# The impact of cybersecurity on protecting the political, economic, and social foundations of the state

Sanaa Hikmat Hasan Mahmood*

Hai Al-Zahraa secondary school for girls, Directorate of studies and scientific research, Iraq
*Corresponding author, email: sanah.hikmat@uodiyala.edu.iq

**Article History**
Received: 11 March 2026
Revised: 25 April 2026
Accepted: 7 May 2026

**Keywords**
Cybersecurity
Economic Impact
Geopolitics
Globalization
Political Impact

**Abstract**
The rapid growth of Information and Communication Technologies (ICT) and cyberspace has created a new form of power known as cyber power. Unlike conventional power historically dominated by states, cyber power is decentralized and shared among governments, non-state actors, and individuals. This transformation has significantly influenced political and economic processes, enabling various actors to shape state structures and decision-making through cyberspace. Cyber power has become essential in achieving political and economic objectives, including improving social welfare and supporting sustainable development. However, increasing dependence on digital systems has also heightened vulnerability to cyberattacks. Cyberattacks pose serious threats due to their potential to cause economic damage, particularly in financial and banking sectors, while also weakening state power domestically and globally. In response, cybersecurity has emerged as a fundamental framework for protecting digital infrastructure. It encompasses strategies, technologies, and practices designed to safeguard systems, networks, and data from unauthorize nvd access, disruption, and destruction. Cybersecurity is no longer solely a technical issue but a shared responsibility among governments, institutions, and individuals. Addressing evolving cyber threats requires continuous capacity building, advanced technical capabilities, proactive risk management, public awareness, comprehensive training, and secure data management. Strengthening cybersecurity systems is therefore crucial for building resilient digital environments and ensuring sustainable political, economic, and social stability.

## 1. Introduction

The digitalization of modern societies has altered the very structure of security, power, and governance due to the rapid pace of digitalization (Xu et al., 2022). The spread of the Information and Communication Technologies (ICT), as well as the spread of cyberspace has offered unexplored possibilities in the development of economies, political engagement, and social growth. Nevertheless, such developments, in turn, have created complicated vulnerabilities, which put the states and institutions into a broad range of cyber threats that overcome the traditional geographical and political borders (IBM Security, 2025).

The concept of cybersecurity has become an important pillar of national security and sustainable development in this changing environment. Digital infrastructures are becoming more and more important to the operation of modern states, controlling vital services such as financial systems, healthcare, energy and governance. As a result, any interference with these systems, be it by cyberattacks, data breaches, and/or digital espionage can have significantly far-reaching impacts on political stability, economic performance, and social cohesion (World Economic Forum, 2024).

The very notion of power has been transformed in the digital age. Non-state actors such as individuals and organized groups have been empowered by cyber power to influence people in a manner similar to the way the states can. This change disputes the conventional concept of sovereignty and forces governments to rethink their policy of control and how to safeguard national interests in a highly interconnected and data-driven world (Accenture., 2023).

Moreover, the interdependence among states has been enhanced by globalization, increasing the benefits as well as dangers of digital connectivity (Luo., 2021). Along with making information exchange and economic integration faster and easier, cyberspace offers a platform to cybercrime, cyber warfare, and manipulation of information. Such dynamics have turned cybersecurity into a

doi: 10.62672/hucse.v3i2.65

ISSN: 3110-7648

multidimensional issue instead of being a technical one that involves political, economic, and social aspects (International Telecommunication Union, 2024).

Although there is increased knowledge on cybersecurity issues, most nations, especially the developing ones still experience great shortfalls in institutional capacity, legal frameworks and technical expertise. Such loopholes expose them to cyber threats and reduce their response capabilities. Hence, the challenge of cybersecurity in ensuring the safety of the basic elements of the state has turned out to be a burning research question (ENISA, 2023).

The research will explore the influence of cybersecurity on the security of political, economic, and social systems of the state. It discusses how cyber threats are changing, how cybersecurity can help to strengthen national resilience, and how the wider concept of state sovereignty and development in the digital age.

# 2. Theoretical Framework

## 2.1. Research Problem

Although the digital infrastructures are becoming more relied upon in governmental, economic, and social sectors, cyber threats are becoming more complex and more prevalent. Cyberattacks against critical systems in many states make them susceptible to huge losses and disruptions. This leads to one of the main issues about the efficiency of cybersecurity practices in terms of protecting the key state operations. Based on this, the following problem statement can be formulated:

> "How well does cybersecurity offer sufficient security to critical state systems and mitigate the related political and economic risks?"

This issue is indicative of the increasing disparagement between the accelerating technological change and the capacity of institutions to adequately secure their cyber space especially within developing settings where cybersecurity capacity remains low (Salman., 2021).

## 2.2. Research Hypothesis

The main hypothesis of this study is as follows is cybersecurity plays a major role in ensuring a system, network, and data protection against cyber threats and minimizes political and economic risks and makes the state infrastructure more resilient. This supposition is based on current cybersecurity models, which highlight the importance of active defense measures, threat mitigation, and ongoing system monitoring as key elements of national security (Suleiman., 2020; OECD., 2021).

## 2.3. Research Significance

The relevance of the current research is due to the growing significance of cybersecurity in safeguarding confidential information and maintaining the stability of the state institutions. In the digital era, information is a strategic resource, and their security is directly connected to the national sovereignty and economic sustainability. Cybersecurity contributes to:

a. Improve safe government and institutional data security against unauthorized access.
b. Lessening the vulnerabilities to computer crimes and cyber-spying.
c. Improving the confidence in the digital systems and economic growth.
d. Protecting the political systems against outside influence and interference.

Additionally, the research indicates the need to incorporate cybersecurity in the national policies, especially now that there is an increasing reliance on digital technologies in governance and economic life (Word Bank., 2021).

## 2.4. Key Definitions

a. Cybersecurity

Cybersecurity is a combination of technologies, processes and practices that are used to safeguard systems, networks and data against digital attacks (Sendjaja et al., 2024). The motives of these attacks are frequently to access, modify or destroy sensitive information or interfere with

normal operations. It includes preventive, detecting and correcting actions to guarantee confidentiality, integrity and availability of information systems (NIST., 2022).

b. Cyberspace

Cyberspace is a multifaceted environment with interconnected digital systems, such as hardware, software, networks, and consumers (Mallick & Nath, 2024). It is a physical and virtual space where information is generated, stored, and shared (Cisco., 2022).

c. Cybercrime

Cybercrime is any criminal activity performed with the use of computers or digital networks and usually entails unauthorized access, data theft, fraud or malfunction of the system (Goni., 2022). Such crimes need rules and tools of law to provide accountability (Palo Alto Networks., 2023).

d. Cyber Deterrence

Cyber deterrence is a set of strategies and actions that can be taken to prevent cyberattack, minimizing vulnerabilities and making attacks costlier (Shahid & Khan, 2022). It encompasses technical defenses, policy action, and international collaboration to curb taking advantage of the vulnerabilities in the systems (Kaspersk., 2023).

# 3. Cybersecurity

## 3.1. Evolution of Cybersecurity

The notion of cybersecurity has been changing with the advancement of computing technologies and networked systems. Cybersecurity was not a pressing issue in its early days because computer systems were not that accessible and computer networks did not exist. Nonetheless, as internet and digital networks have grown since the late twentieth century, cyber threats have grown more complex and extensive. Cybersecurity has become a strategic area that is closely interconnected with national security and the digital economy (Arab Monetary Fund., 2022).

Cybersecurity is no longer tied to the need to secure individual systems in the modern world but has been expanded to cover critical infrastructures, national security resources, and international digital ecosystems. The fact that technologies like cloud computing, artificial intelligence, and the Internet of Things (IoT) are becoming more interconnected has further increased the attack surface and, therefore, cybersecurity is becoming an ever-changing discipline that needs dynamic and offensive approaches (Brookings Institution., 2021).

## 3.2. The longterm Importance of Cybersecurity

The increased dependency on digital systems to run sensitive information and critical processes has seen cybersecurity become a requirement to modern states. Data storage and processing systems are very essential to governmental, financial, healthcare and military institutions, and most of them hold very sensitive information. Any unauthorized access to such data may lead to extreme political, economic, and social impacts (Deloitte., 2023). Three fundamental principles could be used to comprehend the significance of cybersecurity:

a. Confidentiality: This involves having sensitive information available to the authorized parties.
b. Integrity: There must be accuracy and consistency of data.
c. Availability: Ensuring systems and data are available when required.

These are the principles of the contemporary cybersecurity models and they are crucial in preserving trust in online systems and providing continuity of the operations (McKinsey & Company., 2022). Additionally, cybersecurity is essential in building national resilience by:

a. Securing important infrastructure against disruption.
b. Improving economic stability by means of safe online transactions.
c. Supporting digital transformation and innovation.
d. Improve and increase the public confidence in electronic systems of governance.

Recent research points out that those countries that are capable of effective cybersecurity are more in a position to experience sustainable development and geopolitical stability in the cyber era (INTERPOL., 2022).

## 3.3. Principles of Cybersecurity.

Cybersecurity is a broad field of functional areas that are targeted at securing digital spaces. These functions include:

a. Network Security This includes safeguarding computer networks against unauthorized access, intrusions, and malicious attacks. It incorporates intrusion detection systems, firewalls and encryption protocols.
b. Application Security The security measures should be included at the design stage and not after the deployment (European Central Bank., 2022).
c. Information Security This role is to ensure confidentiality, integrity, and availability of data when stored and when they are transferred over digital networks.
d. Operational Security Operational security incorporates policies and procedures that govern the manner data is processed, accessed and stored along with user permissions and access control settings.
e. Disaster Recovery and Business sustainability. Organizations should be ready to counter a cyber incident with recovery measures that can recover systems and operations in an effective manner. Business continuity planning is a plan that guarantees the organizations the ability to continue with critical operations even in times of discontinuity (International Monetary Fund., 2022).

## 3.4. Cyber Threat Landscape

This has seen the global cyber threat environment grow both in magnitude and complexity. The level of cyberattacks has increased and is more targeted and financially driven. The recent world reports indicate that billions of records are being exposed each year through data breaches, including in fields like healthcare, finance, and the government services (Microsoft., 2023). There are several types of cyber threats:

a. Cybercrime: attacks by individuals or organized groups of people with financial motivations.
b. Cyber espionage: Attacks to gather sensitive political or economic information.
c. Cyber terrorism: Tactics that aim at instilling fear and destabilizing the society.
d. Malware attacks: Virus, ransomware, spyware, and botnets.

Malware is the most widespread and frequent type of cyber threat that can be disseminated by way of phishing email or malicious downloads. Such attacks can be employed in stealing data, extorting finances, or disrupting the system (Google Cloud, 2024).

## 3.5. Mechanisms of Cyber Attacks

Cyberattacks refer to intentional attempts to disrupt, modify, or steal data by disrupting information systems. These attacks can be directed at individuals, organizations or even states and can be perpetrated by state actors, criminal groups or even by independent hackers. Effective cyberattacks tend to take advantage of System vulnerabilities, including old software, lax security settings, or user ignorance. Human factors are considered to be one of the most significant vulnerabilities, since attackers often use social engineering methods to obtain unauthorized access (PwC, 2023). Cyberattacks can be classified into:

a. Active attacks: e.g. denial-of-service (DoS) attacks and manipulation of the system.
b. Passive attacks: These include surveillance, interception of data, and eavesdropping.

The growing popularity of cyber warfare among states underscores the strategic aspect of cyberattacks when digital means are used to deliver military or political goals without actual physical engagement (United Nations, 2021).

### 3.6. Achieving Cybersecurity

Effective cybersecurity can only be achieved through a multi-layered approach that integrates human, technical and organizational aspects. Key practices include:

a. With reliable and safe sites (HTTPS protocols)
b. Not falling prey to phishing emails and shaddy links.
c. Regularly updating systems and software
d. Having secure data backups.

Moreover, to improve cybersecurity, it is necessary:

a. Training of cybersecurity strategies nationally.
b. Investing in capacity building and training
c. Enhance legal and regulatory systems.
d. The work on the awareness and digital literacy.

All these measures help minimize vulnerabilities and enhance the capability to effectively respond to cyber threats (NATO Cooperative Cyber Defence Centre of Excellence., 2022).

## 4. Geopolitics, Cybersecurity, Its Political and Economic Implications

The cyberspace has completely changed the conventional concept of geopolitics. Cyberspace breaks through geographical limits, unlike the traditional geopolitical arenas that are established based on geography, cyberspace provides a platform that competition of power and strategic influence (Riordan., 2018; Lobastova., 2020). This has altered the balance of power among states, with the power to control information and the digital infrastructure becoming a decisive factor of national power (Brookings Institution., 2021).

In the digital era, no longer is geography the dice roller or the source of conflict. States are now able to infiltrate the informational and technological systems of one another without having to physically confront each other (Joyner & Lotrionte, 2017). This has resulted in the new geopolitical aspect where cyberspace is a strategic space alongside the land, sea, air and space (Deloitte., 2023).

Moreover, the emergence of cyber space has empowered non-state actors such as corporations, hacker groups and transnational organizations to have a major role in international relations. This leaves the state no longer as the exclusive influence in the formation of geopolitical dynamics and creates another layer of complexity in the process of dealing with security and sovereignty (McKinsey & Company., 2022).

### 4.1. Cybersecurity Globalization Political Implications.

Globalization has enhanced the penetration of digital technologies in the political sphere, changing the essence of governance, intelligence and national security. National security has grown to encompass more than the traditional military threats of national security to cyber threats to information systems, public opinion, and institutional stability (Alguliyev,et al., 2021; Ripsman & Paul, 2005).

In this interconnected environment, cybersecurity is essential towards defending state sovereignty. Cyberattacks, such as cyber espionage and information warfare, are able to affect political processes, such as elections, policymaking, and public discourse. This has seen governments put up dedicated cyber units and digital intelligence systems to combat such threats (INTERPOL., 2022).

In addition, the growing access to information by the Internet has given citizens more power to be more involved in the political processes. Though this strengthens the democratic process, it also opens up political systems to threats of misinformation, manipulation, and online propaganda (Microsoft., 2023).

In spite of these issues, cybersecurity does not destroy the sovereignty of states but only transforms it. States must assume new roles and responsibilities such as controlling cyberspace, security of digital infrastructures and integrity of information flows. This metamorphosis underscores the changing sovereignty in the virtual era (OECD., 2021).

## 4.2. Nationwide Security and Cyberspace.

Cybersecurity is now a major element in the national security policies across the globe. Cyber warfare has brought forth a different type of warfare that is no longer based on the use of a conventional military force but rather on digital systems and critical infrastructures. Cyber threats are a great threat to national security in that:

a. Negatively impact essential services such as energy, healthcare, and finance
b. Hacking sensitive governmental information.
c. Weakening the faith of people in institutions.
d. Weakening economic stability

This has led to redefinition of national security structures of many states to include cybersecurity as a central component. This involves building up defensive and offensive cyber capabilities, investing in technological innovation, and increasing international collaboration (INTERPOL., 2022). The increasing role of cybersecurity underscores the shift in the paradigms of security to multidimensional and more sophisticated systems that deal with both physical and cybersecurity risks.

## 4.3. The Cybersecurity and the State Power

The concept of power has changed with the involvement of technological advancements and the birth of cyberspace. The cyber power has emerged as an important determinant of the world position of states. Economically, cybersecurity promotes development by facilitating the security of digital transactions, promoting e-commerce, and generating new jobs. Safe online spaces promote investment and innovation that will lead to the general economic growth (Word Bank., 2021).

Politically, states use cyberspace to increase their power, control of information and governance. Control and protection of the digital infrastructures have turned out to be a strength of a nation. Those countries which have invested in cybersecurity technologies and research are more likely to compete on the global scale and have strategic advantages (European Central Bank., 2022).

Also, cyber power has decentralized power among actors in the international system, enabling technologically advanced countries to have a major influence in international politics, as well as non-state actors. The reallocation of power is a challenge to old power structures and a new competition and cooperation.

## 4.4. Global Cybersecurity Index (GCI)

The Global Cybersecurity Index (GCI) was created as a universal instrument to measure the readiness of nations in dealing with cyber threats. The GCI assesses the countries on the five major dimensions: Legal measures; Technical measures; Organizational measures; Capacity building; and Cooperation. These indicators give a comprehensive picture of national cybersecurity capabilities and preparedness to confront the cyberattacks (International Telecommunication Union, 2024).

According to recent GCI reports, there are considerable differences between nations in regard to cybersecurity maturity. The developed countries are more likely to be on the top of the list because of the well-developed infrastructure, strong legal regulations, and significant investment in cybersecurity. On the contrary, most of the developing nations struggle with the issues of resource scarcity, ineffective regulatory and legal frameworks.

Over the past years, some countries in the Arab region have made strides in this regard as they have been ranked highly as a result of strategic investment in cybersecurity. Nonetheless, the situation in other countries remains subpar and underpins the necessity to improve regional collaboration and the formulation of policies to increase cybersecurity resilience (Arab Monetary Fund., 2022).

The next part provides empirical evidence to prove the analysis of cybersecurity inequities and economic effects in the world. Figure 1 shown a cybersecurity maturity distribution by tier.

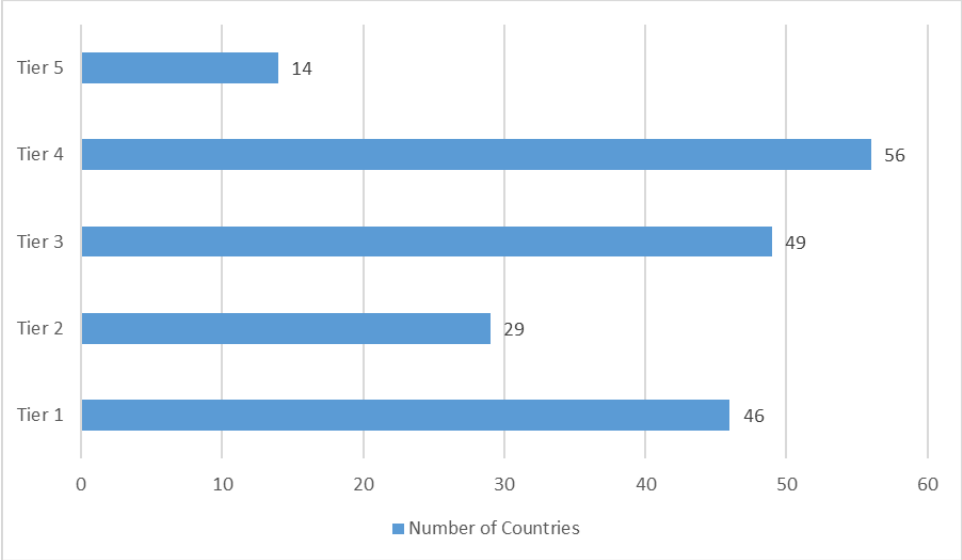


**Figure 1. Cybersecurity Maturity Distribution by Tier (Globally) (2024).**

Figure 1 shows the distribution of countries in the world, according to levels of cybersecurity maturity based on the Global Cybersecurity Index (GCI) 2024. The 2024 index is based on a tier-based system as opposed to the ranking system in the previous versions, with Tier 1 (role-modelling) on the one end and Tier 5 (building) on the other end. The findings indicate that there are few countries (46) in the top tier, with most countries falling in Tier 3 and Tier 4, which means that countries are still developing their cybersecurity capabilities. This distribution underscores the unequal cybersecurity preparedness of the whole world and shows that the legal, technical, and organizational structures should be further invested in (IBM Security, 2025). Distribution of cybersecurity tiers by region (2024) on the globe can be seen in Figure 2.

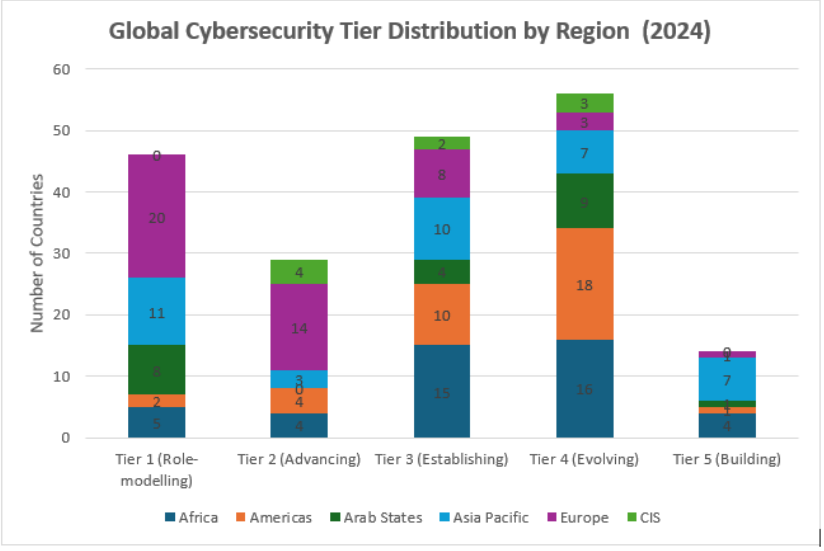


**Figure 2. Distribution of Cybersecurity Tiers by Region (2024) on the globe**

Figure 2 shows the distribution of countries by region based on the Global Cybersecurity Index (2024) into various levels of cybersecurity maturity. The findings indicate that the most countries of high performance (Tier 1) are located in Europe, Asia-Pacific, and the Arab States, with many countries in Africa and developing regions being in Tier 3 and Tier 4. This distribution indicates the disparities in cybersecurity preparedness globally and the variation in the institutional capacity, technical infrastructure, and policy formulation across the regions.

This proves the fact that the development of cybersecurity is not a worldwide affair, and there are apparent gaps in the regions (World Economic Forum, 2024). Global data breach cost (in USD Millions) can be seen in Figure 3.

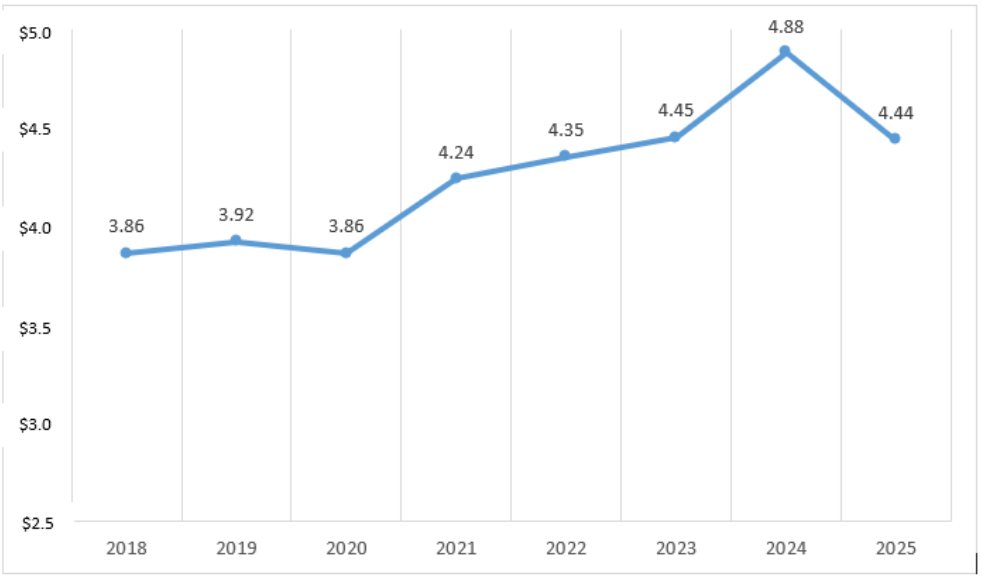


**Figure 3. Global data breach cost (in USD Millions)**

Figure 3 demonstrates the development of the cost of data breach (in USD millions) in the world between 2018 and 2025. The data indicate that the costs will continue to rise steadily until 2024 and then decrease slightly to USD 4.44 million in 2025, which is mainly caused by better detection and response mechanisms through AI and automation (World Economic Forum, 2024). Table 1 shown a

**Table 1. Average cost of Data Breaches by Country/Region (2024-2025) (World Economic Forum, 2024)**

| Rank | Country | Trend | 2025 Cost (USD M) | 2024 Cost (USD M) |
|---|---|---|---|---|
| 1 | United States | ↑ | $10.22 | $9.36 |
| 2 | Middle East | ↓ | $7.29 | $8.75 |
| 3 | Benelux | ↑ | $6.24 | $5.90 |
| 4 | Canada | ↑ | $4.84 | $4.66 |
| 5 | United Kingdom | ↓ | $4.14 | $4.53 |
| 6 | Germany | ↓ | $4.03 | $5.31 |
| 7 | Latin America | ↓ | $3.81 | $4.16 |
| 8 | France | ↓ | $3.73 | $4.17 |
| 9 | ASEAN | ↑ | $3.67 | $3.23 |
| 10 | Japan | ↓ | $3.65 | $4.19 |
| 11 | Italy | ↓ | $3.44 | $4.73 |
| 12 | South Korea | ↓ | $2.84 | $3.62 |
| 13 | Australia | ↓ | $2.55 | $2.78 |
| 14 | India | ↑ | $2.51 | $2.35 |
| 15 | South Africa | ↓ | $2.37 | $2.78 |
| 16 | Brazil | ↓ | $1.22 | $1.36 |

The difference in costs of data breach in different countries is indicative of structural economic and regulatory disparities. As an example, the average cost was highest in the United States, recording USD 10.22 million, which is much higher than the average in the rest of the world, as a result of more strict regulatory settings and greater costs of detection. Table 2 shown a effects of AI adoption on the cost of data breach.

**Table 2. Effects of AI Adoption on the cost of data breach (World Economic Forum, 2024).**

| AI Usage | Cost |
|---|---|
| No AI | 5.52M |
| With AI | 3.62M |

AI and automation can greatly mitigate the economic consequences of cybersecurity attacks. Companies that heavily used AI incurred an average breach cost of USD 3.62 million versus USD 5.52 million to companies that did not, demonstrating a cost savings of about USD 1.9 million. Figure 4 shown a cost components of data breaches.

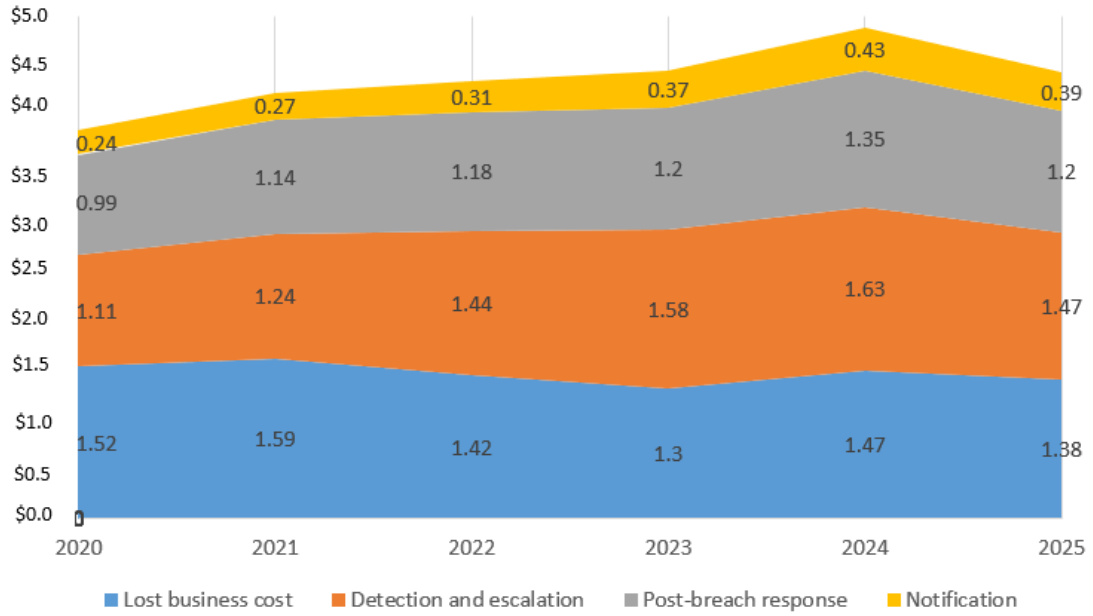


**Figure 4. Cost Components of Data Breaches**

Data breach has various cost elements that affect the economy, such as lost business, detection and escalation, cost of post-breach response, and cost of notification. Of these, the lost business costs, including reputational damage and loss of customers, are a large part of the overall economic impact. Table 3 shown a leading countries on cybersecurity readiness top tier.

**Table 3. Leading Countries on Cybersecurity Readiness Top Tier (International Telecommunication Union, 2024).**

| Country | Cybersecurity Tier | Score (Approx.) | Status |
|---|---|---|---|
| United States | Tier 1 | 100 | Global leader |
| United Kingdom | Tier 1 | 99.5 | Advanced framework |
| Saudi Arabia | Tier 1 | 99.2 | Leading Arab country |
| Estonia | Tier 1 | 99.0 | Digital governance leader |
| South Korea | Tier 1 | 98.5 | Strong technical capacity |
| Singapore | Tier 1 | 98.0 | Institutional strength |
| Spain | Tier 1 | 97.5 | Strong cooperation |
| Malaysia | Tier 1 | 97.0 | Rapid development |
| Canada | Tier 1 | 96.5 | High resilience |
| France | Tier 1 | 96.0 | Balanced performance |

Presents the leading countries in cybersecurity readiness based on the Global Cybersecurity Index (2024). In contrast to the previous editions, which were based on ranking systems, the most recent methodology divides countries into five levels based on their degree of cybersecurity commitment. The nations mentioned in this table belong to Tier 1, which is the most mature cybersecurity. The performance of these countries is high in the areas of legal, technical, organizational, capacity-building, and cooperation, which are indicative of mature national cybersecurity systems and great resilience to cyber threats. It is important to note that the GCI 2024 does not provide a strict ranking but rather categorizes countries into performance tiers. Table 4 shown a cybersecurity maturity level of arab countries.

**Table 4. Cybersecurity Maturity Levels of Arab Countries (International Telecommunication Union, 2024)**

| Country | Tier (GCI 2024) | Cybersecurity Status |
|---|---|---|
| Saudi Arabia | Tier 1 | Global leader |
| United Arab Emirates | Tier 1 | Advanced capabilities |
| Oman | Tier 2 | Strong performance |
| Qatar | Tier 2 | Developing rapidly |
| Egypt | Tier 1 | High maturity (recent improvement) |
| Jordan | Tier 3 | Moderate development |
| Bahrain | Tier 2 | Established framework |
| Tunisia | Tier 3 | Developing |
| Morocco | Tier 3 | Developing |
| Kuwait | Tier 3 | Moderate |
| Algeria | Tier 3 | Moderate |
| Iraq | Tier 4 | Evolving |
| Lebanon | Tier 4 | Limited progress |
| Sudan | Tier 4–5 | Low capacity |
| Yemen | Tier 5 | Early stage |

Table 4 shows the cybersecurity maturity of Arab countries, according to the Global Cybersecurity Index (2024). The present-day methodology takes countries into five levels indicating the overall commitment of the country to cybersecurity, rather than previous versions that used numerical ranking and scorecards on pillars. The findings demonstrate that Saudi Arabia, the United Arab Emirates, and Egypt are located at Tier 1, which means that these countries have high levels of cybersecurity. Conversely, a country like Iraq, Lebanon, and Yemen is ranked in the bottom rungs, which indicates a continuous struggle to build cybersecurity infrastructure, laws, and institutional capacity.

According to the Global Cybersecurity Index (2024), Iraq belongs to Tier 4, which is characterized by the developing cybersecurity framework with the notable gaps in institutional capacity, enforcement of laws and regulations, and technical infrastructure in comparison to the major countries of the region. The global distribution of the cybersecurity maturity level according to the Global Cybersecurity Index (2024) is shown in Figure 5.

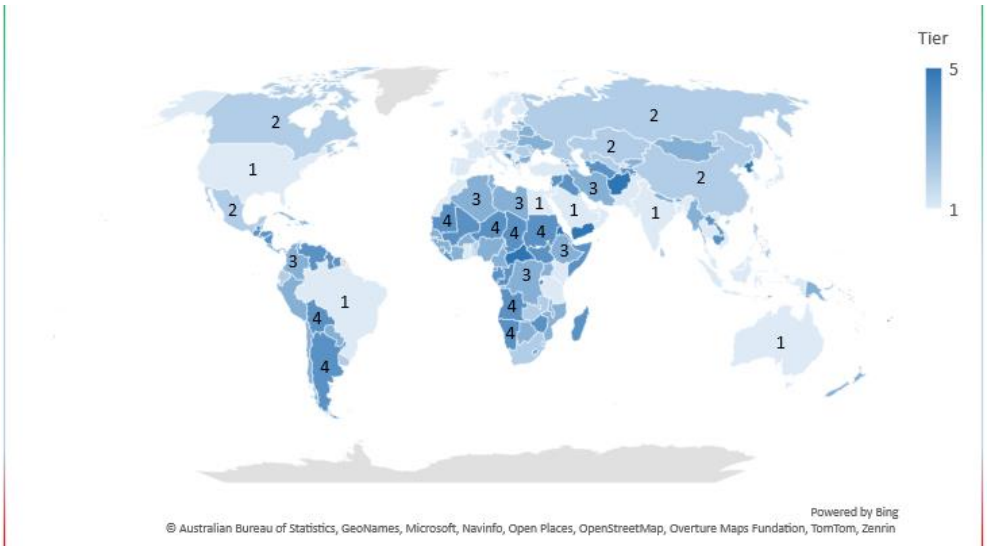


**Figure 5. World Cybersecurity Maturity Distribution by Tier (2024)**

There are five levels of commitment to cybersecurity, Tier 1 (role-modelling) and Tier 5 (building), to describe the extent of commitment of countries to cybersecurity in legal, technical, organizational, capacity development and cooperation dimensions. The map indicates that the most successful countries are clustered in North America, Europe and parts of Asia and Middle East, whereas most of the countries are in Africa and developing regions where they have been clustered

into lower categories. This distribution underlines the existing worldwide digital gap in cybersecurity preparedness and the necessity to invest more in cybersecurity capacities.

# 5. Economic Impacts of Cybersecurity

## 5.1. Global Economic Impact

Cybersecurity has strong economic consequences, both with regard to avoiding losses and facilitating growth. Cyberattacks may cause significant financial losses in the banking, healthcare, industry, and government services sectors. Such effects are reflected in both direct and indirect economic losses. Direct losses will consist of financial theft, ransom, and incident response and system recovery costs. Indirect losses, in contrast, are reputational losses, disruption of the operations, regulatory fines, and loss of customer trust.

The latest empirical results suggest that the average cost of a data breach worldwide is around USD 4.44 million in 2025, which is an indication that cyber attacks are increasingly complex and expensive in terms of finances (IBM Security, 2025). This trend underscores that cybersecurity is not just a technical problem but one of the fundamental economic problems, which affect the sustainability of organizations and the stability of the national economy.

## 5.2. Sectoral Impact

Cyber threats have the following economic effects:

a. Direct financial losses as a result of fraud and theft.
b. Costs related to system recovery and incident response.
c. Customer mistrust and tarnished reputation.
d. Breakage of business processes.

Research has shown that the financial industry is one of the most attacked industries considering the sensitivity and value of the financial information. Likewise, the healthcare sector has witnessed rising cyberattacks because medical data is very vital and the continuation of services is urgent. Hacking into these sectors can easily lead to overly high losses relative to other industries (World Economic Forum, 2024).

Additionally, cyberattacks on the critical infrastructure like energy, transportation, and water systems have the potential to produce cascading economic impacts that are not only limited to individual organizations but also to entire countries. The disruptions can cause loss of productivity, high costs of operation and greater economic instability (Accenture., 2023). On the other hand, spending on cybersecurity yields the following positive economic impact, such as:

a. Development of jobs in cybersecurity and IT.
b. Support for digital transformation and innovation
c. Improvement of economic resilience and business resilience.
d. The appeal of foreign direct interest in investment by safe online spaces.

As such, cybersecurity must be perceived as a safeguarding system rather than merely as a response to safeguard the economy but also it may be viewed as a strategic driver of economic development and sustainability.

## 5.3. Country-Level Impact

On the national scale, the economic effects of cybersecurity are directly associated with the digital maturity of a country, regulations, and institutional capacity. The information in Table 1 and Table 2 shows that the economic effects of cybersecurity-related issues differ significantly among countries. More developed economies are likely to have greater absolute financial losses because of the size of their digital systems and the worth of their data resources. Nonetheless, the resilience of these countries is also higher because of the effective developed cybersecurity measures and reaction systems.

Conversely, developing countries usually report less financial losses but have a higher relative economic vulnerability. This is mainly because of poor cybersecurity systems and inadequate technical capability and enforcement of regulations. Consequently, in these settings, cyber attacks can be disproportionately devastating to both the economic and societal services. This can be seen with the example of Iraq. Iraq being a nation at an immature stage of cybersecurity maturity has numerous issues concerning institutional coordination, technical expertise, and policy implementation. All these issues enhance vulnerability to cyber risks, especially in vital sectors like finance and government services.

Altogether, country-level analysis proves the fact that the maturity of cybersecurity is closely related to the economic resilience. Those countries which invest in the cybersecurity infrastructure, legal frameworks, and human capital are in a better position to counter the economic losses and use the digital transformation to achieve sustainable development (International Telecommunication Union, 2024).

As illustrated in Figure 6, industries that deal with high value and sensitive information especially finance and healthcare are the most affected in terms of economic losses. This proves the fact that the cyber risks are concentrated in data-intensive sectors and the necessity of industry-specific cybersecurity measures (World Economic Forum, 2024).

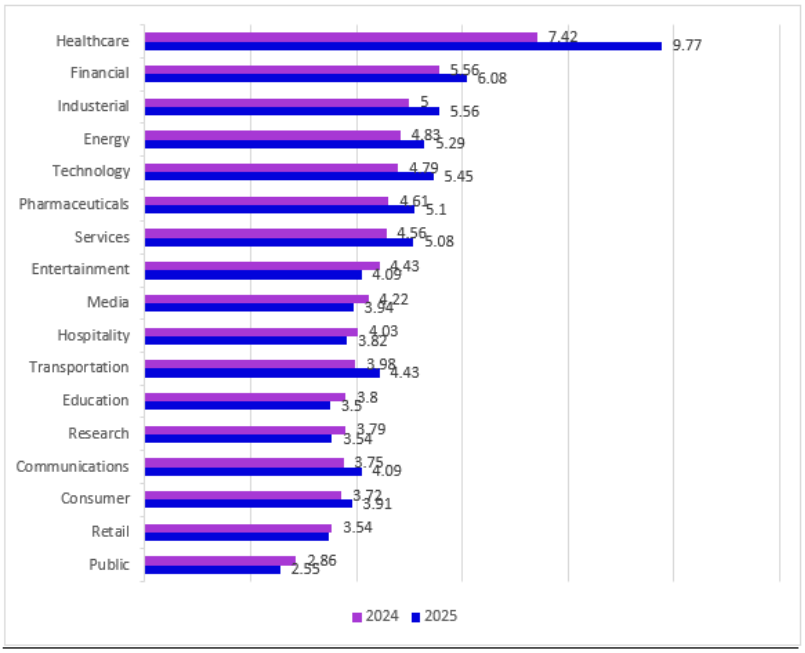


**Figure 6. The Economic Sectors with the majority of cyberattacks (USD Millions) are shown**

## 6. Discussion

The results of this paper proceed to affirm the fact that cybersecurity has become a multidimensional strategic space that has a direct impact on political stability, economic performance and social resilience. The combination of empirical evidence, especially the reports on cybersecurity in the world and the economic impacts of the threats, proves that cyber threats are no longer the specific technical events but the systemic threats of the country development processes.

Economically, the analysis shows that the financial implication of cyberattacks is on a steadily rising trajectory, with the average cost of a data breach in the world amounting to about USD 4.44 million in 2025. This pattern indicates the rise in complexity of cyber threats and the growing importance of digital assets in the contemporary economies (IBM Security, 2025; World Economic Forum, 2024). Further, the fact that the costs in different regions vary widely, with higher costs in the United States being much higher than those in developing areas, underscores the importance of regulatory frameworks, digital maturity, and incident response capabilities in driving economic results.

The findings also indicate that the adoption of technology, especially artificial intelligence and automation, is a key factor in reducing economic losses. Companies that operate with high levels of cybersecurity technology will incur much less costs in breaches which means that spending on cybersecurity is not only a defensive measure but a strategy with respect to economy (Accenture., 2023).

On the geopolitical level, the analysis establishes the fact that cybersecurity has transformed the traditional understanding of power and the concept of sovereignty. The data presented by the Global Cybersecurity Index (GCI) demonstrate that there are significant inequalities in cybersecurity preparedness on the country and regional levels. Large economies in the Tier 1 classifications overshadow Tier 1 countries, although numerous developing nations such as Iraq are found in the tiers of Tier 1, showing structural difficulties within the legal systems, institutional capacity and technical infrastructure (International Telecommunication Union, 2024; ENISA, 2023).

The regional analysis of Arab countries further back up this conclusion. Saudi Arabia and the United Arab Emirates are very mature in cybersecurity, and others, including Iraq, are in the transition phase. This gap indicates that the quality of governance, prioritization of investments and effectiveness of policy implementation are associated with the development of cybersecurity.

The situation in Iraq, at the national level, demonstrates some crucial gaps in cybersecurity preparedness. Although greater awareness has been made, the challenges associated with institutional fragmentation, inadequate technical capability, and lack of cybersecurity integration in the national development strategies are hindering growth of cybersecurity in the country. These obstacles put the critical infrastructures and economic systems at a high level of risk especially in areas like finance and government services (Salman., 2021).

The discussion affirms that cybersecurity is not merely a defensive tool, but also a significant determinant of national competitiveness, economic sustainability as well as geopolitical power in the digital age. These results show that cybersecurity maturity is strongly connected and inline with economic resiliance, institutional standard procedures, and technological investment, reinforcing its role as a strategic player in national development directions.

## 7. Conclusion

This research concludes with the argument that cybersecurity is one of the pillars of protecting the political, economic, and social bases of contemporary states. The high rate of development of digital technologies has opened new development opportunities and, at the same time, presented new complex and dynamic risks. The results indicate that cyber threats have extensive consequences beyond the technical disturbances, including economic stability, governance systems, and trust in the society. The rising price of cyberattacks underscores the necessity to have viable cybersecurity measures, especially in developing nations whereby vulnerabilities are still high.

Moreover, the paper establishes that institutional capacity, legal framework, technological infrastructure, and investment level differences affect the existence of disparities in cybersecurity preparedness among countries. Those countries putting cybersecurity as a priority field are in a better position to attain resilience, economic growth and geopolitical stability. When it comes to Iraq, the analysis proves that though some initial measures are taken to develop cybersecurity, there are still gaps. To eliminate these gaps, a multi-faceted and coordinated strategy must be created, involving policy change, capacity development, and technology. Finally, cybersecurity should be perceived as a cross-cutting concern, which involves the areas of national security, economic growth, and global governance, which means it is a major element of state sustenance in the digital era.

## 8. Recommendations

Based on the findings, the study proposes the following:

a. Create a National Cybersecurity Strategy. Governments, especially those in the developing world ought to develop holistic cybersecurity policies in line with the national development objectives.

b. Enhance Legal and Regulatory Regimes. The revising of cybercrime laws and enforcement systems is necessary to correspond to new threats and hold people responsible (Suleiman., 2020).
c. value Human Capital investment. The human factor should be considered as the weakest aspect of cybersecurity systems, and capacity building and specialized training programs should be prioritized.
d. Make Cybersecurity a part of Economic Planning. Cybersecurity is to be seen as an instrument of economic growth and not a purely cost center.
e. Adopt Advanced Technologies Artificial intelligence, machine learning, and automation should be used more extensively to enhance detection and response functions.
f. Increase Regional and International Cooperation. The threat of cyber-attacks should be addressed with combined efforts of sharing information and collaborative efforts worldwide.
g. Target Critical Infrastructure Protection. Such priority sectors as finance, healthcare, and energy should be safeguarded by sophisticated protection systems.

## Author Contributions

All authors have equal contributions to the paper. All the authors have read and approved the final manuscript.

## Funding

No funding support was received.

## Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/ or publication of this article.

## Data Availability

The datasets generated during and/ or analyzed during the current study are available from the corresponding author on reasonable request.

## Declaration on AI Use

The authors declare that no artificial intelligence (AI) or AI-assisted tools were used in the preparation of this manuscript.

## References

Accenture. (2023). *State of cybersecurity resilience 2023*. Accenture Report

Alguliyev, R. M., Imamverdiyev, Y. N., Mahmudov, R. S., & Aliguliyev, R. M. (2021). Information security as a national security component. Information Security Journal: A Global Perspective, 30(1), 1-18.

Arab Monetary Fund. (2022). *Cybersecurity in Arab financial systems*. Arab Monetary Fund

Brookings Institution. (2021). *Cybersecurity and state resilience*. Brookings Institution

Cisco. (2022). *Cyber threat trends report*. Cisco Cyber Threat Trends

Deloitte. (2023). *Future of cybersecurity report*. Deloitte Report

European Central Bank. (2022). *Cyber risk and the financial system*. ECB Publication

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. ENISA Threat Landscape

Goni, O. (2022). Cyber crime and its classification. *Int. J. of Electronics Engineering and Applications*, 10(1), 01-17.

Google Cloud. (2024). *Cybersecurity forecast 2024*. Google Cloud Forecast

IBM Security. (2025). *Cost of a data breach report 2025*. IBM Security

International Monetary Fund. (2021). *Cybersecurity risk supervision*. IMF Publication

International Telecommunication Union. (2024). *Global cybersecurity index 2024*. ITU Cybersecurity Index

INTERPOL. (2022). *Global cybercrime strategy*. INTERPOL Strategy

Joyner, C. C., & Lotrionte, C. (2017). Information warfare as international coercion: Elements of a legal framework. In The Use of Force in International Law (pp. 433-473). Routledge.

Kaspersky. (2023). *Cyber threat intelligence report*. Kaspersky Threat Intelligence

Lobastova, S. (2020). Geopolitics of Cyberspace and Virtual Power. Journal of Liberal Arts and Humanities, 3, 97-113.

Luo, Y. (2021). New OLI advantages in digital globalization. International Business Review, 30(2), 101797.

Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News, 190(1), 1-69.

McKinsey & Company. (2022). *Cybersecurity trends and impacts*. McKinsey Cybersecurity

Microsoft. (2023). *Microsoft digital defense report 2023*. Microsoft Digital Defense Report

National Institute of Standards and Technology. (2024). *Cybersecurity framework (Version 2.0)*. NIST Cybersecurity Framework

NATO Cooperative Cyber Defence Centre of Excellence. (2022). *Cyber threats and international security*. CCDCOE

Organisation for Economic Co-operation and Development. (2021). *Cybersecurity policy frameworks*. OECD Cybersecurity

Palo Alto Networks. (2023). *Unit 42 threat report 2023*. Unit 42 Threat Report

PwC. (2023). *Global digital trust insights 2023*. PwC Digital Trust Insights

Riordan, S. (2018). The geopolitics of cyberspace: A diplomatic perspective. Brill research perspectives in diplomacy and foreign policy, 3(3), 1-84.

Ripsman, N. M., & Paul, T. V. (2005). Globalization and the national security state: a framework for analysis. International Studies Review, 7(2), 199-227.

Salman, M. I. (2021). Cybersecurity and its impact on Iraqi national security. *Journal of Legal and Political Sciences, 10*(2), 45–61.

Sendjaja, T., Irwandi, E. P., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity in the digital age: Developing robust strategies to protect against evolving global digital threats and cyber attacks. International Journal of Science and Society, 6(1), 1008-1019.

Shahid, N., & Khan, A. (2022). Addressing cyber vulnerabilities through deterrence. Journal of Contemporary Studies, 11(1), 50-68.

Suleiman, A. F. (2020). Legal frameworks for cybercrime. *Tikrit University Journal of Law, 5*(1), 112–128.

United Nations. (2021). *Open-ended working group on ICT security report*. UN ICT Security Report

World Bank. (2021). *Cybersecurity for development*. World Bank Publication

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum Report

Xu, J., She, S., & Liu, W. (2022). Role of digitalization in environment, social and governance, and sustainability: Review-based study for implications. Frontiers in psychology, 13, 961057.