Journal of Technology Innovations and Energy
https://doi.org/10.56556/jtie.v3i2.907
ISSN: 2957-8809

REVIEW ARTICLE

Cyber Security and Digital Economy: Opportunities, Growth and Challenges

Ashish Juneja[1], Shankha Shubhra Goswami[2*], Surajit Mondal[3]

[1]Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, 244001, India
[2,3]Abacus Institute of Engineering and Management, Magra, Hooghly, 712148, India

Corresponding Author: Shankha Shubhra Goswami: email: ssg.mech.official@gmail.com
Received: 04 May, 2024, Accepted: 19 May, 2024, Published: 20 May, 2024

Abstract

The digital age has witnessed the exponential growth of the international economy, propelled by digital technology and the deepening interconnectedness of the global landscape. However, amidst this rapid expansion lies a plethora of Cyber Security (CS) risks within the Digital Economy (DE), ranging from hacker assaults to data breaches and intellectual property theft. The heightened importance of CS resonates across organizations, nations, and individuals worldwide. This study delves into the dynamics of development and expansion within the DE while concurrently addressing the looming threats to CS. Central to its analysis is the imperative of implementing efficient CS protocols, encompassing preventive measures, detection strategies, and swift response mechanisms against online threats. Moreover, the discourse extends to strategies for enhancing CS resilience through investments in infrastructure, capacity building initiatives, and public awareness campaigns, involving both corporate entities and governmental bodies. Furthermore, this research probes into the intricate interplay between cutting-edge technologies such as blockchain, Artificial Intelligence (AI), and the Internet of Things (IoT) and their impact on CS. While these technologies hold immense potential to revolutionize the DE landscape, they concurrently introduce novel security vulnerabilities that malicious actors may exploit. In conclusion, the study underscores that while the DE offers boundless opportunities for development and innovation, robust CS measures stand as indispensable safeguards against online threats, ensuring the sustained viability and integrity of the sector in the long term.

Keywords*:* Cyber Security, Digital Economy, Cyber-attacks, Internet of Things, Artificial Intelligence, Blockchain

Introduction

CS refers to prevent cyber-attacks, which include malware infections, phishing scams, hacking, and denial-of-service attacks. Effective CS also minimizes the impact of cyber threats on organizations and individuals (UNCTAD, 2021). CS is an increasingly critical concern in the digital age, as more and more aspects of our lives and businesses are conducted online, and cyber threats continue to evolve in complexity and frequency. Figure 1 clearly represents the growth of CS market in the last 5 years which boosted the DE market of India as well (Yengula et al., 2024). Sustainable digitalization refers to the integration of digital technologies and practices in a way that supports environmental, social, and economic sustainability. It involves using digital technologies to enhance sustainability, while also ensuring that the use of these technologies does not harm the environment or exacerbate social inequalities. In practice, sustainable digitalization can take many forms (Aiyer et al., 2022).

For example, it can involve the use of digital technologies to reduce energy consumption and carbon emissions, such as through the adoption of smart grids or energy-efficient buildings. It can also involve using digital technologies to support sustainable transportation, such as through the use of electric vehicles or ride-sharing apps. Sustainable digitalization also involves promoting digital literacy and access to digital technologies to ensure that everyone has an equal opportunity to benefit from them. This includes efforts to bridge the digital divide, provide affordable internet access, and support digital skills training and education (Chandwani, 2023; Sahoo and Goswami, 2024). Another important aspect of sustainable digitalization is data privacy and security. The current penetration of the CS technologies is very high and tends to increase in upcoming years. However, the penetrations of different CS technologies are portrayed graphically in Figure 2. Digital technologies rely on the collection and storage of vast amounts of personal data, and it is essential to ensure that this data is protected and used ethically and responsibly (Aiyer et al., 2022). Sustainable digitalization aims to harness the potential of digital technologies to create a more sustainable and equitable future, while also addressing the potential risks and challenges associated with their use.

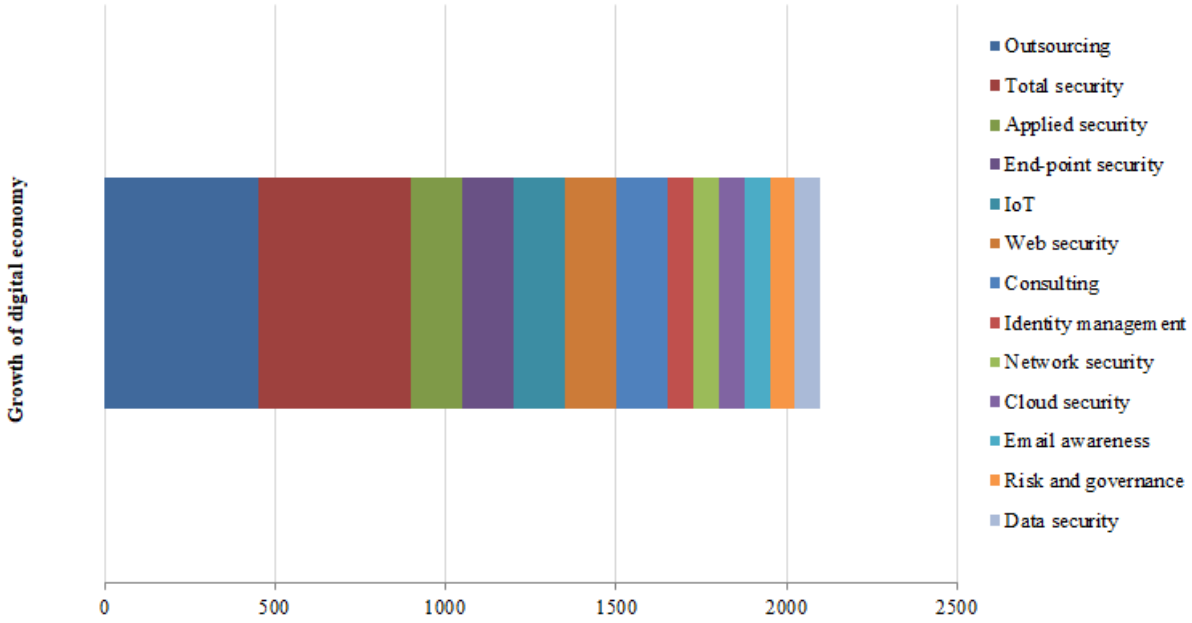

Figure 1. Market growth of digital economy in last 5 years
(Source: Aiyer et al., 2022)

To address these issues, the following research article serves the following objectives as follows.

i. To study the DE and its growth.
ii. To study the impact of CS on growth of DE.
iii. To study the linkage between CS and economic loss in the era of DE.
iv. Impact of cyber-attacks / weak cyber infrastructure on the value of DE (Understanding the economic loss due to cyber-attacks).
v. To identify the opportunities for India a trillion dollar DE.
vi. To recognize different indicators related to international trade, employment and e-commerce market.
vii. To understand the different pillars of DE.

Role of cyber security and its significance in digital economy

The role of CS is critical in the DE. As more and more aspects of our lives and businesses move online, the need to protect digital assets and information from cyber threats has become increasingly important. CS is essential to maintaining the trust and confidence of individuals and organizations in the DE, which in turn is essential for its growth and success. CS is significant in the DE for several reasons (Ministry of Electronics and IT, 2023). Firstly, it is essential for protecting digital assets and information, including personal data, intellectual property, and financial information, from theft, damage, or unauthorized access. Effective CS measures are essential to prevent cyber-attacks such as hacking, phishing, and malware infections, which can have severe consequences for individuals and organizations alike.

Secondly, CS is crucial for maintaining the integrity and reliability of digital systems and networks. Cyber-attacks can disrupt digital systems and networks, causing downtime and affecting the smooth functioning of businesses and governments (Yengula et al., 2024). Effective CS measures can minimize the impact of cyber-attacks, ensuring that digital systems and networks remain operational and secure.

Thirdly, CS is critical for promoting trust and confidence in the DE. Without effective CS measures, individuals and organizations may be reluctant to engage in online activities such as e-commerce, online banking, and remote working (Chandwani, 2023; Upadhyay, 2020). This can slow down the growth and development of the DE, limiting its potential for innovation and economic growth. The significance of CS in the DE cannot be overstated. Effective CS measures are essential for protecting digital assets and information, maintaining the integrity of digital systems and networks, and promoting trust and confidence in the DE.

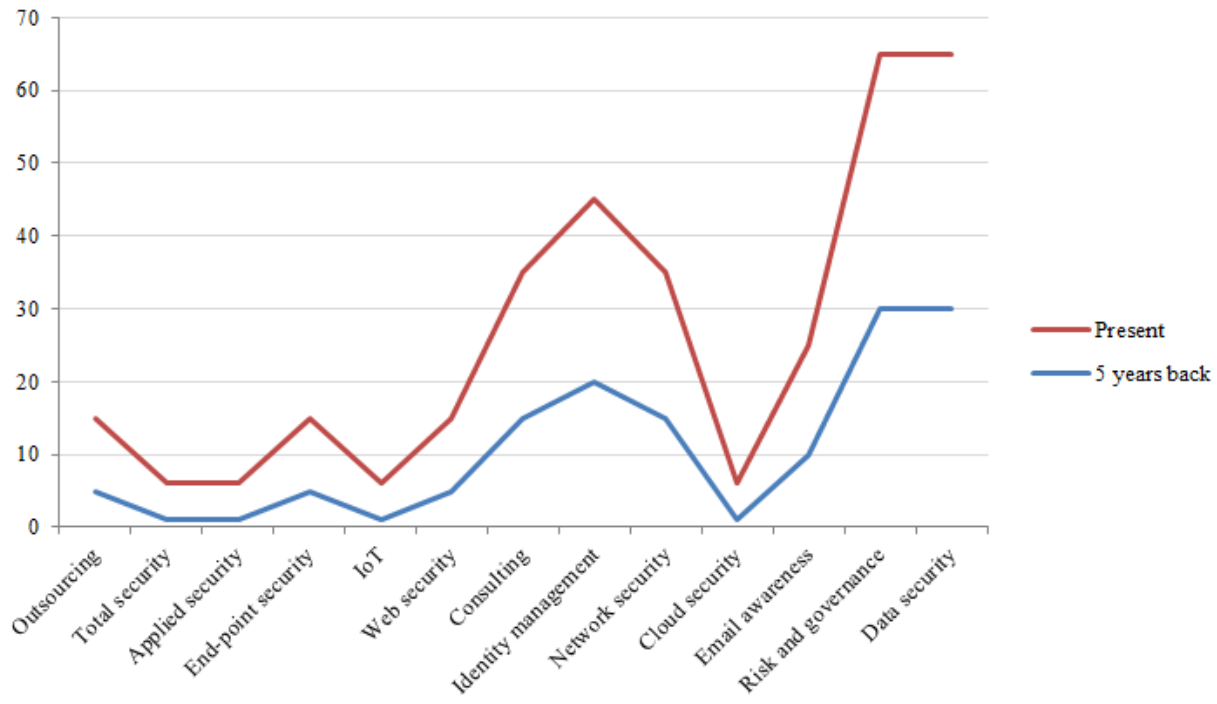

Figure 2. Market penetration growth of cyber security on digital economy
(Source: Aiyer et al., 2022)

Digital economy and the value of digital economy in the last 5 years

The value of the DE has grown rapidly in the last five years. According to reports, the value of global e-commerce sales has more than doubled since 2015, from around $2.2 trillion in 2015 to over $4.9 trillion in 2020. Similarly, the value of the global DE is projected to reach $23 trillion by 2025, up from $11.5 trillion in 2016 (UNCTAD, 2021). Figure 3 clearly portrays the financial growth of DE in last 7 years, and forecasted up to 2025. The COVID-19 pandemic has accelerated the growth of the DE, as more and more people turned to online channels for work, education, shopping, and entertainment (Zhang et al. 2022; Chandwani, 2023). For example, online retail sales increased by over 27% in the US in 2020, while digital payments and mobile banking also saw significant growth. The value of the DE is not only measured in monetary terms but also in its contribution to economic growth and development, job creation, and innovation. The DE has enabled businesses and entrepreneurs to reach new markets and customers, create new products and services, and improve productivity and efficiency (Ministry of Electronics and IT, 2023). The DE has also enabled the rise of the gig economy, with platforms such as Uber, Airbnb, and TaskRabbit creating new opportunities for people to earn income and participate in the workforce. The gig economy has grown rapidly in the last five years, with over one-third of US workers now participating in some form of gig work. In addition, the DE has also had a significant impact on traditional industries, such as retail, banking, and healthcare.

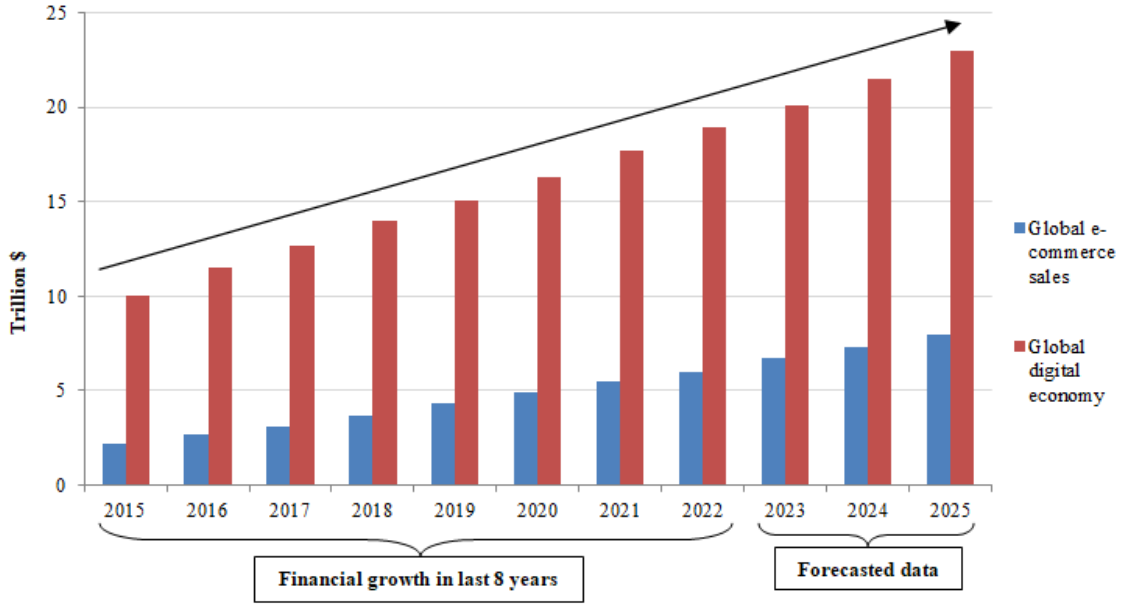

Figure 3. Previous and the forecasted growth of digital economy throughout the span of 10 years (Source: UNCTAD, 2021)

Online channels have become increasingly important for these industries, with businesses adopting digital technologies to improve customer experiences, streamline operations, and reduce costs. The value of the DE has also been driven by advancements in digital technologies such as AI, blockchain, and the Internet of Things (IoT) (Zhang et al. 2022). These technologies have enabled new forms of innovation and disruption, such as the rise of smart cities, autonomous vehicles, and personalized medicine. The DE has not been without its challenges, however. CS threats, data privacy concerns, and the digital divide are just some of the issues that must be addressed to ensure that the benefits of the DE are realized by all. Nevertheless, the value of the DE in the last five years has been undeniable, and it is expected to continue to drive economic growth and innovation in

the coming years (Sahoo and Goswami, 2024; Yengula et al., 2024). The study is structured to examine the prospects for development and expansion in the DE while concurrently addressing the threats to CS and emphasizing the significance of implementing efficient CS procedures, exploring avenues for improvement through investments in infrastructure and capacity building initiatives, and investigating the impact of cutting-edge technologies on CS resilience.

Literature Review

The DE has become a crucial driver of growth and innovation worldwide, but it also presents new security challenges. As the use of technology continues to increase, so does the risk of cyber threats. This paper will explore the relationship between CS and the DE, with a focus on the challenges and opportunities for businesses and governments.

Existing literature on literature on cyber security and digital economy

CS is an essential aspect of modern-day computing and is a constantly evolving field of study. With the growth of the internet and the increasing reliance on computer systems, CS has become an important concern for businesses, governments, and individuals. This literature review explores some of the latest research and trends in CS. The frequency and severity of cyber-attacks continue to increase, with attackers using sophisticated techniques to exploit vulnerabilities in computer systems. In a study by Alhayani et al. (2021), they identified the top ten cyber threats that organizations face, including phishing attacks, ransom ware, and distributed denial of service (DDoS) attacks. They also proposed measures that organizations can implement to mitigate these threats, such as regular security audits and employee training programs. Various standards and best practices has been taken for implementing CS measures that provides a systematic approach to managing CS risks. In a study by Abduvakhidov et al. (2021), they evaluated the effectiveness of the NIST CS Framework in improving the CS posture of organizations. They found that the framework was effective in helping organizations identify and manage CS risks.

AI and ML techniques are increasingly being used in CS to identify and mitigate cyber threats. In a study by Santos et al. (2020), they explored the use of machine learning techniques in detecting and preventing DDoS attacks. They found that the use of ML algorithms improved the accuracy and effectiveness of DDoS detection. IoT is a rapidly growing network of interconnected devices, which presents unique CS challenges. In a study by Monteith et al. (2021), they examined the security challenges of the IoT and proposed a framework for securing IoT systems. The framework included measures such as device authentication and access control to mitigate the risks associated with the IoT. It is a rapidly growing area of the global economy and has significant implications for businesses, governments, and individuals. This literature review explores some of the latest research and trends in the DE.

In a study by Popkova and Gulzat (2020), they examined the impact of digital transformation on the Indian banking industry. They found that digital transformation has resulted in significant rise in recent years, with more and more consumers opting to shop online. In a study by Chen et al. (2021), they examined the factors that influence consumers' online shopping behavior in India. They found that factors such as product quality, price, and delivery time significantly influenced consumers' decision to shop online. Digital platforms refer to online platforms that facilitate interactions between different groups, such as businesses and consumers. In a study by Xu (2020), they examined the role of digital platforms in the Chinese sharing economy. They found that digital platforms play a significant role in enabling sharing economy transactions and reducing transaction costs. In the DE, big data and analytics play a crucial role in providing insights that can inform business decisions. In a study

by Wilson et al. (2022), they examined the impact of big data and analytics on the Indian insurance industry. They found that big data and analytics can help insurers improve risk management, customer experience, and operational efficiency.

Evaluation of previous studies literature on cyber security and growth of digital economy

CS is an increasingly important area of research, with a growing number of studies examining different aspects of this field. For example, a study by Tosun et al., (2021) explored the relationship between cyber-attacks and stock market performance. They found that cyber-attacks had a significant negative impact on stock market performance, highlighting the need for effective CS measures to mitigate these risks. Another study by Yenugula et al. (2024) examined the use of machine learning algorithms in CS. They found that machine learning techniques could be effective in identifying and mitigating cyber threats, particularly when used in combination with other CS measures. A study by Sobb et al. (2020) explored the challenges of CS risk management in the context of supply chain management. They found that CS risks were a significant concern for supply chain management and that effective risk management strategies were needed to address these risks. The DE is a rapidly growing area of research, with a wide range of studies examining different aspects of this field.
For example, a study by Zhang et al. (2021) highlights the potential benefits of investing in digital infrastructure and skills. Another study by Mützel (2021) examined the growth of the DE, with increased adoption of digital payments leading to increased digital entrepreneurship and innovation. A study by Pan et al. (2022) explored the role of digital platforms in the growth of the DE. They found that digital platforms could help drive innovation and growth in the DE, particularly by facilitating collaboration and enabling new business models. There is a growing body of research exploring different aspects of CS and the measurement and growth of the DE. These studies provide valuable insights into the challenges and opportunities presented by these rapidly evolving fields, and highlight the need for continued research to address these challenges and leverage these opportunities.

Past literatures on cyber security addressing economic advancements and economic concerns

Previous literature has inspected the association between CS and monetary advancements as well as economic concerns. One study by Litvinenko (2020) examined the link between CS and financial growth in South Korea. The study found that investment in CS was positively associated with economic growth, suggesting that CS measures could play an vital role in promoting economic development. Another study by Lis and Mendel (2019) explored the impact of cyber-attacks on the global economy. The study estimated that cyber-attacks could cost the global economy up to $2.1 trillion by 2019, highlighting the potential economic impact of CS threats. A study by Yudhiyati et al. (2021) examined the impact of CS on e-commerce in Indonesia. The study found that CS concerns were a significant barrier to the growth of e-commerce in Indonesia, and that effective CS measures were needed to promote the growth of this important economic sector.
In addition, a study by Sturgeon (2021) explored the relationship between CS and financial stability. The study found that CS risks posed a significant threat to financial stability, and that effective CS measures were needed to mitigate these risks and maintain the stability of the financial system. These studies demonstrate the importance of CS in promoting economic growth and stability, as well as the potential economic impact of CS threats. They highlight the need for continued research and investment in CS measures to address these challenges and promote economic development.

Research gap on cyber security and digital economy

While there is a growing body of literature on CS and the DE, there are still some research gaps that need to be addressed. One research gap is the need for more research on the specific CS risks and challenges faced by different sectors of the DE, such as e-commerce, fintech, and online platforms. This could include exploring the effectiveness of different CS measures in addressing these risks, as well as identifying best practices for managing CS in these sectors. Another research gap is the need for more research on the impact of CS on the adoption and growth of emerging technologies such as blockchain, AI, and the Internet of Things. This could include exploring the potential benefits and risks of these technologies in terms of CS, as well as identifying effective CS measures for managing these risks.

There is also a need for more research on the relationship between CS and economic development, particularly in developing countries. This could include exploring the effectiveness of different CS measures in promoting economic growth, as well as identifying the specific challenges faced by developing countries in implementing effective CS strategies. Finally, there is a need for more research on the role of CS in promoting digital inclusion and addressing the digital divide. This could include exploring the potential benefits and risks of different CS measures for different groups of users, as well as identifying strategies for promoting CS awareness and education among underserved communities. Addressing these research gaps could help to improve our understanding of the complex relationship between CS and the DE, and identify effective strategies for managing CS risks and promoting economic development in the digital age.

Novelty on cyber security and digital economy

One area of novelty in the study of CS and the DE is the increasing focus on the intersection of these two fields. As the DE continues to grow and evolve, the importance of CS as a critical component of this ecosystem is becoming increasingly clear. Another area of novelty is the emergence of new CS challenges and risks as a result of the rapid growth of the DE. For example, the rise of the sharing economy has led to new CS risks associated with the sharing of personal information and financial transactions on online platforms. Similarly, the growing use of blockchain technology is presenting new CS challenges related to the security and integrity of distributed ledgers. Finally, there is novelty in the development of new CS technologies and solutions designed specifically for the DE. For example, machine learning and AI are being used to develop more advanced threat detection and response capabilities, while blockchain technology is being used to create more secure and transparent data storage and sharing systems. The increasing integration of CS and the DE, the emergence of new CS risks and challenges, and the development of new CS solutions and technologies all represent novel and rapidly evolving areas of research and practice in this field.

Sources of Cyber Security, Measurement and Growth of Digital Economy

Sources of information on CS and the measurement and growth of the DE can be found in a variety of academic journals, reports, and other publications. These sources, among others, can provide valuable insights into the current state of CS and the DE, as well as emerging trends and challenges in these fields (UNCTAD, 2021). Different agencies and companies have established various CS frameworks to mitigate the risk of cyber threats and simultaneously enhancing the cyber protection security. However, the authors have identified 8 potential CS frameworks depicted in Figure 4.

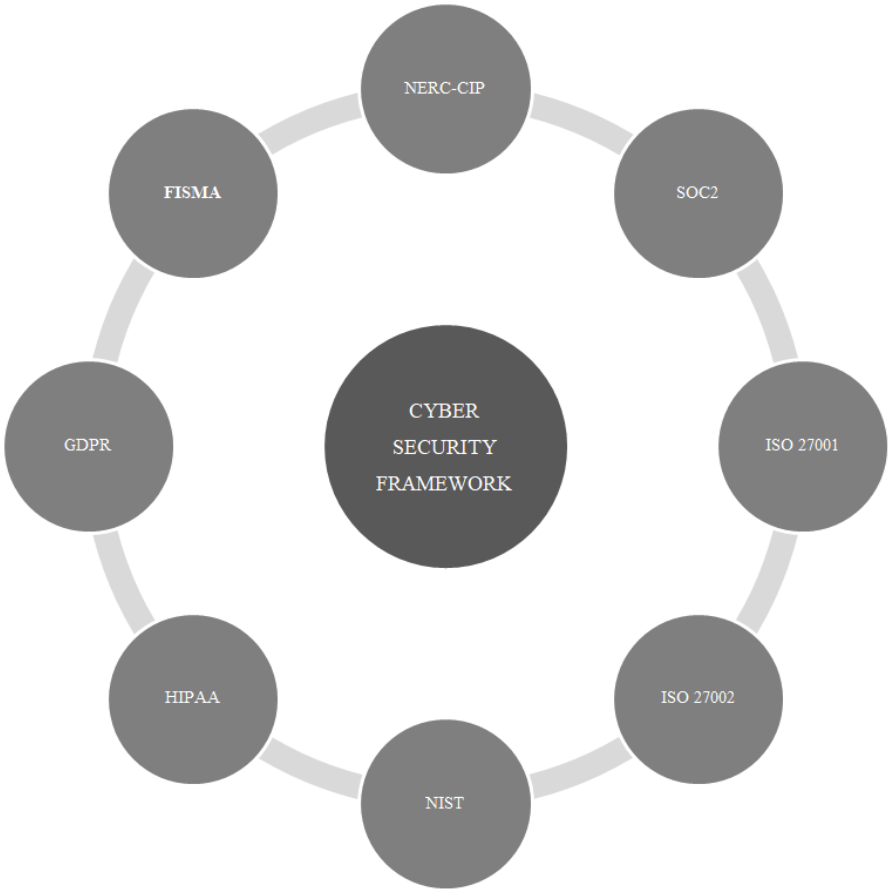

Figure 4. Cyber security frameworks
(Source: Cisternelli, 2023)

Sustainable digitization standards

Sustainable digitization standards refer to the principles and guidelines that ensure that digital technologies are developed and used in a way that is environmentally sustainable, socially responsible, and economically viable (Abduvakhidov et al. 2021; Chandwani, 2023). Here are some examples of sustainable digitization standards with detailed explanations. Digital economic indicators are also evaluated for different Asian countries using SPSS22.0 for the last 5 years of time span and depicted in Figure 5. Sustainable digitization standards emphasize the importance of energy efficiency in digital technologies. This includes the design and use of hardware and software that consume less energy and reduce carbon emissions. For example, data centers and servers can be designed to use renewable energy sources, such as solar or wind power. Additionally, software can be optimized for energy efficiency by minimizing the use of resources such as CPU and memory. Sustainable digitization standards promote the use of digital products that can be easily upgraded and maintained. Additionally, end-of-life products can be recycled or repurposed, rather than being disposed of in landfills. Sustainable digitization standards also focus on ethical and social responsibility in the development and use of digital technologies. This includes the protection of privacy, the prevention of discrimination, and the promotion of diversity and inclusion. Additionally, digital technologies should be developed and used in a way that supports human rights and environmental sustainability.

Sustainable digitization standards promote the use of open standards in the development of digital technologies. This ensures that digital products and services are interoperable and can be easily integrated with other systems. Additionally, open standards promote innovation and competition, which can drive down costs and improve efficiency. Sustainable digitization standards also prioritize accessibility, ensuring that digital technologies are usable by people with disabilities. This includes the use of assistive technologies, such as screen readers and voice recognition software, and the development of accessible user interfaces. Sustainable digitization standards focus on energy efficiency, circular economy, ethical and social responsibility, open standards, and accessibility. By following these principles and guidelines, digital technologies can be developed and used in a way that is environmentally sustainable, socially responsible, and economically viable. It is better to look at the sustainable digitalization standards that will help to boost the financial economy and simultaneously also reduce the complexity of CS compliance. The above points define the goals of DE to promote the sustainable digitalization standards.

Risk assessments in cyber security economic growth

Risk assessments are a critical component of CS, as they help organizations identify and prioritize potential risks to their digital assets, data, and systems. Effective risk assessments can help prevent cyber-attacks, reduce the impact of successful attacks, and ensure business continuity. In turn, this can contribute to economic growth by safeguarding the reputation, intellectual property, and financial stability of organizations. Here are some ways in which risk assessments can contribute to economic growth in the context of CS. Figure 6 portrays different aspects on mitigating the risk of cyber threats and enhancing the growth of digital economy. Risk assessments can help identify potential threats to intellectual property, such as trade secrets, patents, and copyrights. By implementing appropriate safeguards, such as access controls, encryption, and data backup, organizations can reduce the risk of theft or misuse of this valuable information. Risk assessments can help identify potential threats to an organization's reputation, such as data breaches or cyber-attacks. By implementing appropriate response plans, organizations can minimize the impact of these incidents on their reputation and avoid potential economic fallout. By addressing CS risks, organizations can create a more secure environment for innovation and entrepreneurship. This can foster economic growth by enabling the development of new technologies and business models that rely on digital infrastructure. Risk assessments are a critical component of CS and can contribute to economic growth by protecting critical infrastructure, safeguarding intellectual property, ensuring regulatory compliance, mitigating reputational damage, and promoting innovation. By investing in CS risk assessments, organizations can create a more secure and resilient digital environment that can support long-term economic growth.

Encryption and data protection in cyber security and economic growth

Encryption and data protection are critical components of CS, as they help safeguard sensitive data from unauthorized access, theft, and misuse (Li et al., 2020). Effective encryption and data protection can contribute to economic growth in several ways. Encryption and data protection can help protect valuable intellectual property, such as trade secrets, patents, and copyrights. By preventing unauthorized access to this sensitive information, organizations can reduce the risk of theft or misuse that could negatively impact their bottom line. Many regulations require organizations to protect sensitive data through encryption and other security measures. By ensuring compliance with these regulations, organizations can avoid costly fines and legal penalties that could negatively impact their bottom line. Many countries require organizations to use encryption and other security measures when conducting international trade. By implementing effective encryption and data protection,

organizations can facilitate international trade and expand their global reach, contributing to economic growth. Encryption and data protection can foster innovation by creating a secure environment for the development of new technologies and business models that rely on digital infrastructure. By protecting sensitive data and intellectual property, organizations can encourage the development of new and innovative products and services, contributing to long-term economic growth. Encryption and data protection are critical components of CS that can contribute to economic growth by protecting intellectual property, ensuring regulatory compliance, maintaining customer trust, facilitating international trade, and encouraging innovation (Li et al., 2020; Popkova and Gulzat, 2020). By investing in effective encryption and data protection, organizations can create a more secure and resilient digital environment that can support long-term economic growth.

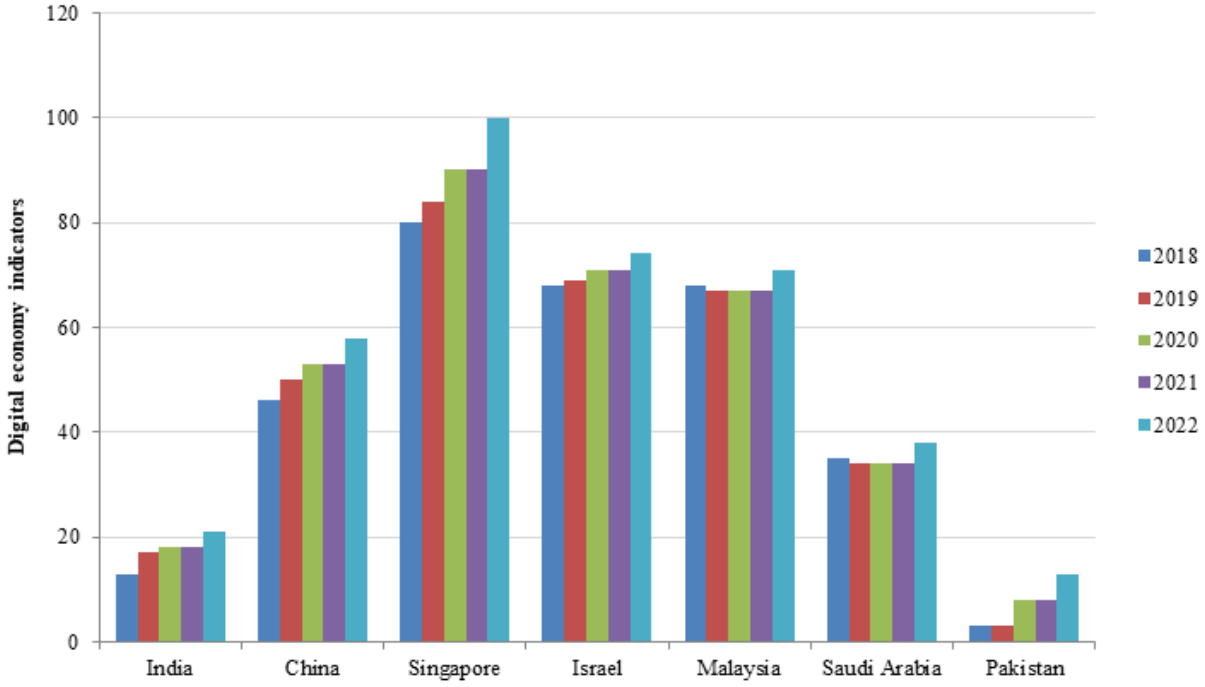

Figure 5. Digital economic indicators of different Asian countries from 2018 to 2022
(Source: UNCTAD, 2021)

Security testing and vulnerability assessments of cyber security on economic growth

Security testing and vulnerability assessments are critical components of CS, as they help organizations identify potential security weaknesses and vulnerabilities in their digital infrastructure (Chen et al. 2021; Tosun et al., 2021). Effective security testing and vulnerability assessments can contribute to economic growth in several ways. The vulnerability assessment of CS on economic growth has been clearly illustrated in Figure 7. By reducing the risk of successful cyber-attacks, organizations can avoid costly data breaches and other security incidents that could negatively impact their bottom line. Many regulations require organizations to conduct security testing and vulnerability assessments to ensure the security of their digital infrastructure. By ensuring compliance with these regulations, organizations can avoid costly fines and legal penalties that could negatively impact their bottom line. Security testing and vulnerability assessments can foster innovation by creating a secure environment for the development of new technologies and business models that rely on digital infrastructure. By identifying potential security weaknesses and vulnerabilities, organizations can work to

address them and create a more secure and resilient digital environment that can support the development of new and innovative products and services. Security testing and vulnerability assessments can help organizations meet industry standards for CS. By adhering to these standards, organizations can demonstrate a commitment to CS best practices and differentiate themselves from competitors, contributing to long-term economic growth. Security testing and vulnerability assessments are critical components of CS that can contribute to economic growth by reducing the risk of cyber-attacks, improving regulatory compliance, enhancing customer trust, encouraging innovation, and supporting industry standards (Tosun et al., 2021). By investing in effective security testing and vulnerability assessments, organizations can create a more secure and resilient digital environment that can support long-term economic growth.

G20 summit for digital economy

The G20 summit represents the world's major economies, to discuss and coordinate on various global economic issues. While the G20 has discussed digital economy-related topics in the past, there has not been a specific G20 summit dedicated solely to the digital economy as of my knowledge cutoff in September 2021 (Aliyev, 2022). However, it is important to note that the G20 has recognized the significance of the digital economy and has addressed related issues in its annual summits. The G20 leaders have discussed topics such as digital transformation, digital trade, digital infrastructure, CS, data protection, and digital inclusiveness. Considering the rapid advancements in technology and the growing impact of the digital economy, it is possible that the G20 may convene a dedicated summit to address digital economy-related issues in the future (Aliyev, 2022; Sturgeon, 2021). As year passes by, the concept of digitalization is increasing and reaching on the peak. As per the reports, the DE of India has been growing since last 5 years. The acceleration of growth in DE has been measured as 2.4 times faster than the growth in traditional economy (Sharma, 2022). This summit is very important to shape the future economy of India and most of the important things highly depend on G20. The G20 summit has contributed highly towards the growth of DE of India and it has been accelerated by 'Digital India' campaign. It is also evident that there is high growth of model investment highlighting drive growth towards employment. There is an increase of almost 11.6% in employment status across different sectors and nearly 62.4 million of workers have been engaged in dependent digital economy across the country (Sharma, 2022).

Potential Threats Caused by Cyber-Attacks to Digital Economy

Cyber-attacks can pose significant threats to the DE in several ways (Abduvakhidov et al., 2021; Li et al., 2020). Some of the potential threats caused by cyber-attacks to the DE may be explained as follows. Cyber-attacks can cause financial losses to businesses and individuals, resulting in a decline in the DE's overall financial health and stealing of personal identification, to carry out fraudulent activities, leading to significant financial losses. There is a possibility in data breaches in cyber-attacks, where personal data, trade secrets, and confidential information can be exposed, resulting in financial and reputational damage. Cyber-attacks can undermine consumer confidence in online transactions and e-commerce platforms, leading to a decline in the DE's growth. Consumers may become reluctant to conduct online transactions, leading to a significant decrease in the volume of digital commerce. Cyber-attacks can damage the reputation of businesses and individuals, resulting in a decline in their digital presence and sales. This can have a ripple effect across the DE, leading to decreased economic activity and growth. Cyber-attacks can pose significant threats to the DE, resulting in financial losses, disruptions of critical infrastructure, data breaches, impacts on consumer confidence, and damage to reputation (Li et al., 2020; Monteith et al., 2021). Therefore, it is essential to implement robust CS

measures to protect against cyber threats and safeguard the DE's growth and prosperity. Risk can highly affect the status of digital economy which can ultimately decide one country's future.

Cyber security and economic loss

CS is a critical concern for both governments and businesses due to the potential economic losses associated with cyber-attacks (Goswami and Behera, 2021; Santos et al., 2020). Cyber-attacks can lead to various forms of economic loss. Some of them have been elaborately discussed in the section as follows. The collapse of a cryptocurrency exchange can result in legal actions against the exchange's operators, including investigations, lawsuits, and potential criminal charges. Authorities may aim to hold individuals or entities accountable for any wrongdoing or negligence that contributed to the collapse. The Jamtara frauds are notorious for targeting online banking users. They use various techniques to gain unauthorized access to victims' online banking accounts, such as keylogging, fake mobile apps, or manipulating victims into sharing their login credentials. Once they gain access, they can siphon off funds from the victims' accounts, leading to significant financial losses. Fraudsters also lure individuals into fraudulent investment schemes promising high returns. They create fake investment websites or social media profiles, attracting victims with lucrative offers. Once victims invest their money, the fraudsters disappear, leaving victims with significant financial losses. Fraudsters create fake UPI apps that closely resemble legitimate ones.

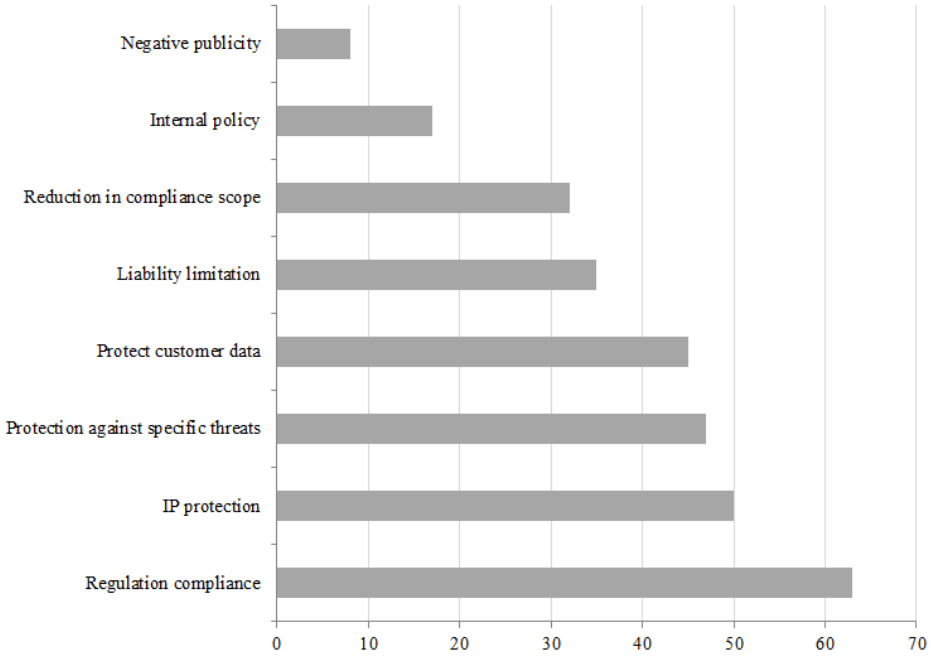

Figure 6. Contribution of different aspects on growth of digital economy
(Source: Overvest et al., 2016)

When users download and use these apps, their login credentials and sensitive information are captured by the fraudsters. These fake apps can also trick users into making payments to fraudulent accounts instead of intended recipients. Fraudsters use skimming devices to capture credit card information when the card is swiped or inserted into compromised payment terminals. This information is then used to create counterfeit cards or for online transactions. To prevent this, individuals should be cautious when using their cards at unfamiliar or suspicious-looking payment terminals and regularly monitor their credit card statements for any unauthorized

charges. To mitigate the risk of economic loss, it is important for businesses to educate their employees and customers about the risks and to implement security measures such as two-factor authentication and email filtering (Monteith et al., 2021; Santos et al., 2020). It is also important for individuals to be vigilant and cautious when responding to emails or messages, and to report suspicious activity to the appropriate authorities. However, different ways may be adopted by the government to mitigate the risk of economic loss. The pyramid structure shown in Figure 8 completely illustrates the step-wise solution to reduce the risks of economic loss in DE.

Role of Sustainability in Promoting Digital Economy

Sustainability and CS are closely interconnected, and promoting sustainable digitization can help improve CS in the DE (Ma and Zhang, 2019; Yenugula et al., 2024).

Environmental impact

The environmental impact of digital technologies is a critical factor in promoting CS and sustainable digitization in the economy (Goswami et al., 2022; Yengula et al., 2023). Here are some of the ways that environmental impact can promote CS and sustainable digitization. Digital technologies consume a significant amount of energy, and improving energy efficiency can help reduce the environmental impact of digital technologies while promoting CS. This can be achieved by adopting energy-efficient hardware and software solutions, reducing unnecessary digital activity, and optimizing data center operations. Sustainable infrastructure, such as renewable energy sources, can help reduce the carbon footprint of digital technologies. In addition, sustainable infrastructure can be designed with CS in mind, making it more resilient to cyber threats. The environmental impact of digital technologies is closely tied to data privacy. Collecting and storing data can lead to significant energy consumption and carbon emissions. Therefore, protecting data privacy can reduce the environmental impact of digital technologies while promoting CS. The circular economy, which promotes the reuse and recycling of materials, can also be applied to digital technologies. Adopting a circular economy approach to digital technologies can help reduce waste and the environmental impact of digital technologies, while also promoting CS through secure data disposal and responsible e-waste management. The environmental impact of digital technologies is closely tied to CS and sustainable digitization in the economy (Ma and Zhang, 2019; Zhang et al., 2021). Improving energy efficiency, adopting sustainable infrastructure, protecting data privacy, promoting a circular economy, and promoting digital literacy can all contribute to a more sustainable and secure DE. Therefore, environmental issues are one of the important aspects that need to be handled very carefully while dealing with CS and DE.

Ethical use of technology

The ethical use of technology plays a crucial role in promoting CS and sustainable digitization in the economy (Barmuta et al., 2020; Sobb et al., 2020). Here are some of the ways that ethical use of technology can promote CS and sustainable digitization. Ethical considerations should be included in the design and development of digital technologies. Responsible innovation practices can help ensure that digital technologies are developed with security and sustainability in mind, reducing the risk of cyber threats and promoting a more sustainable DE. Ethical hacking can help identify vulnerabilities in digital systems and promote CS. By using ethical hacking practices, businesses and organizations can identify and address potential cyber threats before they can cause harm. Promoting digital literacy and ethical use of technology can help individuals and organizations understand the importance of CS and sustainable digitization. By promoting digital literacy and ethical use of technology,

individuals and organizations can take a more proactive approach to CS, reducing the risk of cyber threats and promoting a more sustainable DE. The ethical use of technology is essential in promoting CS and sustainable digitization in the economy. Responsible innovation, data privacy, corporate social responsibility, ethical hacking, and digital literacy are all important components of ethical use of technology (Chen et al. 2021; Popkova and Gulzat, 2020). By promoting ethical use of technology, businesses and organizations can reduce the risk of cyber threats, promote sustainability, and ensure a secure and resilient DE.

Resilient digital infrastructure

Resilient digital infrastructure is a critical factor in promoting CS and sustainable digitization in the economy (Lis and Mendel, 2019; Pan et al., 2022). Here are some of the ways that resilient digital infrastructure can promote CS and sustainable digitization. Resilient digital infrastructure is designed to be secure and resistant to cyber threats. By implementing security measures such as firewalls, intrusion detection systems, and data encryption, businesses and organizations can reduce the risk of cyber-attacks and promote CS. Resilient digital infrastructure is designed to be reliable and available, even in the event of a cyber-attack or other disruption. By ensuring that digital systems and services are available and reliable, businesses and organizations can maintain productivity and minimize the impact of cyber threats. Resilient digital infrastructure is designed to be scalable and flexible, allowing businesses and organizations to adapt to changing needs and requirements. This can include the ability to quickly add or remove digital resources, such as servers or storage, in response to changing demand. Resilient digital infrastructure can also be designed with sustainability in mind, by incorporating energy-efficient hardware and software solutions, optimizing data center operations, and using renewable energy sources.

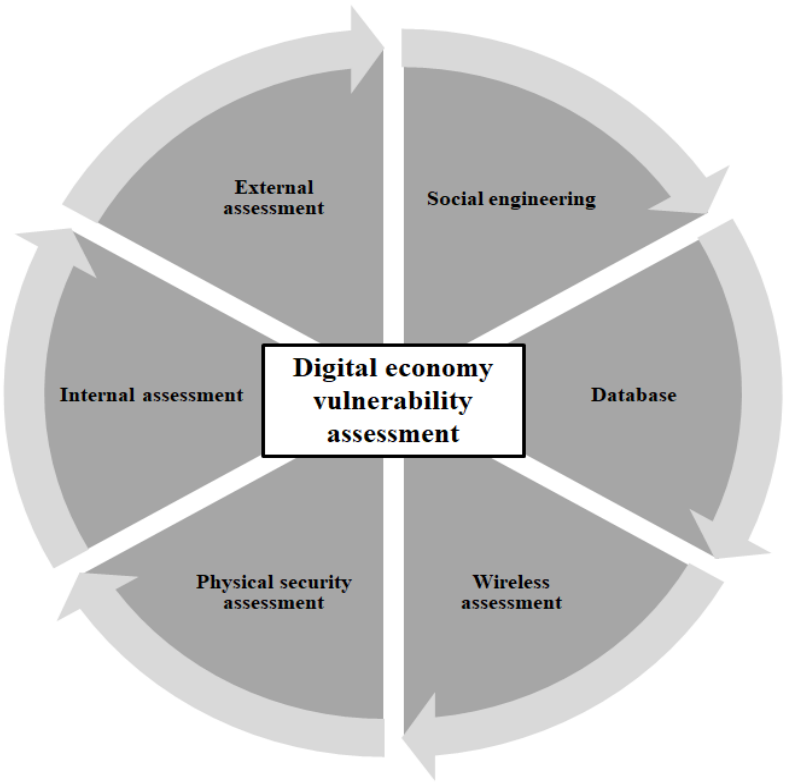

Figure 7. Vulnerability of digital economy
(Source: Infosight, 2016)

This can help reduce the environmental impact of digital technologies while promoting CS. Resilient digital infrastructure can include disaster recovery solutions, such as backup and recovery systems that allow businesses and organizations to quickly recover from a cyber attack or other disruptive event. By implementing disaster recovery solutions, businesses and organizations can minimize downtime and maintain productivity. Resilient digital infrastructure is critical in promoting CS and sustainable digitization in the economy. Security, reliability, scalability, sustainability, and disaster recovery are all important components of resilient digital infrastructure (Yudhiyati et al., 2021). By implementing resilient digital infrastructure, businesses and organizations can reduce the risk of cyber threats, maintain productivity, and promote a more sustainable and secure DE.

Innovation and collaboration

Innovation and collaboration play an important role in promoting CS and sustainable digitization in the economy (Aliyev, 2022; Lis and Mendel, 2019; Yudhiyati et al., 2021). Here are some ways in which innovation and collaboration can promote CS and sustainable digitization. Innovation in digital technologies can lead to the development of new and more secure technologies, making it more difficult for cyber criminals to compromise digital systems. This can include the development of AI and machine learning technologies that can help detect and respond to cyber threats in real time. Collaboration among organizations can help promote best practices and standards for CS and sustainable digitization. This can include the sharing of threat intelligence and CS practices, which can help organizations, learn from each other and improve their CS posture. Collaboration between the public and private sectors can help promote CS and sustainable digitization. Governments can provide guidance and resources to help businesses and organizations improve their CS posture, while businesses can share their expertise and best practices with government agencies. Innovation in education and awareness campaigns can help promote CS and sustainable digitization. By educating individuals and organizations on the importance of CS and sustainable digitization, we can create a culture of CS and sustainability that promotes safe and responsible use of digital technologies. Investment in research and development can lead to the development of new and innovative solutions for CS and sustainable digitization. This can include the development of new technologies, as well as the development of new policies and frameworks to promote CS and sustainability. Innovation and collaboration are important in promoting CS and sustainable digitization in the economy (Mützel, 2021). By promoting technology innovation, collaboration among organizations, public-private partnerships, education and awareness, and investment in research and development, we can create a more secure and sustainable DE.

Different Pillars of Digital Economy

The digital economy is a broad term that encompasses various aspects of economic activity facilitated by digital technologies and the internet. While different frameworks exist, the following are commonly recognized as the pillars of the DE (Popkova and Gulzat, 2020; Tosun et al., 2021). In the following article five pillars of DE have been identified and explained as follows. The 5 pillars are also illustrated in Figure 9. This pillar encompasses a wide range of services delivered digitally. It includes online platforms for entertainment (streaming services, online gaming), digital content creation and distribution (e-books, digital music, podcasts), online advertising, cloud computing, software-as-a-service (SaaS), and various online platforms and marketplaces that facilitate service provision. The DE relies on robust and advanced infrastructure, including telecommunications networks, broadband internet access, data centers, and cloud computing services. These foundational elements enable the

smooth functioning of various digital activities, including data storage, data transfer, and real-time communication. This pillar refers to the digitalization of financial services, commonly known as fintech.
It includes online banking, mobile payment platforms, digital currencies (such as Bitcoin), crowd funding, robo-advisors, and peer-to-peer lending. Digital finance has brought about financial inclusion, streamlined processes, and enabled innovative financial products and services. This pillar focuses on the technologies and platforms that facilitate digital communication and collaboration.

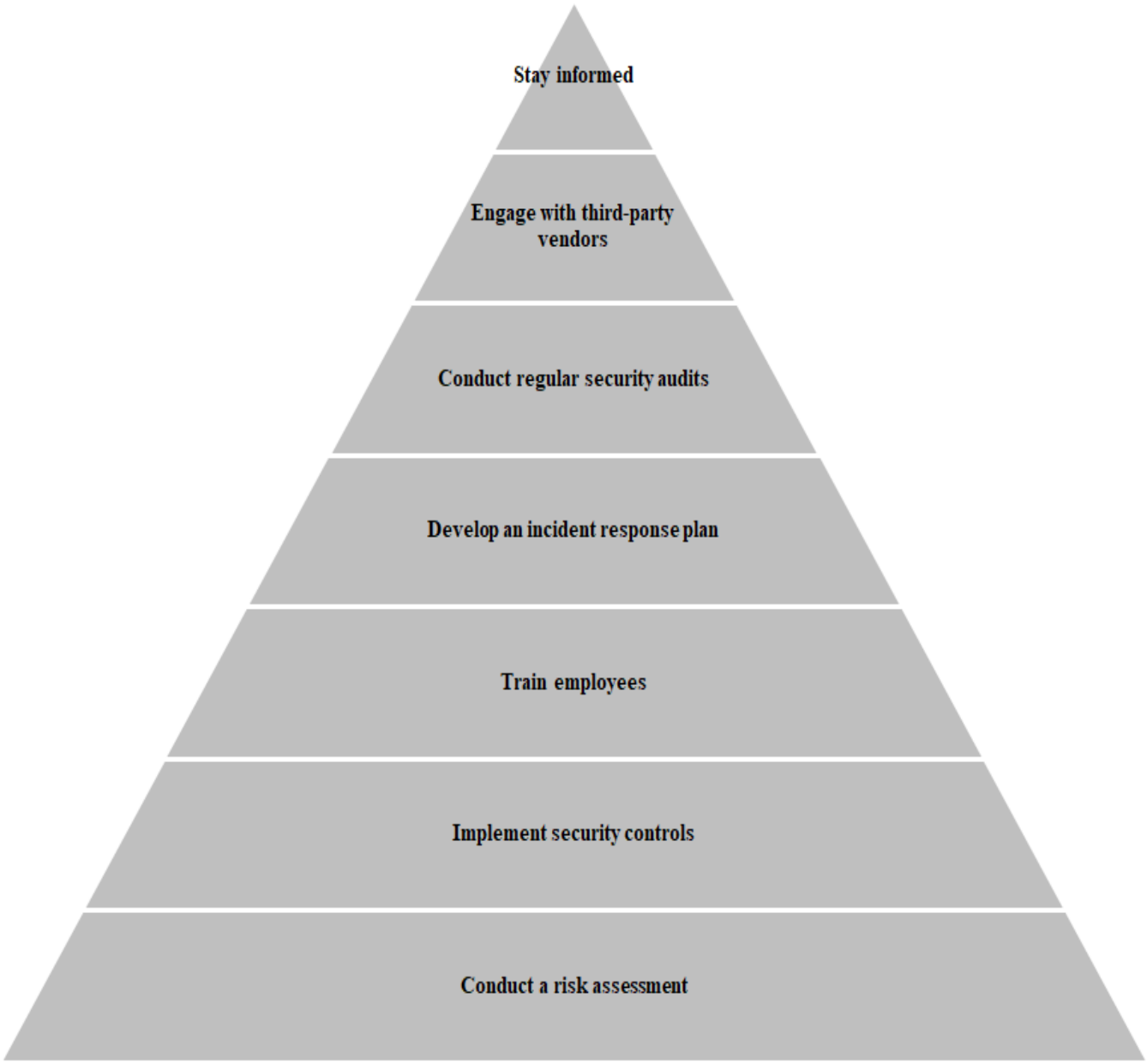

Figure 8. Step-wise Solution to Mitigate the Risk of Cyber Security
(Source: Author's own elaboration)

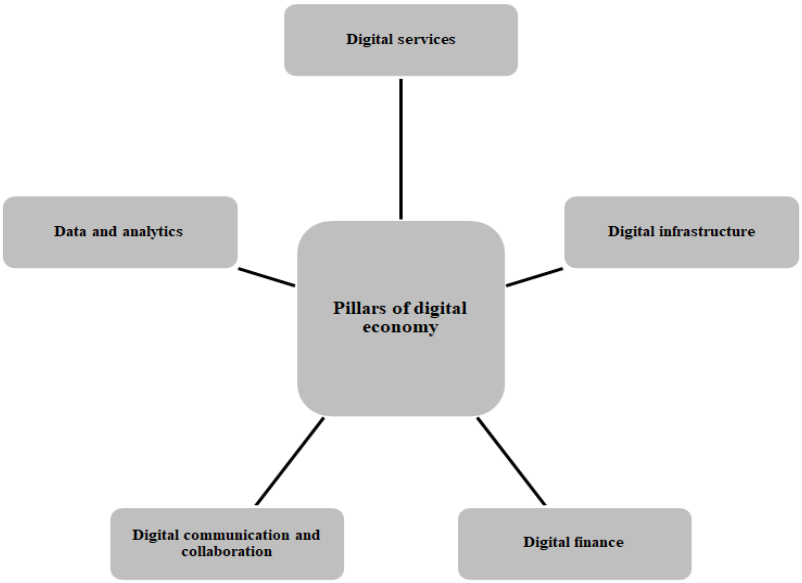

Figure 9. Pillars of digital economy
(Source: Cusolito et al., 2022)

It includes email, instant messaging, video conferencing, virtual meetings, project management tools, and collaborative workspaces. Digital communication and collaboration tools have transformed the way individuals and organizations interact, enabling remote work, global collaboration, and improved productivity.The DE generates vast amounts of data, and this pillar revolves around the collection, analysis, and utilization of that data. Data and analytics provide valuable insights, inform business strategies, enhance customer experiences, and drive innovation. These pillars are interconnected and mutually reinforcing, shaping the modern economy and driving digital transformation across industries (Popkova and Gulzat, 2020). They create opportunities for economic growth, innovation, efficiency gains, and new business models.

Conclusion

The rapid expansion of the DE has ushered in myriad opportunities for businesses, governments, and individuals alike. However, this growth has concurrently introduced a host of challenges, particularly in the realm of CS threats. Cyber-attacks pose significant risks to the DE ecosystem, encompassing financial losses, reputational harm, and erosion of consumer trust. Mitigating these risks necessitates the implementation of robust CS measures that foster sustainable digitization practices. Addressing these challenges calls for concerted efforts and collaboration among stakeholders, spanning governments, businesses, civil society organizations, and individuals. By prioritizing the adoption of stringent CS protocols, promoting ethical utilization of technology, fostering innovation and research initiatives, advocating for sustainability principles, and championing corporate responsibility, we can cultivate a more resilient and secure DE. Although formidable obstacles may impede progress, the allure of growth and innovation within the DE remains undeniable. With a strategic and holistic approach, we can harness the transformative potential of digital technologies to forge a future characterized by prosperity, security, and sustainability for all stakeholders.

Practical implications

The research on CS and the DE has practical implications for a wide range of stakeholders, including businesses, governments, civil society organizations, and individuals. Here are some practical implications that can be drawn from this research. The research highlights the need for robust CS measures to protect digital assets and data. Businesses, governments, and individuals must prioritize CS to mitigate the risks of cyber-attacks and data breaches. The research emphasizes the importance of collaboration among stakeholders to promote CS and sustainable digitization. This includes public-private partnerships, sharing of best practices, and collaborative research and development. The research highlights the need for ethical use of technology to promote CS and sustainability. Businesses and individuals must use digital technologies responsibly and avoid using them for malicious purposes. The research emphasizes the importance of promoting sustainability in the DE. This includes optimizing data center operations, reducing energy consumption, and using renewable energy sources to power digital infrastructure. The research underscores the importance of education and awareness on CS and sustainable digitization. Businesses and individuals must be educated on the risks of cyber-attacks and data breaches, and on how to implement best practices to mitigate these risks. The practical implications of this research call for a collaborative and proactive approach to CS and sustainable digitization. By prioritizing CS, collaborating among stakeholders, promoting ethical use of technology, promoting sustainability, and investing in education and awareness, we can create a more secure and sustainable DE that will benefit everyone.

Limitations

Despite the numerous opportunities and challenges presented by the DE and CS, there are limitations to this research that must be acknowledged. Here are some potential limitations of this research: One of the main limitations of this research is the limited availability of data on CS incidents and their impact on the DE. The lack of comprehensive data can limit the accuracy and reliability of the findings. There is currently no consensus on the best practices for promoting CS and sustainable digitization. This can lead to differences in opinion and perspectives among stakeholders, which can limit the effectiveness of the proposed solutions. Implementing robust CS measures and promoting sustainable digitization can require significant resources and investments. Limited resources and budget constraints can limit the ability of businesses and governments to implement the proposed solutions. The DE and CS landscape is global, which can make it challenging to achieve consensus on policies, regulations, and best practices. Differences in political, cultural, and economic systems can limit the effectiveness of proposed solutions. These limitations highlight the need for further research and collaboration among stakeholders to address the challenges and opportunities presented by the DE and CS. By acknowledging and addressing these limitations, we can develop more comprehensive and effective solutions to promote a more secure and sustainable DE.

Future scope

The research on CS and the DE provides valuable insights into the challenges and opportunities of the digital age. However, there is still much to explore and discover in this field. Here are some potential areas of future research. The DE is constantly evolving, with new technologies such as AI, blockchain, and IoT gaining traction. Future research can explore the potential impact of these emerging technologies on CS and the DE. The increasing use of technology and digital infrastructure in critical sectors such as defense, energy, and finance has raised concerns about the potential for cyber-attacks to disrupt national security and international relations. Future research can explore the geopolitical risks of CS and the DE. CS is not just a technical issue, but also a

human issue. Future research can explore the role of human behavior, such as phishing and social engineering, in cyber-attacks and how to mitigate these risks. Future research can explore the intersection of CS and privacy, and how to balance the need for both in the digital age. Future research can explore the potential for CS and sustainable digitization to address climate change and promote environmental sustainability. The future of research on CS and the DE is vast and promising. By exploring these and other areas of research, we can continue to develop innovative solutions to promote a more secure, sustainable, and prosperous DE.

Acknowledgment: The authors are extremely thankful to all the individuals and organizations that contributed, encourage and provided valuable feedback throughout the research process. We are especially grateful to the experts and stakeholders who generously shared their knowledge, insights, and experiences, which greatly enriched this research. Lastly, our immense gratitude towards god for keeping us safe and healthy to complete this report on time.

Funding: This research didn't receive any funding from any agencies.

Conflict of Interest: No conflict of interest exists to declare.

Author's contribution: Surajit Mondal: Data collection and Draft preparation; Ashish Juneja: Investigation, Literature review, Methodology and Writing; Shankha Shubhra Goswami: Conceptualization, Validation, Supervision, Review and Editing.

Data availability: All the data are included in the article.

References

Abduvakhidov, A. M., Mannapova, E. T., & Akhmetshin, E. M. (2021). Digital Development of Education and Universities: Global Challenges of the DE. *International Journal of Instruction*, *14*(1), 743-760. https://doi.org/10.29333/iji.2021.14145a

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022). New survey reveals $2 trillion market opportunity for CS technology and service providers. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Alhayani, B., Abbas, S. T., Khutar, D. Z., & Mohammed, H. J. (2021). Best ways computation intelligent of face cyber-attacks. *Materials Today Proceedings*, 26-31. https://doi.org/10.1016/j.matpr.2021.02.557

Aliyev, A. G. (2022). Technologies Ensuring the Sustainability of Information Security of the Formation of the DE and their Perspective Development Directions. *International Journal of Information Engineering and Electron Business*, *14*(5), 1-14. https://www.mecs-press.org/ijieeb/ijieeb-v14-n5/IJIEEB-V14-N5-1.pdf

Barmuta, K. A., Akhmetshin, E. M., Andryushchenko, I. Y., Tagibova, A. A., Meshkova, G. V., & Zekiy, A. O. (2020). Problems of business processes transformation in the context of building DE. *Entrepreneurship and Sustainability Issues*, *8*(1), 945. https://doi.org/10.9770/jesi.2020.8.1(63)

Chandwani, N. (2023). DE has a New Global Captain – India. The Times of India. https://timesofindia.indiatimes.com/blogs/desires-of-a-modern-indian/digital-economy-has-a-new-global-captain-india/

Chen, Y., Kumara, E. K., & Sivakumar, V. (2021). Invesitigation of finance industry on risk awareness model and digital economic growth. *Annals of Operations Research*, 1-22. https://doi.org/10.1007/s10479-021-04287-7

Cisternelli, E. (2023). 7 cybersecurity frameworks that help reduce cyber risk. Bitsight. https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

Cusolito, A. P., Gévaudan, C., Lederman, D., & Wood, C. A. (2022). Three foundational pillars of the digital economy. World Bank Group E-Library. https://doi.org/10.1596/978-1-4648-1663-5_ch6

Goswami, S. S., & Behera, D. K. (2021). Solving material handling equipment selection problems in an industry with the help of entropy integrated COPRAS and ARAS MCDM techniques. *Process Integration and Optimization for Sustainability*, *5*(4), 947-973. https://doi.org/10.1007/s41660-021-00192-5

Goswami, S. S., Mohanty, S. K., & Behera, D. K. (2022). Selection of a green renewable energy source in India with the help of MEREC integrated PIV MCDM tool. *Materials Today: Proceedings*, *52*, 1153-1160. https://doi.org/10.1016/j.matpr.2021.11.019

Infosight. (2016). Vulnerability & cyber security assessment. https://www.infosightinc.com/solutions/advisory-services/vulnerability-assessment.php

Li, K., Kim, D. J., Lang, K. R., Kauffman, R. J., & Naldi, M. (2020). How should we understand the digital economy in Asia? Critical assessment and research agenda. *Electronic commerce research and applications*, *44*, 101004. https://doi.org/10.1016/j.elerap.2020.101004

Lis, P., & Mendel, J. (2019). Cyber-attacks on critical infrastructure: An economic perspective. *Economics and Business Review*, *5*(2), 24-47. https://doi.org/10.18559/ebr.2019.2.2

Litvinenko, V. S. (2020). DE as a factor in the technological development of the mineral sector. *Natural Resources Research*, *29*(3), 1521-1541. https://doi.org/10.1007/s11053-019-09568-4

Ma, Y., & Zhang, H. (2019). Development of the sharing economy in China: Challenges and lessons. In: Liu, K. C., Racherla, U. S. (eds), Innovation, Economic Development, and Intellectual Property in India and China. *ARCIALA Series on Intellectual Assets and Law in Asia. Springer, Singapore*. https://doi.org/10.1007/978-981-13-8102-7_20

Ministry of Electronics and IT. (2023). First meeting of G20 DE. https://pib.gov.in/PressReleasePage.aspx?PRID=1899538

Mittal, U. (2023). Detecting hate speech utilizing deep convolutional network and transformer models. *International Conference on Electrical, Electronics, Communication and Computers, IEEE*, pp. 1-4. https://doi.org/10.1109/ELEXCOM58812.2023.10370502

Mittal, U., & Panchal, D. (2023). AI-based evaluation system for supply chain vulnerabilities and resilience amidst external shocks: An empirical approach. *Reports in Mechanical Engineering*, *4*(1), 276-289. https://doi.org/10.31181/rme040122112023m

Mittal, U., Yang, H., Bukkapatnam, S. T., & Barajas, L. G. (2008). Dynamics and performance modeling of multi-stage manufacturing systems using nonlinear stochastic differential equations. *International Conference on Automation Science and Engineering*, *IEEE*, pp. 498-503. https://doi.org/10.1109/COASE.2008.4626530

Monteith, S., Glenn, T., Geddes, J., Severus, E., Whybrow, P. C., & Bauer, M. (2021). Internet of things issues related to psychiatry. *International Journal of Bipolar Disorders*, *9*(1), 1-9. https://doi.org/10.1186/s40345-020-00216-y

Mützel, S. (2021). Unlocking the payment experience: Future imaginaries in the case of digital payments. *New Media & Society*, *23*(2), 284-301. https://doi.org/10.1177/1461444820929317

Overvest, B., Straathoff, B., & Kiseleva, T. (2016). Cyber security risk assessment for the economy. *CPB Communication*. https://www.researchgate.net/publication/309807000_Cyber_Security_Risk_Assessment_for_the_Economy

Pan, W., Xie, T., Wang, Z., & Ma, L. (2022). DE: An innovation driver for total factor productivity. *Journal of Business Research*, *139*, 303-311. https://doi.org/10.1016/j.jbusres.2021.09.061

Popkova, E.G., & Gulzat, K. (2020). Contradiction of the DE: Public well-being vs. cyber threats. In: Popkova, E., Sergi, B. (eds), DE: Complexity and Variety vs. Rationality. *Lecture Notes in Networks and Systems*, Springer, Cham, vol 87, pp. 112-124. https://doi.org/10.1007/978-3-030-29586-8_13

Sahoo, S., & Goswami, S. (2024). Theoretical framework for assessing the economic and environmental impact of water pollution: A detailed study on sustainable development of India. *Journal of Future Sustainability*, 4(1), 23-34. http://dx.doi.org/10.5267/j.jfs.2024.1.003

Santos, R., Souza, D., Santo, W., Ribeiro, A., & Moreno, E. (2020). Machine learning algorithms to detect DDoS attacks in SDN. *Concurrency and Computation: Practice and Experience*, *32*(16), e5402. https://doi.org/10.1002/cpe.5402

Sharma, A. K. (2022). Opportunity to lead G20 digital economy agenda. The Economic Times. https://economictimes.indiatimes.com/news/economy/policy/opportunity-to-lead-g20-digital-economy-agenda/articleshow/96464683.cms?from=mdr

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of CS challenges, solutions and future directions. *Electronics*, *9*(11), 1864. https://doi.org/10.3390/electronics9111864

Sturgeon, T. J. (2021). Upgrading strategies for the digital economy. *Global strategy journal*, *11*(1), 34-57. https://doi.org/10.1002/gsj.1364

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795

UNCTAD. (2021). DE report. United Nations. https://unctad.org/system/files/official-document/der2021_en.pdf

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management*, *54*, 102120. https://doi.org/10.1016/j.ijinfomgt.2020.102120

Wilson, K. B., Karg, A., & Ghaderi, H. (2022). Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. *Business Horizons*, *65*(5), 657-670. https://doi.org/10.1016/j.bushor.2021.10.007

Xu, X. (2020). How do consumers in the sharing economy value sharing? Evidence from online reviews. *Decision Support Systems*, *128*, 113162. https://doi.org/10.1016/j.dss.2019.113162

Yenugula, M., Sahoo, S, K., & Goswami, S. S. (2023). Cloud computing in supply chain management: Exploring the relationship. *Management Science Letters*, *13*. 10.5267/j.msl.2023.4.003

Yenugula, M., Sahoo, S., & Goswami, S. (2024). Cloud computing for sustainable development: An analysis of environmental, economic and social benefits. *Journal of Future Sustainability*, *4*(1), 59-66. http://dx.doi.org/10.5267/j.jfs.2024.1.005

Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of CS risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society*, *19*(4), 446-462. https://doi.org/10.1108/JICES-03-2021-0035

Zhang, J., Zhao, W., Cheng, B., Li, A., Wang, Y., Yang, N., & Tian, Y. (2022). The impact of DE on the economic growth and the development strategies in the post-COVID-19 era: Evidence from countries along the "Belt and Road". *Frontiers in Public Health*, *10*, 856142. https://doi.org/10.3389/fpubh.2022.856142

Zhang, W., Zhao, S., Wan, X., & Yao, Y. (2021). Study on the effect of DE on high-quality economic development in China. *PloS one*, *16*(9), e0257365. https://doi.org/10.1371/journal.pone.0257365