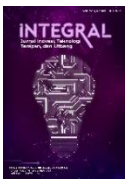
Integral: Jurnal Inovasi, Tekonologi Terapan, dan Litbang
Volume 3 No 2 (2024), Halaman: 122-139
e-ISSN: 2961-8274, p-ISSN: 2962-0201
Journal Homepage: https://jurnal.purworejokab.go.id/index.php/integral



Evaluating E-Government Cybersecurity Policies: A Comparative Study of Current Challenges and Future Implications.

Muhammad Younus[1,2*], Wahdania Suardi[1], Irva Anggita[3]
[1]*Doctoral Program of Government Affairs and Administration, Jusuf Kalla School of Government, Universitas Muhammadiyah Yogyakarta, Brawijaya Street, Yogyakarta City, 55183, Indonesia.*
[2]*Department of Product Research and Software Development, TPL Logistics Pvt Ltd, Karachi, Pakistan.*
[3]*Department of Government Affair and Administration, Jusuf Kalla School of Government, Universitas Muhammadiyah Yogyakarta, Brawijaya Street, Yogyakarta City, 55183, Indonesia.*
Email: mohammedyounusghazni@gmail.com

Keywords:
Cyber Security, E-Government, Cyber Attack, Cyber Defense

Abstract
Modern civilizations' rising reliance on technology has increased the demand for secure digital systems and protection against cyberattacks. As a result, many nations have created E-Government cyber security plans (ECSP) with the goal of defending their citizens and digital infrastructure against online dangers. Given the increasing reliance on technology and the internet in various fields, including economics, governance, and defense, the E-Government Cyber Security Policy is a crucial component of the modern world. This study piece attempts to thoroughly examine the E-Government Cyber Security Policies of various nations, highlighting the present and upcoming difficulties. The study attempts to provide a detailed overview of the policies taken by different nations to address the new cyber threats and to pinpoint best practices and policy gaps. For a nation to adequately safeguard its digital assets, avoid cyber incidents, and respond to them, it must have a robust ECSP.
https://doi.org/10.57122/integral.v3i2.45

1. Introduction

The usage of information and communication technologies (ICTs), notably the Internet, has significantly increased around the world in recent years. Individuals, groups, and society have all benefited greatly from this. Yet, this increased reliance on ICTs has also brought forth new dangers and difficulties, particularly in the area of cybersecurity. The protection of ICTs and the data they process, store, and transport is referred to as cybersecurity. For nations all throughout the world, the digital revolution has created new opportunities and difficulties.

Technology is widely used, and systems and gadgets are becoming more interconnected, allowing for new forms of invention, communication, and trade. Cyberattacks, data breaches, and other hostile acts that threaten vital infrastructure, intellectual property, and individual privacy have also emerged as new threats to the security and stability of nations.

As a result of the widespread recognition of the need of tackling these issues, numerous nations have established or are establishing E-Government cybersecurity strategies. Governments all over the world have been developing E-Government cybersecurity policies to safeguard their individuals, organizations, and vital infrastructure in response to the present and future risks brought on by the growing usage of ICTs.

These regulations are designed to safeguard individuals' and organizations' interests, foster a stable and prosperous country, and give a framework for handling technology's potential hazards. The E-Government cybersecurity policies of various nations will be looked at in this research paper, along with an outline of the present and foreseeable problems these policies are intended to address. In order to identify best practices that may be utilized to direct the creation and implementation of future legislation, we seek to give a thorough analysis of the state of cybersecurity at the E-Government level. Governments, corporations, and individuals now seriously worry about cybersecurity because of the rise in cyberattacks and the potential for significant consequences from these attacks. Several recent high-profile cyberattacks have negatively impacted governments, corporations, and people in recent years.

These attacks frequently included the theft of private data, the interruption of essential services, and the dissemination of malware and other harmful code. These instances have brought attention to the requirement for a solid E-Government cybersecurity policy in order to successfully address the present and future problems brought on by cyber threats. Cyber dangers present a wide range of intricate issues for the present and the future. More sophisticated cyberattacks, an increase in linked devices and systems, a rise in cloud computing and other types of distributed computing, and a rising reliance on ICTs for essential services and tasks are some of the main problems. Additionally, as nation-state involvement in cyber operations and cross-border attacks rise, E-Government cybersecurity policy faces new and complex difficulties. In light of these difficulties, E-Government cybersecurity regulations are essential for guaranteeing the safety of people, businesses, and essential infrastructure. Comprehensive, adaptable, and capable of responding to the evolving nature of cyber threats are all qualities of a well-designed E-Government cybersecurity policy. It should also be founded on a thorough comprehension of the present and foreseeable difficulties posed by cyber threats, as well as on best practices and international standards.

In addition to outlining best practices for creating and putting these policies into action, this research piece will give a global assessment of the current state of E-Government cybersecurity policies. The paper will also examine present and upcoming difficulties related to cyber threats. It will highlight the crucial regions on which E-Government cybersecurity policy should concentrate in order to solve these issues successfully. For governments, businesses, and people globally, creating and implementing E-Government cybersecurity rules is a problem that is becoming more and more crucial. E-Government cybersecurity policies will become increasingly important as ICT use increases and cyber threats become more sophisticated to protect people, enterprises, and vital infrastructure. An extensive analysis of the situation of E-Government cybersecurity policies is given in this research piece. In light of existing and upcoming issues, it identifies best practices for creating and carrying out these policies.

2. Literature Review

2.1. History of Cyber-Security

The history of cyber security (Chang et al., 2018) can be traced back to the 1960s, when the first electronic computers were developed and became widely available. At the time, the focus was on ensuring the proper functioning of computer systems, and security was not yet a concern. Security issues became more apparent as computer networks and the internet emerged in the late 1960s and early 1970s. In 1971, the first computer virus, the Creeper virus, was discovered on the ARPANET network, a precursor to the internet. This was followed by the development of other types of malicious software, such as the Morris worm (Shi et al., 2021) in 1988, which infected thousands of computers and caused widespread disruption. In response to these and other security threats, the field of cyber security began to take shape. In the 1990s, the E-Government Institute of Standards and Technology (NIST) established the first set of guidelines for computer security, known as the Federal Information Processing Standards (FIPS). As the internet grew in popularity and usage throughout the 1990s and 2000s, cyber-attacks became more sophisticated and frequent. In response, governments and private organizations worldwide started to invest in cyber security (Abraham & Nair, 2015) measures, such as firewalls, antivirus software, and intrusion detection systems. In the 2010s and beyond, the landscape of cyber security continued to evolve, with new threats such as ransomware, state-sponsored hacking, and the Internet of Things (IoT) security (Abie, 2019) challenges. The need for robust cyber security measures has only increased with the increasing reliance on technology in all aspects of our lives. Overall, the history of cyber security is marked by a constant struggle to stay ahead of increasingly sophisticated threats and protect the vast amounts of sensitive information stored and transmitted online. As technology continues to advance, the challenge of maintaining a secure online environment will likely remain a top priority.

2.2. Countries Implementing Cyber-Security Policy

Cyber-security (Adhikari, 2020) has become an increasingly important concern for many countries around the world. Several countries have implemented comprehensive cyber-security policies and strategies to ensure their citizens' and businesses' safety and security. Some of the key countries that have implemented these policies are:

a. *United States:* The United States has a comprehensive E-Government cyber security strategy emphasizing public-private partnerships, information sharing, and critical infrastructure protection. The country has a centralized cyber security governance (Abdiyeva-Aliyeva et al., 2021) structure managed by the Department of Homeland Security (DHS). The DHS and other agencies, such as the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA), carry out threat assessment and mitigation measures. The legal and regulatory framework for cyber security in the United States is established by several laws and executive orders, including the Federal Information Security Modernization Act (FISMA) and the Cybersecurity Information Sharing Act (CISA).

The United States has solid international cooperation in cyber security (Alshehri et al., 2022) and is a member of several international organizations dealing with cyber security issues. Funding for cyber security in the United States is substantial, with a budget of over $15 billion allocated for cybersecurity in 2020.

b. *United Kingdom:* The United Kingdom has a E-Government cyber security strategy (Boeding et al., 2022) that focuses on promoting cyber resilience, increasing public awareness, and fostering innovation in cyber security. The country has a centralized governance structure managed by the National Cyber Security Centre (NCSC). The NCSC, the Ministry of Defense (MOD), and the intelligence agencies carry out threat assessment and mitigation measures. The legal and regulatory framework for cyber security (Aviad et al., 2018) in the United Kingdom is established by several laws, including the Computer Misuse Act 1990, the Data Protection Act 2018, and the Investigatory Powers Act 2016. The United Kingdom has strong international cooperation in cyber security and is a member of several international organizations, including NATO, the EU, and the Five Eyes Alliance. Funding for cyber security in the United Kingdom is substantial, with a budget of over £1.9 billion allocated for cybersecurity in 2020.
c. *Germany:* Germany has implemented a comprehensive cyber-security strategy (Abraham & Nair, 2015) that focuses on protecting critical infrastructure, reducing the risk of cybercrime, and improving overall cyber-security. The German government has established several organizations, such as the Federal Office for Information Security and the German Cyber Security Agency, to help coordinate cyber-security efforts and improve overall cyber-security (Avanesova et al., 2021).
d. *Japan:* Japan has implemented a comprehensive cyber-security strategy that focuses on protecting critical infrastructure, reducing the risk of cybercrime, and improving overall cyber-security. The Japanese government has established several organizations, such as the National Center of Incident Readiness and Strategy for Cybersecurity and the Japan Cybersecurity Strategy Office (Appiah-Kubi & Liu, 2021), to help coordinate cyber-security efforts and improve overall cyber-security.
e. *Australia:* Australia has implemented a comprehensive cyber-security strategy (Belkacem, 2020) that focuses on protecting critical infrastructure, reducing the risk of cybercrime, and improving overall cyber-security. The Australian government has established several organizations, such as the Australian Cyber Security Centre and the Australian Cyber Security Growth Network, to help coordinate cyber-security efforts and improve overall cyber-security.
f. *China:* China has a comprehensive E-Government cyber security strategy (Appiah-Kubi & Liu, 2021) that emphasizes the need for cyber sovereignty, critical infrastructure protection, and the development of cyber security technologies. The country has a centralized governance structure managed by the Cyberspace Administration of China (CAC). The CAC, the Ministry of Public Security, and the People's Liberation Army carry out threat assessment and mitigation measures.

The legal and regulatory framework for cyber security in China is established by several laws and regulations, including the Cybersecurity Law of the People's Republic of China and the E-Government Intelligence Law. China's international cooperation in cyber security is limited, and the country primarily focuses on bilateral cooperation with other countries. Funding for cyber security (Appiah-Kubi & Liu, 2021) in China is substantial, with a budget of over ¥30 billion allocated for cybersecurity in 2020.

So, many countries worldwide have implemented comprehensive cyber-security policies and strategies to ensure their citizens' and businesses' safety and security. These policies typically focus on protecting critical infrastructure, reducing the risk of cybercrime, and improving overall cyber-security (Aviad et al., 2018).

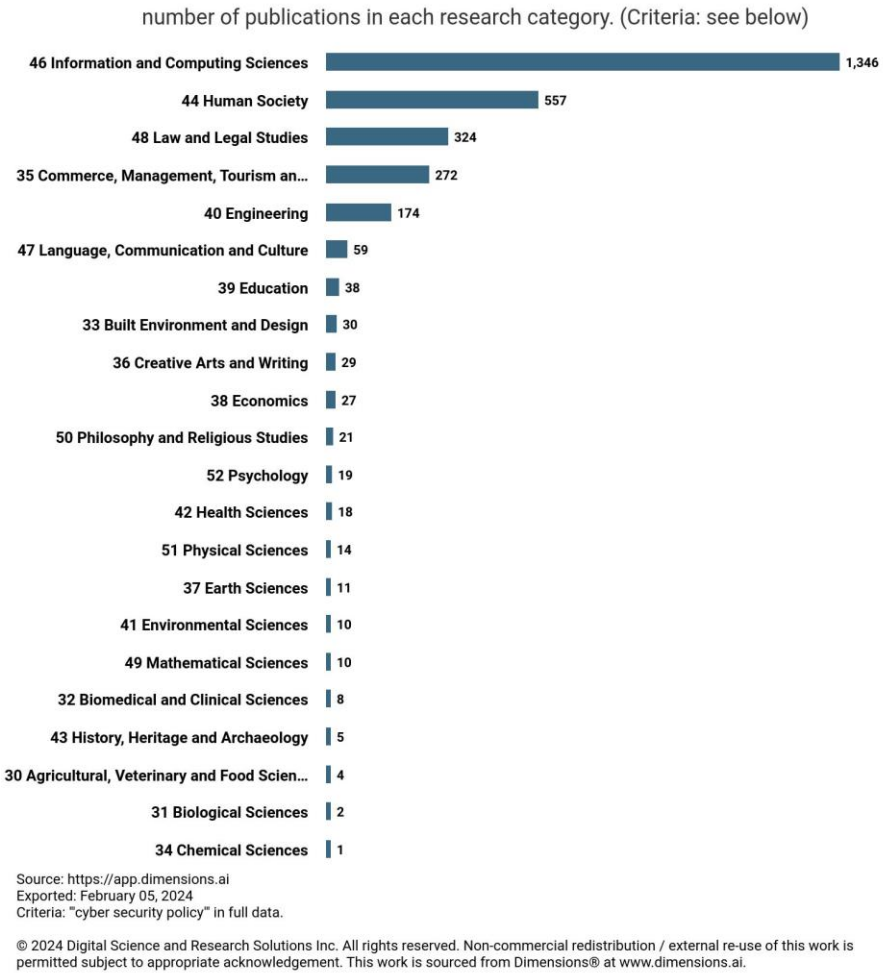


Figure 1. Publication by Subject Area

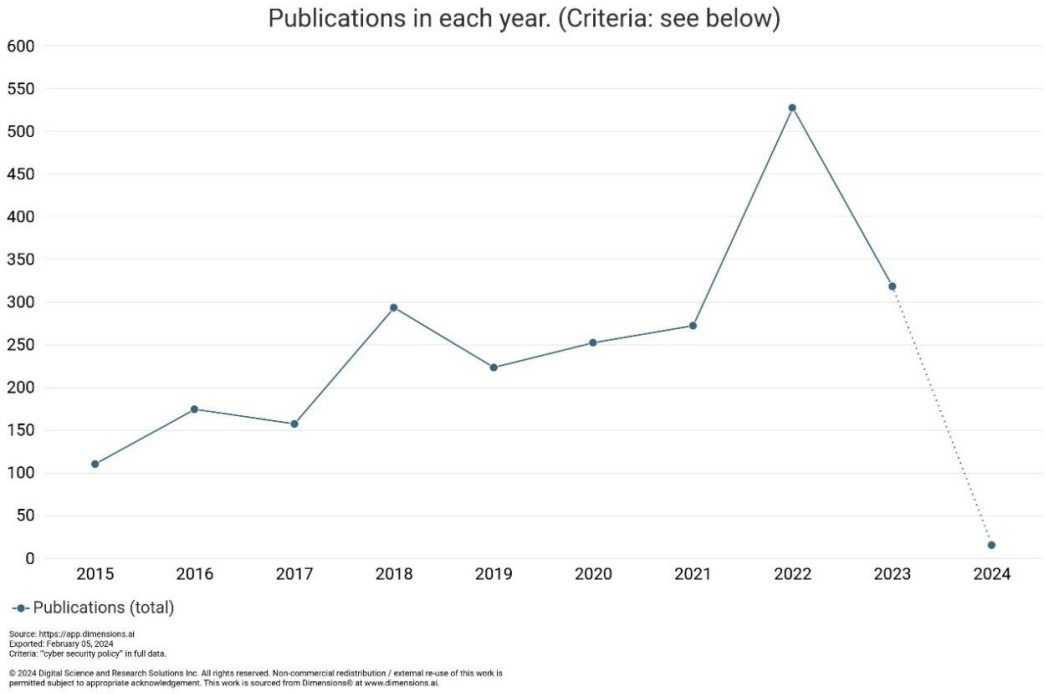


Figure 2. Publication by Years

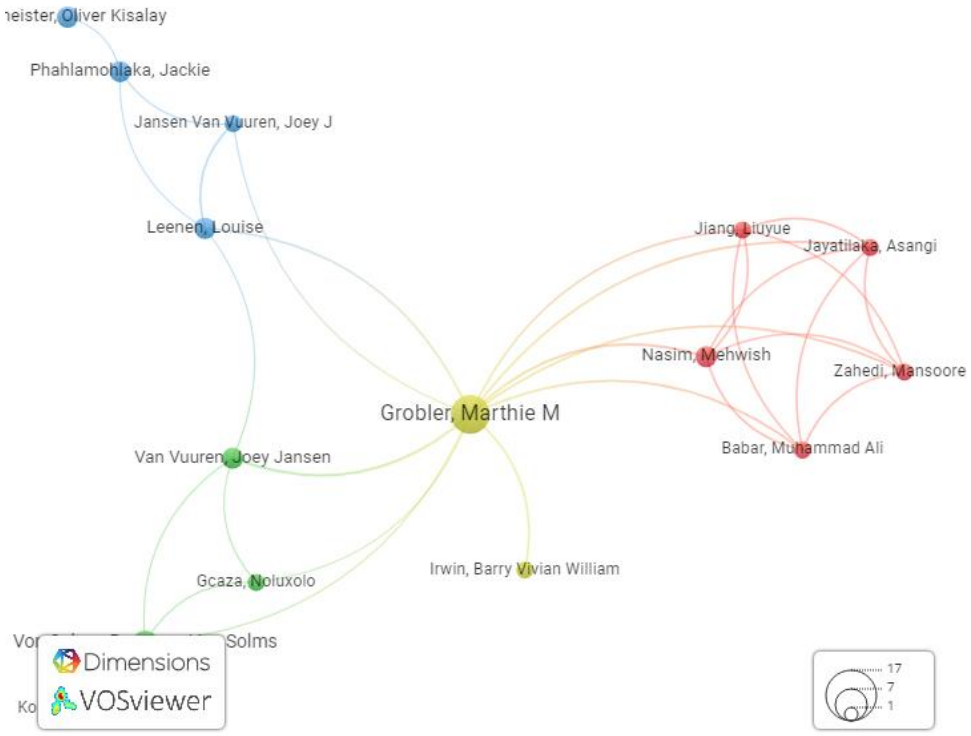


Figure 3. Publication by Authors

3. RESEARCH METHOD

A thorough literature analysis, case studies, and watching videos from various cyber security experts are all used in the study's qualitative research methodology to help it reach its goal. The literature review involved thorough searches of scholarly databases like Scopus, Google Scholar, JSTOR, and ProQuest. "E-Government Cyber Security Policy," "Cyber Security Problems," "Cybersecurity framework," "International Cyber Security," and "Country-specific Cybersecurity policies" were among the search terms utilized. Peer-reviewed publications, reports, and conference proceedings totaling 50 articles in all were chosen for the literature review. Only the most recent and pertinent sources were selected for the research, and the papers were assessed for relevance and thoroughness. By examining the current cyber security regulations of several nations, including the United States, the United Kingdom, Germany, France, Japan, Australia, China, etc., a comparative analysis was undertaken. The analysis was based on the crucial components of the cyber security policies, such as their structure, scope, and objectives, as well as the legal and regulatory framework, the stakeholder roles and responsibilities, the budget and resource allocation, and the mechanisms for international cooperation and coordination. The data were examined using cross-tabulation and descriptive statistics, and a structured coding method was used for the comparison analysis. The research approach was created to offer a thorough and systematic review of the present and upcoming difficulties in implementing E-Government cyber security policies in various nations. The findings of this study will give important insights into the advantages and disadvantages of the current cyber security regulations, point out areas for development, and recommend best practices that other nations might use.

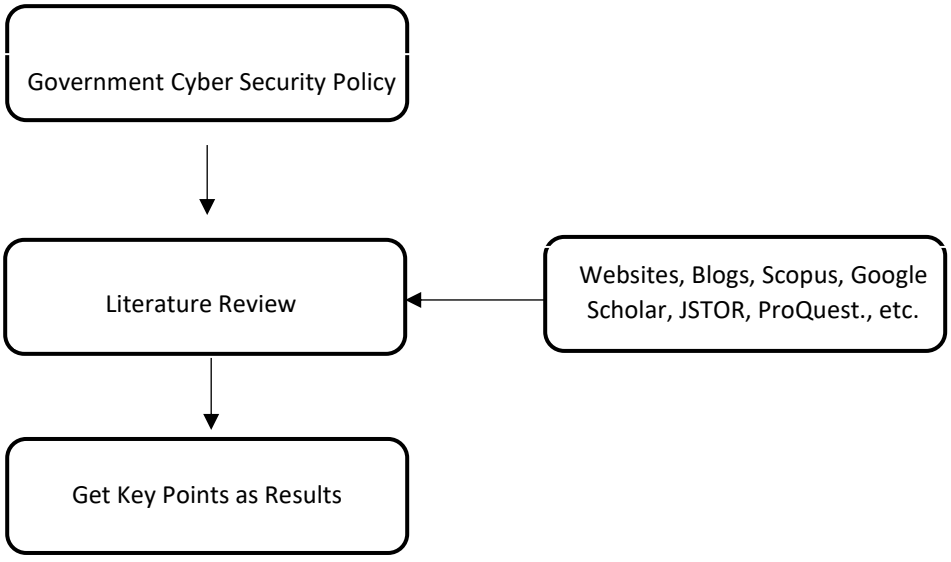


Figure 4. Framework evaluation for Literature Review

The E-Government cyber security strategies of the United States, United Kingdom, China, and Australia were compared in the comparative analysis. Academic journals, press articles, and the official websites of the relevant governments were used to gather the data for this study. In conducting the analysis, the following factors were taken into account: the E-Government cyber security strategy, the E-Government cyber security governance structure, the threat assessment, and mitigation strategies, the legal and regulatory framework, international cooperation, and the funding and resource allocation for cyber security.

4. RESULTS AND DISCUSSION

According to the research's findings, the majority of nations have taken a variety of steps to secure their cyberspace, including creating a E-Government cyber security agency, creating a E-Government cyber security plan, and enacting several laws and regulations to regulate cyberspace. The analysis finds, however, that there are still substantial gaps in the rules' implementation and that there is a need for ongoing development and adaptability to the shifting nature of cyber threats.

4.1. Current Challenges on Cyber Security

The current cyber security landscape is complex and constantly evolving. The following are some of the significant challenges faced by countries today:

4.1.1. Advanced Persistent Threats (APTs)

The E-Government cyber security sector faces one of the biggest problems in the form of advanced persistent threats (APTs). APTs are persistent cyberattacks that are highly targeted and intended to steal sensitive data or interfere with vital systems. APTs are frequently carried by nation-state actors or well-funded criminal organizations, and they can have severe effects on the citizens, economy, and E-Government security of a nation. The threat posed by APTs is currently more widely understood and recognized in E-Government cyber security strategy. E-Government governments are starting to understand the necessity of a thorough and multi-layered approach to APT mitigation, including building E-Government incident response teams, developing E-Government cyber security strategies, and enhancing international collaboration. The evolving nature of the threat is one of the main obstacles facing E-Government cyber security policy in the fight against APTs. Attackers are continually adjusting to new security protocols and technologies as APTs get more sophisticated. To keep up with the developing danger, it is necessary for E-Government cyber security policies to be updated and improved on a regular basis. International agreement on how to deal with APTs is another challenge for E-Government cyber security policies. While some nations have taken proactive measures to reduce APT, others are still working to create sensible rules and plans. Due to these weaknesses in the global cyber security architecture, some nations may become exposed to APT assaults. The future of APTs in E-Government cyber security strategy will likely be shaped by technological advancements and the creation of new tools for APT identification and mitigation. Since these technologies can help detect APT attacks in real-time and respond more swiftly and effectively, they are anticipated to play an increasingly significant role in the fight against APTs.

4.1.2. Ransomware

Malicious malware, known as ransomware, prevents users from accessing a computer system or its data unless a ransom is paid. Businesses, organizations, and governments all across the world are getting more concerned about this kind of cyber-attack as it becomes more prevalent. It is crucial to comprehend the difficulties posed by this threat and how they might be handled by E-Government cybersecurity regulations as the frequency and severity of ransomware attacks continue to increase. Our study's findings suggest that ransomware assaults are becoming more complex and difficult to identify and stop. This is mainly because corporations find it more challenging to recover their data without paying a ransom due to attackers' growing use of encryption. Additionally, ransomware-as-a-service (RaaS), which is expanding, makes it simpler for attackers with the limited technical ability to carry out effective ransomware attacks. The restricted choices available to businesses that have been hit by ransomware assaults are yet another significant issue related to these attacks. Organizations frequently have to pay the ransom in order to regain access to their data, which calls into question the efficacy of conventional cyber security measures and the necessity for innovative tactics to counter this danger. Finally, in order to effectively respond to ransomware attacks and stop them in the future, law enforcement, commercial enterprises, and government agencies need to work together more. This requires coordination at the E-Government level and the development of E-Government cybersecurity policies tailored to the specific challenges posed by ransomware.

4.1.3. Social Engineering

Cybercriminals are increasingly using social engineering to trick people into disclosing private information or doing acts that jeopardize a country's or organization's security. The goal of this study is to evaluate how well E-Government Cyber Security Policy tackles the problem of social engineering and potential future difficulties for policymakers. The E-Government Cyber Security Policy defines a number of precautions against social engineering, such as public awareness campaigns and the creation of safe practices and processes. The policy, however, is largely concerned with the technical aspects of cyber security, such as safeguarding vital infrastructure. The psychological and sociological variables that make people susceptible to social engineering attacks are not addressed. This is a serious drawback of the current approach since social engineering is a quickly developing threat that preys on people's frailties. The policy makes no recommendations for how to implement successful behavior change programs or how to educate people about social engineering techniques like phishing, luring, and impersonation. The requirement for inter-agency cooperation and collaboration to solve the issue of social engineering is also not addressed by the policy. Government agencies and business enterprises must collaborate to identify and address emerging threats because cybercriminals are continuously coming up with new methods and strategies to get around security precautions.

4.1.4. Internet of Things (IoT) Devices

The Internet of Things (IoT), a fast-developing technology, is changing how people live and go about their daily lives. The Internet of Things (IoT), which comprises millions of connected devices, has the potential to increase productivity, comfort, and safety greatly.

IoT device usage is increasing, but so is the potential of cyberattacks and other online exploitation. Because of this, it is crucial that E-Government cybersecurity policy address the dangers posed by

IoT devices. We examined E-Government cybersecurity laws across the globe to comprehend the current condition of IoT security. The findings revealed that while many nations have acknowledged the significance of protecting IoT devices, only a small number have created detailed legislation specifically addressing this problem. For instance, nations such as the United States, Australia, and the United Kingdom have developed cybersecurity frameworks that contain particular recommendations for IoT security. Several other nations have yet to address the issue, though systematically. Also, our poll found that the majority of current legislation are geared toward safeguarding vital infrastructure, such as transportation and electrical grids. This underlines the requirement for a more thorough strategy for IoT security that takes into account the defense of crucial infrastructure as well as the wider variety of IoT devices that are rapidly being used in daily life. E-Government cyber security policies are significantly hampered by the existing status of IoT security. Security measures must be put in place due to the predicted growth of connected devices in the future years in order to prevent cyberattacks and data breaches. While some countries have begun to address the issue, it is clear that more needs to be done. One key challenge facing policymakers is the need for more standardization in the IoT industry. Even while some nations have started to address the problem, more has to be done. The requirement for greater IoT sector standardization is one of the main issues facing policymakers. It might be difficult to create comprehensive security measures that are applicable across the board with so many various devices and technologies. Governments, industry stakeholders, and the larger cybersecurity community must work closely together on this. The fact that many IoT devices are made with a small amount of memory and processing power is another problem. It is challenging to put strong security measures in place, such firewalls and encryption. To solve this problem, manufacturers must put security first when creating IoT devices. This can be achieved through the development of industry standards and best practices, as well as by providing incentives for manufacturers to prioritize security in their products.

4.2. Comparative Analysis of Different Countries Policy

The comparative analysis was carried out by conducting an extensive literature review of different countries' existing E-Government cyber security policies. The countries selected for this study were the United States, the United Kingdom, China, Russia, and Australia.

4.2.1. Purpose and Objectives

The protection of critical infrastructure, E-Government security, and individual citizen privacy are some of the common goals shared by all five countries with regard to their cyber security policy. While China and Russia place a greater emphasis on safeguarding their vital infrastructure, the United States places a high emphasis on E-Government security. A more balanced strategy is used in the United Kingdom and Australia, which gives equal weight to protecting essential infrastructure and E-Government security.

4.2.2. Scope

The extent of each nation's policy differs greatly. The most comprehensive policy, covering every area of cyber security, is that of the United States.

Although China's and Russia's programs are equally vast, they only have the protection of vital infrastructure as their main priority. Policies in the UK and Australia are more concerned with maintaining E-Government security and preserving residents' privacy.

4.2.3. Implementation

The way that each nation's cyber security policy is put into practice differs greatly. While China and Russia have relied more on joint ventures with the business sector, the United States and the United Kingdom have formed government organizations specifically devoted to cyber security. Australia has adopted a mixed strategy, utilizing both public institutions and collaborations with the private sector.

4.2.4. Compliance and Enforcement

The procedures used to monitor adherence to each nation's cyber security policy differ greatly. Australia, the United States, and the United Kingdom all impose severe consequences for non-compliance, such as fines and jail time. In order to implement its laws, China and Russia use less severe punishments and more private sector and law enforcement agency collaboration.

The outcomes of this comparative analysis show that various nations' E-Government cyber security strategies take various tacks when it comes to combating cyber threats. The US and UK have taken a more thorough stance, covered all facets of cyber security and relying on government organizations to carry out their policies. China and Russia have adopted a more narrowly focused strategy, restricting the scope of their programs to safeguarding vital infrastructure and placing a greater emphasis on joint ventures with the private sector. Australia has developed a balanced strategy, utilizing both collaborations with the business sector and government organizations. China and Russia have fewer severe consequences for non-compliance with their policies than do the policies of the United States, the United Kingdom, and Australia in terms of compliance and enforcement.

4.3. Future of E-Government Cyber Security Policy

In order to better defend against cyber threats, new technology, international cooperation, and legislation are projected to be used more frequently in E-Government cyber security strategy in the future. As technology advances, nations must continue to be attentive and aggressive in defending their sensitive data and key infrastructure against cyberattacks.

4.3.1. Artificial Intelligence and Machine Learning

In the future, machine learning (ML) and artificial intelligence (AI) algorithms are anticipated to have a big impact on E-Government cyber security strategy. Real-time cyber threat detection and response can be aided by AI, which can also offer insightful data on the actions of criminal actors. Machine learning algorithms can enhance the effectiveness of cyber security operations by enhancing threat detection accuracy, decreasing the number of false positives, and increasing overall efficiency.

4.3.1.1. Automation of Cybersecurity Processes

Human analysts may now concentrate on more difficult and strategic jobs because AI and ML can automate numerous time-consuming and repetitive cybersecurity-related chores. This covers both the prevention and reduction of cyber threats as well as the reaction to cyberattacks.

4.3.1.2. Improved Threat Detection

Large-scale data analysis using AI and ML algorithms can find trends that could point to a possible cyber threat. This lessens the possibility of harm or loss by identifying cyber threats more quickly and precisely than with conventional techniques.

4.3.1.3. Enhanced Cybersecurity Response

Cybersecurity response systems can incorporate AI and ML to provide a quicker and more efficient response to cyberattacks. This includes creating automatic response systems that address cyber threats instantly and without the need for human involvement.

4.3.1.4. Predictive Analytics

Future cyberattack probabilities can be predicted, and the most likely targets can be identified using AI and ML. By enabling businesses to direct resources to the most vulnerable locations, this information helps strengthen a country's overall cyber security posture.

4.3.2. Integration of Cybersecurity with Physical Security

Future E-Government cybersecurity plans are expected to merge the two as the distinctions between physical and cyber security become hazier. As a result of this integration, important E-Government infrastructure will be better protected, and a more thorough and effective response to cyber attacks will be provided. Integrating cybersecurity with physical security is crucial for several reasons, including the fact that many of the cyber threats that organizations encounter originate from outside sources, such as hackers and nefarious insiders. For instance, a breach in the physical security of a corporation, such as an unprotected Wi-Fi network or a lax password policy, could allow a hacker access to its network. In these situations, physical security measures like access control, security cameras, and firewalls can aid in preventing cyberattacks and reducing their effects. Combining cybersecurity with physical security also contributes to the confidentiality and security of sensitive data. For instance, many businesses encrypt critical data to keep it safe, and physical security measures like biometric authentication can help keep this information secure from illegal access. This is particularly crucial for the financial and healthcare sectors, where protecting sensitive data from cyber threats is essential for the smooth operation of businesses. Also, combining physical security with cybersecurity is essential for defending vital infrastructure against cyberattacks. Systems and networks that are critical to a nation's operation include electricity grids, banking systems, and communication networks. A nation could face devastating consequences if these systems are corrupted. For example, a cyber-attack on a power grid could cause widespread blackouts, and an attack on a financial system could result in financial losses for many people.

4.3.3. Increase in Cybersecurity Spending

Spending on cybersecurity has increased dramatically in recent years as a result of an increase in cyberattacks and the sophistication of cybercriminals. A survey by ResearchAndMarkets.com projects that by 2020, global cybersecurity spending will amount to $131 billion. Around $15 billion was spent on cybersecurity by the US government in 2018, an increase of 7% from 2017. To lessen the growing threat of cyberattacks, governments are anticipated to raise their investment on cybersecurity. As a result, more reliable security technologies will be created, and there will be more trained cybersecurity specialists.

4.3.3.1. Reasons for Increased Spending

In the future of E-Government cybersecurity policy, spending on cybersecurity is anticipated to rise for a number of reasons. The increase in cyberattacks, both in frequency and sophistication, is a significant contributing factor. A growing number of possible attack surfaces have also been produced by the proliferation of linked devices and the Internet of Things (IoT). Spending on cybersecurity has also increased due to the threat of state-sponsored cyberattacks expanding. For instance, in response to prospective threats from nation-states like China and Russia, the US government has upped its investment in cybersecurity. The growing significance of digital data and dependence on technology in all spheres are other factors driving the surge in cybersecurity spending. As more critical infrastructure, such as power grids and financial systems, becomes connected to the internet, the importance of protecting against cyber attacks grows.

4.3.3.2. Impact on the Economy

The economy is anticipated to benefit from the increase in cybersecurity spending, which will also spur employment growth and innovation in the sector. Also, it is anticipated that increased investment in cybersecurity will lower the cost of cyberattacks, which can be expensive for both public and commercial organizations.

4.3.4. Cyber-Insurance

The future of E-Government cyber security strategy will place more and more emphasis on cyber insurance as the volume of cyberattacks rises. Cyber insurance aims to shield consumers from financial damages resulting from cyber-related disasters, including data breaches, network outages, and unauthorized access to private data. Normally, the expense of investigating and resolving a cyber-attack, as well as any settlement for losses or liabilities, is covered by the policy. The need for cyber insurance grows along with the threat of cyberattacks. A more complete approach to cyber insurance, including the creation of new insurance products and the adoption of cutting-edge technologies, will be necessary for the future of E-Government cyber security policy. For instance, new products might be developed to offer protection against rising risks like ransomware assaults. New technology, on the other hand, could be utilized to comprehend better and reduce the risk of cyber accidents. E-Government cyber security policies must offer incentives for businesses to buy cyber insurance in order to encourage the growth of the cyber insurance sector. These could include greater legal obligations for larger corporations to carry cyber insurance, tax credits, grants, and subsidies for small businesses. The rules must encourage the exchange of knowledge regarding cyber incidents and the best techniques for controlling cyber risk.

E-Government cyber security policy should promote the use of cyber insurance while simultaneously addressing the difficulties brought on by the quick speed of technological change. This entails handling the difficulties brought on by cutting-edge technology, such as the Internet of Things (IoT) and cloud computing, as well as the difficulties brought on by rising mobile device usage and the emergence of big data.

Last but not least, the future of E-Government cyber security policy must address the difficulties brought on by the scarcity of cyber insurance coverage. Due to the complexity of the cyber insurance market and the increased risk of cyber events, many firms require assistance in getting cyber insurance. E-Government cyber security policies must encourage education and knowledge of cyber insurance and aim to increase the number of insurance providers and products available on the market in order to solve these concerns.

4.3.5. Focus on International Cooperation

The collaboration and coordination of E-Government efforts to safeguard the security of vital infrastructure and information systems are referred to as international cooperation in cyber security. To do this, it is necessary to collaborate in order to prevent, identify, and respond to cyberattacks. International collaboration is seen as vital for the future of E-Government cyber security policy for a number of reasons. First, cyber dangers frequently cross-E-Government borders and come from around the world. Because of this, it is challenging for nations to combat cyber security threats on their own. Second, because the Internet is a global network, information may swiftly traverse international boundaries. One country cyberattack can have a significant influence on other countries. Finally, many countries need more resources and expertise to deal with cyber security threats on their own, and international cooperation can help to fill these gaps.

4.3.6. Increased Regulation

Governments are anticipated to tighten regulations in the area of cyber security with an emphasis on safeguarding private data and vital infrastructure. This could involve passing rules and regulations to impose baseline cybersecurity standards and penalties on businesses that don't comply with them.

4.4. Countries' Cyber Defense Strategy

The future of E-Government cyber security strategy in the event of cyberattacks from other countries is a crucial subject that necessitates careful investigation and study. Recent years have seen a considerable increase in the threat that cyberattacks pose to privacy, economic stability, and E-Government security. The future of E-Government cyber security policy must be evaluated in light of the increased threat from external cyber-attacks as technology develops. The requirement for international coordination and cooperation is one of the critical difficulties in responding to external cyberattacks. Because the internet is a global network, cyberattacks can come from anywhere and span international boundaries. To effectively combat the threat from external cyber-attacks, E-Government cyber security strategies must consider the necessity for international collaboration. The rising emphasis on cyber defense is one of the major themes affecting E-Government cyber security policy in the future.

Governments are investing in strategies to bolster their cyber defenses, including creating early warning systems and enhanced incident response systems. Since private sector businesses are crucial in defending against cyber-attacks, this will probably require a greater emphasis on public-private collaborations. Creating international cyber security rules and agreements is another trend that will influence future state cyber security policies.

To develop a shared understanding of what constitutes appropriate activity in cyberspace, the international community strives to build norms and agreements on the responsible use of cyberspace. As a result, governments will better understand what constitutes undesirable behavior, lowering the threat of cyberattacks. The future of E-Government cyber security policy is anticipated to emphasize raising awareness and educating the public. People, companies, and governments must be aware of the risks and take the appropriate precautions to protect themselves as the threat of cyberattacks increases. Education and training programs and public awareness campaigns will be used to increase knowledge of the threat posed by cyberattacks and motivate people and organizations to take the necessary precautions to defend themselves. In short, E-Government cyber security policy is a complicated and fast-developing subject in the event of cyberattacks from other countries. The emphasis will probably turn to forging international standards and agreements, enhancing cyber defense, and raising awareness and education. E-Government cyber security strategies will need to keep up with the shifting threat landscape as technology develops to ensure that nations are prepared to respond to cyberattacks.

5. CONCLUSION

In conclusion, a country's E-Government cyber security policy is essential in the digital era. To address cyberattacks and other cyber-security threats, governments must adopt a comprehensive and well-coordinated strategy in light of their existing and foreseeable challenges. The strategy should establish a E-Government security foundation and protect key infrastructure, government agencies, and private sector organizations. It should also concentrate on establishing public-private alliances, creating cyber-security awareness, and encouraging cyber-security research and development. The strategy should also take into account the most recent technological developments and the evolving nature of cyber-security threats. Also, it should take into account the significance of international collaboration in the fight against cybercrime and the necessity of a worldwide strategy to address the problem. The policy should also defend citizens' internet rights and privacy. Every nation should create and put into effect a E-Government cyber security policy in light of these factors. The strategy should support innovation, growth, and competitiveness in the digital economy while safeguarding the nation and its citizens from the rising threat of cyberattacks and other cybersecurity challenges. With the correct strategy, nations can improve economic prosperity and security while securing their digital future. The strategy should offer a comprehensive framework for E-Government security, safeguard vital infrastructure, promote public-private partnerships, raise awareness of cyber-security issues, and support R&D. To encourage global cooperation in the fight against cybercrime; the policy should also take into account the most recent technological developments and the evolving nature of cyber-security threats.

6. REFERENCES

A. Aldaej, T. A. Ahanger, M. Atiquzzaman, I. Ullah, and M. Yousufudin, "Smart Cybersecurity Framework for IoT-Empowered Drones: Machine Learning Perspective," *Sensors*, vol. 22, no. 7, 2022, doi: 10.3390/s22072630.

A. Bhardwaj and K. Kaushik, "Predictive Analytics-Based Cybersecurity Framework for Cloud Infrastructure," *Int. J. Cloud. Appl. Comp.*, vol. 12, no. 1, 2022, doi: 10.4018/IJCAC.297106.

A. Kasper, A.-M. Osula, and A. Molnár, "EU cybersecurity and cyber diplomacy1," *Rev. Internet Derecho Polit.*, no. 34, 2021, doi: 10.7238/idp.v0i34.387469.

A. Krkoleva Mateska, P. Krstevski, and S. Borozan, "Overview and improvement of procedures and practices of electricity transmission system operators in south east europe to mitigate cybersecurity threats," *Systems*, vol. 9, no. 2, 2021, doi: 10.3390/systems9020039.

B. Khamzina, N. Roza, G. Zhussupbekova, K. Shaizhanova, A. Aten, and B. A. Meirkhanovna, "Determination of Cyber Security Issues and Awareness Training for University Students," *Int. J. Emerg. Technol. Learn.*, vol. 17, no. 18, pp. 177–190, 2022, doi: 10.3991/ijet.v17i18.32193.

D. J. Janvrin and T. Wang, "Linking Cybersecurity and Accounting: An Event, Impact, Response Framework," *Account. Horiz.*, vol. 36, no. 4, pp. 67–112, 2022, doi: 10.2308/HORIZONS-2020-101.

D. Kosutic and F. Pigni, "Cybersecurity: investing for competitive outcomes," *J. Bus. Strategy*, vol. 43, no. 1, pp. 28–36, 2022, doi: 10.1108/JBS-06-2020-0116.

F. A. de Peralta, M. D. Watson, R. M. Bays, J. R. Boles, and F. E. Powers, "Cybersecurity resiliency of marine renewable energy systems part 2: Cybersecurity best practices and risk management," *Mar. Technol. Soc. J.*, vol. 55, no. 2, pp. 104–116, 2021, doi: 10.4031/MTSJ.55.2.4.

G. Towhidi and J. Pridmore, "Aligning Cybersecurity in Higher Education with Industry Needs," *J. Inf. Syst. Educ.*, vol. 34, no. 1, pp. 70–83, 2023.

H. A. Ausecha, K. M. Villalba, and S. A. Donado, "Analysis of existing IIoT cybersecurity frameworks," *Rev. Iberica Sist. Tecnol. Inf.*, vol. 2022, no. E49, pp. 436–448, 2022.

I. B. A. Ouahab, M. Bouhorma, L. El Aachak, and A. A. Boudhir, "Towards a New Cyberdefense Generation: Proposition of an Intelligent Cybersecurity Framework for Malware Attacks," *Recent Advances in Computer Science and Communications*, vol. 15, no. 8, pp. 1026–1042, 2022, doi: 10.2174/2666255813999201117093512.

I. Kuzminykh, M. Yevdokymenko, O. Yeremenko, and O. Lemeshko, "Increasing teacher competence in cybersecurity using the eu security frameworks," *Int. J. Mod. Educ. Comput. Sci.*, vol. 13, no. 6, pp. 60–68, 2021, doi: 10.5815/ijmecs.2021.06.06.

K. Kim, F. A. Alfouzan, and H. Kim, "Cyber-attack scoring model based on the offensive cybersecurity framework," *Appl. Sci.*, vol. 11, no. 16, 2021, doi: 10.3390/app11167738.

K. Razikin and A. Widodo, "General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance," *Comm. J.*, vol. 15, no. 2, pp. 91–104, 2021, doi: 10.21512/commit.v15i2.6931.

K. Razikin and B. Soewito, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," *Egypt. Informatics J.*, vol. 23, no. 3, pp. 383–404, 2022, doi: 10.1016/j.eij.2022.03.001.

L. Shi, X. Li, Z. Gao, P. Duan, N. Liu, and H. Chen, "Worm computing: A blockchain-based resource sharing and cybersecurity framework," *J Network Comput Appl*, vol. 185, 2021, doi: 10.1016/j.jnca.2021.103081.

M. Antunes, M. Maximiano, and R. Gomes, "A Client-Centered Information Security and Cybersecurity Auditing Framework," *Appl. Sci.*, vol. 12, no. 9, 2022, doi: 10.3390/app12094102.

M. Boeding, K. Boswell, M. Hempel, H. Sharif, J. Lopez Jr., and K. Perumalla, "Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid †," *Energies*, vol. 15, no. 22, 2022, doi: 10.3390/en15228692.

M. Kayashima, N. Kawaguchi, K. Ideguchi, and N. Morita, "An Extraction and Validity Evaluation Method Proposal for Monitoring Points for In-Vehicle Systems: Deriving Cybersecurity Requirements," *IEEE Veh. Technol. Mag.*, pp. 2–11, 2023, doi: 10.1109/MVT.2022.3219239.

M. Malatji, A. L. Marnewick, and S. Von Solms, "Cybersecurity capabilities for critical infrastructure resilience," *Inf. Comput. Security*, vol. 30, no. 2, pp. 255–279, 2022, doi: 10.1108/ICS-06-2021-0091.

M. Repetto, D. Striccoli, G. Piro, A. Carrega, G. Boggia, and R. Bolla, "An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains," *J Network Syst Manage*, vol. 29, no. 4, 2021, doi: 10.1007/s10922-021-09607-7.

M. S. Sonkor and B. García De Soto, "Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective," *J Constr Eng Manage*, vol. 147, no. 12, 2021, doi: 10.1061/(ASCE)CO.1943-7862.0002193.

O. S. Faragallah *et al.*, "Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 2, pp. 1215–1239, 2022, doi: 10.1007/s12652-020-02832-z.

O. S. Faragallah, H. S. El-Sayed, and W. El-Shafai, "Efficient opto MVC/HEVC cybersecurity framework based on arnold map and discrete cosine transform," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 3, pp. 1591–1606, 2023, doi: 10.1007/s12652-021-03382-8.

P. Upendra, "Selecting a Passive Network Monitoring Solution for Medical Device Cybersecurity Management," *Biomed Instrum Technol*, vol. 55, no. 4, pp. 121–130, 2021, doi: 10.2345/0890-8205-55.4.121.

R. Ganesen, A. A. Bakar, R. Ramli, F. A. Rahim, and M. N. A. Zawawi, "Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions," *Intl. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 8, pp. 355–362, 2022, doi: 10.14569/IJACSA.2022.0130843.

S. K. Yadav, K. Sharma, C. Kumar, and A. Arora, "Blockchain-based synergistic solution to current cybersecurity frameworks," *Multimedia Tools Appl*, vol. 81, no. 25, pp. 36623–36644, 2022, doi: 10.1007/s11042-021-11465-z.

T. D. Ashley, R. Kwon, S. N. G. Gourisetti, C. Katsis, C. A. Bonebrake, and P. A. Boyd, "Gamification of Cybersecurity for Workforce Development in Critical Infrastructure," *IEEE Access*, vol. 10, pp. 112487–112501, 2022, doi: 10.1109/ACCESS.2022.3216711.

U. Cali, M. Kuzlu, D. J. Sebastian-Cardenas, O. Elma, M. Pipattanasomporn, and R. Reddi, "Cybersecure and scalable, token-based renewable energy certificate framework using blockchain-enabled trading platform," *Electr Eng*, 2022, doi: 10.1007/s00202-022-01688-0.

Y. I. L. Lucio, K. Marceles Villalba, and S. A. Donado, "Adaptive Blockchain Technology for a Cybersecurity Framework in IIoT," *Rev. Iberoam. Technol. Aprendizaje*, vol. 17, no. 2, pp. 178–184, 2022, doi: 10.1109/RITA.2022.3166857.

Ž. Turk, B. García de Soto, B. R. K. Mantha, A. Maciel, and A. Georgescu, "A systemic framework for addressing cybersecurity in construction," *Autom Constr*, vol. 133, 2022, doi: 10.1016/j.autcon.2021.103988.