 1,261, reversing this process to find the two underlying primes is computationally infeasible with current technology. Quantum computing changes this assumption, as it can perform advanced mathematical calculations significantly faster than modern computers, making it capable of cracking asymmetric cryptographic algorithms. This phenomenon can be observed with Shor's Algorithm, which has been shown to identify the underlying factors of a prime number. Quantum computers are likely too large and expensive for cybercriminals, but it is safe to assume that many nation-state adversaries are exploring practical applications of quantum computing to decrypt sensitive information about foreign governments and civilians (Expert Panel, 2023; Lipman, 2021; Torkington, 2024; Lee, 2021).

Conclusion and Future Research

As the world becomes more technologically advanced, tech companies face several significant cybersecurity challenges. The increasing sophistication of cyberattacks makes it particularly difficult for smaller businesses to protect their systems and data. Advanced cyberattacks, such as phishing, ransomware, and zero-day exploits, are becoming more common, and many businesses lack the resources and personnel to effectively defend against these attacks. Some businesses do not have the budget for a dedicated IT security team or advanced security tools, leaving their networks vulnerable to sophisticated attacks. Navigating these challenges requires significant time and research, which many firms cannot afford, highlighting the importance of academic contributions to solving these issues.

This paper has identified several research questions regarding recent concerns in cybersecurity that underscore the need for more sophisticated research aimed at reducing digital attacks and strengthening defense mechanisms.

1. How can tech companies lower the risk of insider threats by exfiltrating data as it relates to cloud computing without exposing explicit risks inherent in third-party cloud services?

2. What is the correct method for balancing the concern with loopholes that are inevitable within human intervention in monitoring machine learning systems with artificial intelligence monitoring, given that both systems have implicit risks?

3. How would industries adapt to the implementation of quantum computing, which has the capacity to break strong encryption algorithms likely still in use during its procurement? How could developing countries upscale their security operations to compete against quantum computing if their adversaries acquire quantum computing first?

4. How can companies curtail threat actors' ability to measure electromagnetic emissions or power consumption patterns to extract cryptographic keys?

References

Ansari, D. S. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *International Journal of Advanced Research in Computer and Communication Engineering*. doi:https://doi.org/10.17148/IJARCCE.2022.11912

Armbrust, F. G. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58. doi:10.1145/1721654.1721672

Ashton, K. (2009). That 'Internet of Things' thing. *RFID journal*, 97-114. Retrieved from https://www.rfidjournal.com/expert-views/that-internet-of-things-thing/73881 /

Ayala, C. H. (2019). *The Industrial Internet of things; opportunities, risks, mitigations*. Retrieved from https://permanent.fdlp.gov/: https://permanent.fdlp.gov/gpo150586/ia_iiot-intercommections.pdf

Boulaalam, A. (2019). Internet of things: new classification model of intelligence. *Journal of Ambient Intelligence and Humanized Computing*, 2731-2744. doi:10.1007/s12652-018-0965-2

Brumfield, C. (2022, June 27). *5 years after NotPetya: Lessons learned.* Retrieved from https://www.csoonline.com/article/573049/5-years-after-notpetya-lessons-learned.html

Burden, J. (2025). *Embracing the Quantum Economy: A Pathway for Business Leaders.* World Economic Forum. Retrieved from https://www.weforum.org/publications/embracing-the-quantum-economy-a-pathway-for-business-leaders/

Bureau of Economic Analysis. (2023). *Digital Economy.* https://www.bea.gov/data/special-topics/digital-economy.

Burhanuddin, S. I. (2025). AI-Enhanced Cybersecurity: A Comprehensive Review of Techniques and Challenges. *Current and Future Trends on AI Applications, 1178*, 107-125. doi:10.1007/978-3-031-75091-5_7

Cardenas, H. L. (2020). Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations. *IEEE Access, 8*, 61161–61173. doi:10.1109/ACCESS.2020.2983313

Center for Internet Security. (2021). *The SolarWinds Cyber-Attack: What You Need to Know.* Center for Internet Security. Retrieved from https://www.cisecurity.org/solarwinds

Chen, C. S. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly, 36*(4), 1165-1188. doi:10.2307/41703503

Computers, M. (2024). *Quantum Computing in 2024: Breakthroughs, Challenges, and What Lies Ahead.* Microtime. Retrieved from https://microtime.com/quantum-computing-in-2024-breakthroughs-challenges-and-what-lies-ahead/

Dabrowski, U. W. (2017). Grid Shock: Coordinated Load-Changing Attacks on Power Grids. (pp. 303-314). Orlando, FL: Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017) . doi:https://doi.org/10.1145/3134600.313463

Department of Homeland Security. (2025). *Homeland Threat Assessment.* Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf

Deus, D. (2023). *Ransomware costs: when the price to pay is more than just a ransom.* https://www.ricoh-usa.com/en/insights/articles/ransomware-costs.

Expert Panel. (2023). *15 Significant Ways Quantum Computing Could Soon Impact Society.* Forbes. Retrieved from https://www.forbes.com/councils/forbestechcouncil/2023/04/18/15-significant-ways-quantum-computing-could-soon-impact-society/

Gabbai, A. (2015, January). *Kevin Ashton Describes "the Internet of Things"*. Retrieved from https://www.smithsonianmag.com/: https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/

Galer, S. (2023). *If You Think AI Is Hot, Wait Until It Meets Quantum Computing.* Forbes. Retrieved from https://www.forbes.com/sites/sap/2023/03/21/if-you-think-ai-is-hot-wait-until-it-meets-quantum-computing/

Goldfarb, T. (2019). Digital economics. *Journal of Economic Literature, 57*(1), 3-43. doi:https://doi.org/10.1257/jel.20171452

He, Q. A. (2016). Designing for situation awareness of future power grids: An indicator system based on linear eigenvalue statistics of large random matrices. *IEEE Access, 4*, 3557–3568. doi:https://doi.org/10.1109/ACCESS.2016.2581838

Hernandez, A. B. (2014). Smart nest thermostat thermostat: A smart spy in your home. Black Hat USA. Retrieved from https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf

IBM. (2024). *Cost of a Data Breach Report 2024.* https://www.ibm.com/reports/data-breach.

IEC. (2016). *International Electrotechnical Commission (IEC).* IEC. Retrieved from https://webstore.iec.ch/en/publication/25035

Internet Crime Complaint Center. (2023). *Internet Crime Report 2023.* https://www.ic3.gov/. Retrieved from https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Iqbal, A. D. (2020). An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. *IEEE Internet of Things, 7*(10), 10250-10276. doi:10.1109/JIOT.2020.2997651

Jo Rushton, M. W. (2024). *50+ Phishing Statistics You Need to Know – Where, Who & What is Targeted.* Techopedia. Retrieved from https://www.techopedia.com/phishing-statistics

Jones, N. (2024, June 10). The G7 Should Lead the Transition Away from Fossil Fuels. Here's how. *International Institute for Sustainable Development*. Retrieved from https://www.iisd.org/articles/insight/g7-should-lead-transition-away-fossil-fuels-heres-how

Kaur, G. K. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. doi:DOI: 10.1016/j.inffus.2023.101804

Kenney, Z. (2016). The rise of the platform economy. *Issues in Science and Technology, 32*(3), 61. Retrieved from https://issues.org/rise-platform-economy-big-data-work/

Knake, R. (2017). *A Cyberattack on the U.S. Power Grid.* Council on Foreign Relatios. Retrieved from https://www.cfr.org/report/cyberattack-us-power-grid

Kokkola. (2010). *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem.* European Central Bank. Retrieved from https://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf

Krause, E. K. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors, 21*, 6225. doi:https://doi.org/10.3390/s21186225

Kshetri, N. (2021). Economics of Artificial Intelligence in Cybersecurity. *IT Professional, 23*(5), 73-77. doi:10.1109/MITP.2021.3096726

Laghari, L. K. (2024). Internet of Things (IoT) applications security trends and challenges. *Discover Internet of Things, 4*(36). doi:https://doi.org/10.1007/s43926-024-00090-5

Laudon, T. (2020). *E-commerce 2020: Business, Technology, Society.* Pearson. Retrieved from https://www.pearson.com/en-us/subject-catalog/p/e-commerce-2021-business-technology-and-society/P200000001390/9780136931829

Lee, M. (2021). *Quantum Computing and Cybersecurity.* Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity

Li, X. Z. (2015). The internet of things: a survey. *Information Systems Frontiers*, 243-259. doi:https://doi.org/10.1007/s10796-014-9492-7

Lipman, P. (2021). *How Quantum Computing Will Transform Cybersecurity.* Forbes. Retrieved from https://www.forbes.com/councils/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/

Lubacha, M. W. (2023). *The European Digital Economy : Drivers of Digital Transition and Economic Recovery* (1 ed.). Taylor & Francis Group. Retrieved from https://www.taylorandfrancis.com/books/the-european-digital-economy-drivers-of-digital-transition-and-economic-recovery

Macola, I. G. (2020). *The five worst cyberattacks against the power industry since 2014.* Power Technology. Retrieved from https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/

Makhdoom, A. L. (2019). Anatomy of threats to the Internet of Things. *EEE Commun. Surveys Tuts, 21*(2), 1636–1675. doi:http://dx.doi.org/10.1109/COMST.2018.2874978

Malatji, T. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*. doi:https://doi.org/10.1007/s43681-024-00427-4

Malik, P. (2025). *Tech Watch: Nine Innovations That Combine AI And Quantum Computing.* Forbes. Retrieved from https://www.forbes.com/councils/forbestechcouncil/2025/02/18/tech-watch-nine-innovations-that-combine-ai-and-quantum-computing/

Mariah St. John, B. S. (2024). *Cybersecurity Stats: Facts And Figures You Should Know.* Forbes. Retrieved from https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

Masterson, V. (2024). *Can we build a safe and inclusive 'quantum economy'?* World Economic Forum.

Meola, A. (2021). *Smart Farming in 2020: How IoT sensors are creating a more efficient precision agriculture industry.* Business insider. Retrieved from https://www.globalagtechinitiative.com/market-watch/smart-farming-in-2020-how-iot-sensors-are-creating-a-more-efficient-precision-agriculture-industry/

Nagy, C. (2024). *Hacker Nation: The World’s Third-Largest Economy.* https://www.technewsworld.com/story/hacker-nation-the-worlds-third-largest-economy-179108.html.

Okdem, O. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study. *Applied Sciences, 14*(22), 10487. doi:https://doi.org/10.3390/app142210487

Palatty, N. J. (2024). *51 Small Business Cyber Attack Statistics 2024 (And What You Can Do About Them).* https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/.

Parker, A. C. (2016). *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You.* W. W. Norton & Company. Retrieved from ttps://wwnorton.com/books/Platform-Revolution/

Pazur, B. (2025). *Quantum AI: What You Need to Know About This Far-Out Tech.* Cnet. Retrieved from https://www.cnet.com/tech/services-and-software/quantum-ai-what-is-it-and-how-does-it-work/

Petrosyan, A. (2024). *The impact of cybercrime on companies in the U.S. - Statistics & Facts.* Statistica. Retrieved from https://www.statista.com/topics/1731/smb-and-cyber-crime/

Phuangpornpitak, T. (2013). Opportunities and Challenges of Integrating Renewable Energy in Smart Grid System. *34*, pp. 282–290. Energy Procedia. doi:10.1016/j.egypro.2013.06.756

Polit, K. (2018). *Army Takes on Wicked Problems With the Internet of Battlefield Things.* Meri Talk. Retrieved from https://www.meritalk.com/articles/army-takes-on-wicked-problems-with-the-internet-of-battlefield-things/

Pott, T. (2019). *The Real Costs of Ransomware.* https://ransomware.org/blog/the-real-costs-of-ransomware/. Retrieved from https://ransomware.org/blog/the-real-costs-of-ransomware/

Priya, D. (2023). *10 Challenges In Quantum Computing.* Analytics Insight. Retrieved from https://www.analyticsinsight.net/latest-news/10-challenges-in-quantum-computing

Pudjianto, R. S. (2007). Virtual power plant and system integration of distributed energy resources. *IET Renew, 1*, 10-16. doi:https://doi.org/10.1049/iet-rpg:20060023

Rajmohan, N. F. (2022). A decade of research on patterns and architectures for IoT security. *Cybersecurity, 5*(2). doi:https://doi.org/10.1186/s42400-021-00104-7

Rose, E. C. (2015). *The Internet of Things: an overview.* Internet Society. Retrieved from https://www.internetsociety.org/resources/doc/2015/iot-overview/

Said, T. (2021). A Reliable and Scalable Internet of Military Things Architecture. *Computers, Materials & Continua*, 3887-3906. doi:https://doi.org/10.32604/cmc.2021.016076

Sean Steinberg, A. S. (2021). *NotPetya: A Columbia University Case Study.* New York: Columbia University. Retrieved from https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf

Segall. (1983). Routing in packet-switched networks. *IEEE Transactions on Information Theory, 29*, 23–35. doi:10.1109/TIT.1983.1056251

Statista. (2024). *Smart grids in the U.S. - statistics & facts.* https://www.statista.com/topics/1125/smart-grids/#topicOverview.

Statistica. (2023). *Ransomware - statistics & facts.* https://www.statista.com/topics/4136/ransomware/#topicOverview.

Swayne, M. (2023). *What Are The Remaining Challenges of Quantum Computing?* The Quantum Insider. Retrieved from https://thequantuminsider.com/

Tan, R. Z. (2024). Exploring consumers' adoption and recommendation in smart retailing: a cognitive absorption perspective. *Current Psychology*, 22560–22577. doi:https://doi.org/10.1007/s12144-024-06042-0

Tapscott. (1996). *The Digital Economy: Promise and Peril in the Age of Networked Intelligence.* New York: McGraw-Hill Companies. Retrieved from https://openlibrary.org/books/OL7297022M/The_Digital_Economy

Thorsberg, C. (2024, May 2). Seven Major Nations Agree to Phase Out Coal by 2035, Though Vague Language Leaves Wiggle Room. *Smithsonian Magazine*. Retrieved from https://www.smithsonianmag.com/smart-news/seven-major-nations-agree-to-phase-out-coal-by-2035-though-vague-language-leaves-wiggle-room-180984260/

Torkington, S. (2024). *Quantum computing could threaten cybersecurity measures. Here's why – and how tech firms are responding.* World Economic Forum. Retrieved from https://www.weforum.org/stories/2024/04/quantum-computing-cybersecurity-risks/

Tsafos, C. N. (2021). *Cyber and Other Security Risks to the U.S. Electric Power Infrastructure.* Center for Strategic and International Studies. Retrieved from https://www.jstor.org/stable/resrep32324.6

United Nations Climate Change. (2016). *G7 Leaders' Declaration Addresses Paris Agreement.* https://unfccc.int/news/g7-leaders-declaration-addresses-paris-agreement.

US Department of State. (2024). *Artificial Intelligence (AI).* https://www.state.gov/artificial-intelligence/.

Vailshery, L. S. (2024). *Internet of Things (IoT) in the U.S. - statistics & facts.* Statistica. Retrieved from https://www.statista.com/topics/5236/internet-of-things-iot-in-the-us/

Vainilavičius, J. (2023). *Cybercrime is world's third-largest economy thanks to booming black market.* https://cybernews.com/editorial/cybercrime-world-third-economy/.

Vasiliu-Feltes, I. (2023). *Impact of Quantum on the Digital Economy and Society.* Coruzant. Retrieved from https://coruzant.com/quantum/impact-of-quantum-on-the-digital-economy-and-society/

Voas. (2016). *Primitives and Elements of Internet of Things (IoT) Trustworthiness.* NIST. doi:http://dx.doi.org/10.6028/NIST.SP.800-183

Von Solms, V. N. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. doi:https://doi.org/10.1016/j.cose.2013.04.004

Wei, L. J. (2011). Protecting Smart Grid Automation Systems Against Cyberattacks. *IEEE Trans on Smart Grid, 2*, 782–795. doi:10.1109/TSG.2011.2159999

Whitehouse. (2023). *National Cybersecurity Strategy.* Washington D.C.: Whitehouse. Retrieved from https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/

World, Y. (2020). *Monitoring apps: How the Internet of Things can turn your boat into a smart boat.* https://www.yachtingworld.com/.

Xie, X.-F. (2017). Integrated In-Vehicle Decision Support System for Driving at Signalized Intersections: A Prototype of Smart IoT in Transportation. *Transportation Research Board (TRB) Annual Meeting, Washington.* Washington DC. Retrieved from https://trid.trb.org/view/1437314

Zayo. (2024). *Average DDoS Attack Cost Businesses Nearly Half a Million Dollars in 2023, According to New Zayo Data.* https://www.zayo.com/newsroom/average-ddos-attack-cost-businesses-nearly-half-a-million-dollars-in-2023-according-to-new-zayo-data/.

Zhang, N. S. (2021). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review, 55*, 1029-1053. doi:https://doi.org/10.1007/s10462-021-09976-0

Zhao, Z. X. (2020). Logistics sustainability practices: an IoT-enabled smart indoor parking system for industrial hazardous chemical vehicles. *International journal of production research*, 7490-7506. doi:https://doi.org/10.1080/00207543.2020.1720928

Zoltan Acs, A. S. (2021). The evolution of the global digital platform economy: 1971-2021. *Small Business Economy, 57*(1), 1629-1659. doi:https://doi.org/10.1007/s11187-021-00561-x

Zonouz, R. M. (2014). Detecting industrial control malware using automated PLC code analytics. *IEEE Security Privacy, 12*(6), 40-47. doi:https://doi.org/10.1109/MSP.2014.113