Dr. Rehab Hosny Al-Rahmawy

Telecommunications Engineer at the National Media Authority

Cybersecurity Management in the Economic Field

Introduction:

The global economy is witnessing several transformations and changes due to the entry into the digital world. Over the past thirty years, the dependence of governments, companies, and citizens on the Internet and information and communication technologies has increased significantly, forming a cyberspace that reflects what countries contain of data and savings, but in the form of highly sensitive digital information that simulates their economic reality, especially those countries that have been deeply involved in computerized work and have been immersed in information technology. This has made them an arena for cyber conflicts and this conflict was reflected on the economic field with the possibility of controlling it and tampering with its contents. Moreover, the countries that produced this technology are the most exposed to cyber risks, in addition to the difficulty of their commitment to the requirements of maintaining their national security.

Many countries and their institutions and companies face cyber risks that affect the economic field of the state, which made them share a level of responsibility in managing these risks. Therefore, countries and companies must first realize that their digital strategy and agenda should be based on a disciplined approach to confronting and managing cyber risks in them. Negligence and failure to take appropriate measures exposes them to many risks. Furthermore, the cyber threat is increasing due to the availability of a market for malicious software and tools, illegal services, and sensitive data that is not publicly available (at affordable prices). Therefore, data security poses a major challenge to the economic field, and despite this, most institutions have not taken steps to strengthen their cybersecurity skills.

The rapid transition to a global digital economy is leading to an increase in cyberattacks day by day, becoming more complex and impactful. This imposes upon us the need to confront and manage these cyber risks in order to formulate a new and secure digital economic reality. This reinforces the importance of countries securing their systems and entities well and working to manage cyber risks in the economic field to achieve national security through an administrative approach to confront these cyber risks. Many institutions and organizations suffer from the inability to administratively manage cyber risks. Hence, this study came to shed light on how to manage cyber risks in the economic field.

Problem of the Study:

The study aims to research and analyze the The problem of the study lies in identifying cyber risks and their negative effects on the economic field of countries and their institutions and organizations, especially since many countries are currently seeking digital transformation, which has formed a field for cyber intrusions and exposure to cyberattacks that require managing these cyber risks so as not to lead to losses in the economic field of countries and their economic institutions and organizations and to achieve national security.

Significance of the Study:

The significance of the study stems from the fact that cyber risks pose a threat to the economic field of countries and their institutions and organizations, threatening their national security. Especially with the governments' shift to the digital economy, cyber risks have emerged to threaten those achievements. Hence, it is necessary to shed light on these cyber risks, their impact on the economic field of countries, and how to manage their cyber risks, both within countries and within organizations and institutions, to achieve national security for countries.

Objectives of the Study:

To develop a proposed strategy for managing cybersecurity risks in the economic field of countries.

Research Methodology:

A descriptive-analytical approach was employed to analyze how to manage cybersecurity risks for the economic field and to identify the impact of cybersecurity risks on the economic field of countries and their institutions and organizations. This was done in an attempt to answer the main research question:

How can countries manage cybersecurity risks in their economic field and for their organizations and institutions to achieve national security?

The study on cybersecurity risk management in the economic field is structured around five main axes:

Axis 1: Theoretical and conceptual framework of the study.

Axis 2: Impact of cybersecurity risks on the economic field.

Axis 3: Procedures for managing cybersecurity risks in the economic field.

Axis 4: Key features of a proposed strategy for managing cybersecurity risks in the economic field.

Axis 1: Theoretical and Conceptual Framework of the Study

First: The Concept of Cybersecurity Risks:

Cybersecurity risks are operational risks to information and technology assets that have consequences that affect the confidentiality, availability, or integrity of information or information systems. Compared to the categories of risks covered by insurance, cybersecurity risks share the same characteristics and responsibilities as both property and liability risks, as well as catastrophic and operational risks [1].

Second: Classification of Cybersecurity Risks:

Cybersecurity risks in the economic field are classified into two types: operational risks and technical risks, as follows:

1- Operational Risks:

A- **Responsibility**: Lack of a responsible entity for cyberspace and for protecting information.

B- **Classification**: Lack of information classification, on the basis of which information is classified according to its importance.

C- **Strategic Policies**: Lack of cyberspace policies and strategies, or non-compliance with them if they are available.

D- **Human Resources**: Lack of national trained competencies and cadres and a lack of cybersecurity awareness among all segments of society [2].

2- Technical Risks:

A- **Loss**: Loss and disappearance of information as a result of its deletion or damage.

B- **Destruction and Sabotage**: Destruction and sabotage of information by any means by internal or external parties for the purpose of preventing access to information permanently.

C- **Leakage**: Leakage of information from the main storage source.

D- **Change**: Modifying data for the purpose of falsifying it or providing misleading information that may damage the information.

E- **Disruption**: Preventing access to information temporarily.

F- **Obsolescence**: Failure to update information for a period of time, which reduces the value of the information and provides inaccurate results [3].

Third: The Relationship between Cybersecurity and the Economy:

The relationship between the economy and cybersecurity has become intertwined in light of the digital transformation process that many governments are adopting to seize the opportunities of the Fourth Industrial Revolution. Confronting cybersecurity risks, especially in the economic field in the digital age, has become one of the emerging issues that have imposed new variables on governments in many countries around the world. New interests and dangers of a cyber nature have emerged in light of the increasing reliance on cyberspace, the provision of services, the accumulation of wealth, and the negative impact of the lack or weakness of cybersecurity on the economy, especially the digital economy.

This is within the framework of the direct relationship that brings together both dimensions, and its impact on the rates of confidence in the digital environment, digital supply, digital demand, and information infrastructure, especially with the increasing cyber risks in the digital environment, and at the same time the increasing role of the digital economy in economic growth, which has prompted countries to increase spending on cybersecurity and allocate resources in the state's general budget or in its budget concerned with security and defense. This is in light of the renewed challenges imposed by digital transformation operations and their economic applications, which have led to a quantitative and qualitative change in the elements of wealth and economic resources and the pillars of supply and demand.

The economic perspective on cybersecurity confirms that actors from governments, companies, or users have different security demands and interests according to the nature of use. This conflict of interests needs to be subject to self-control standards, whether through monitoring some or taking reactions based on the incentives that drive the motives of each party [4].

Fourth: Cybersecurity Risk Management:

Cybersecurity risk management is typically presented as a process, and the stages consist of the following:

Risk identification, Risk analysis, Risk evaluation, and Risk monitoring and review

Cybersecurity risk management involves applying a logical and systematic approach to identify, analyze, evaluate, treat, and monitor risks in a way that enables organizations to minimize losses and maximize gains. Risk management can be applied at multiple levels within an organization; it can be applied at the strategic and operational levels [5].

Creating a path for emerging risk management and responding quickly and effectively is crucial to ensure a streamlined response and to mitigate any potential risk as much as possible, and to implement response strategies and management processes proactively [6].

Cybersecurity Risk Management Steps:

1. Identify Cybersecurity Risks:

The organization identifies potential cybersecurity risks that could negatively impact a specific operation or project it undertakes. It is also necessary to identify the business environment and contributing factors that can cause cybersecurity risks and the root causes of cybersecurity risks, and to describe the risks and understand the purpose of the risks and the threats facing the organization. It is worth noting that proactive assessment is supported by relevant data, trends, and current events [7]. Risks can be identified from a variety of sources, as follows:

A- Brainstorming with experienced operations personnel.

B- Developing risk scenarios.

C- Data analysis programs.

D- Safety surveys and safety reviews in operations monitoring.

E- Incident investigation statements.

F- Regulatory factors, such as the institution's, organization's, or company's employment and training policies, rewards, and resource allocation.

G- Operational environment factors, such as surrounding noise and vibrations, temperature and lighting, and protective equipment, human factors such as medical conditions, human performance limitations, and the human-machine interface.

H- Regulatory compliance factors, such as compliance with regulations and the approval of equipment, personnel, and procedures.

- Cybersecurity Risk Identification Tools:

Checklists, Surveys, Personal inspections, Expert opinions, Brainstorming, SWOT analysis, Risk surveys, Workshops, Risk analysis, Risk assessment, Risk treatment policies, Risk monitoring and tracking (8).

2 . Cybersecurity Risk Analysis:

Risk analysis is the next step in the risk management process, but it can also be the first step if there are risks that have been identified by means other than risk assessment. The primary purpose of risk analysis is to evaluate. Once specific types of risks have been identified, the organization determines their classification, priorities, controls, and risk levels, and then the probability of their occurrence and their consequences. The goal of analyzing these risks is to increase understanding of each specific risk and how it can affect the organization’s strategic goals.

The five steps (9) of the risk analysis process can be explained as follows:

A- Clear Description of Risks:

There should be a brief statement that describes what the cybersecurity risks are and how they can affect the achievement of goals. The risk review team should agree on the scope of the risk and then describe the risk scenario, which explains what the potential risk event looks like.

B- Causes of Risks:

This means ***“Why does this risk happen?”*** In addition to the immediate causes of the risks, we also need to understand the root causes and main drivers; in order to effectively reduce the likelihood of risks.

C- Preventive Controls:

Once we understand the root causes, we need to agree on the existing controls that help reduce the likelihood of these causes or drivers, and identify additional controls that we can put in place to further reduce the likelihood; organizations that follow a proactive safety risk management strategy believe that they can reduce cybersecurity risks by identifying weaknesses and taking steps to mitigate the negative consequences of emerging risks.

D- Consequences of Risks:

This means what will be the impact if these risks materialize? Identifying these potential consequences in advance helps in developing emergency plans in case of a risk.

E- Mitigating Controls:

- What controls should be implemented that will help reduce the impact of the consequences?
- What additional controls can be put in place to further reduce the impact?

3. Cybersecurity Risk Assessment:

The relevant management must implement cybersecurity risk assessment procedures at a minimum in the following cases:

A- In the early stages of technical projects.

B- Before making a major change to the technical infrastructure.

C- When planning to acquire third-party services.

D- When planning and before launching new technical products and services.

Cybersecurity risk assessment includes the following:

Threat and vulnerability: It also analyzes and takes into account existing mitigating factors (10). The purpose of the risk assessment element is to identify the following:

A- Threats directed at organizations: This means any operations or assets or individuals or threats directed by organizations against other organizations.

B- Weaknesses inside and outside organizations.

C- The damage (i.e., the adverse impact) that may occur in the light of the likelihood of threats.

D- The likelihood of damage.

The practitioner analyzes cybersecurity risks to determine the likelihood that threat events and exposure conditions will lead to harmful effects on a system asset. Similarly, the practitioner analyzes the impact value and calculates the exposure risks using the methodology specified in the organization’s risk strategy, such as (risk probability x risk impact). Therefore, root cause analysis (thinking about past events that have already led to an event) helps to look at the potential consequences of future events. It also helps to document the sequence of outcomes that can arise after a threat event begins. While expert judgment is valuable in estimating risk factors, one way to reduce subjectivity is to supplement this judgment with simulation models (11).

Cybersecurity risks must be reassessed and updated as follows:

A- Periodically for all information and technology assets, and at least annually for sensitive systems.

B- After a cybersecurity incident that violates the security, availability, and confidentiality of information and technology assets.

C- After receiving important audit results or proactive information.

D- In the event of any change to information and technology assets.

The cybersecurity risk assessment process should cover the following:

A- Cybersecurity risk analysis: The cybersecurity management team should assess the likelihood of risks and threats and their resulting impacts, and use the results of this assessment to determine the overall level of these risks. The cybersecurity management team should use a quantitative or qualitative methodology to conduct the risk analysis.

B- Cybersecurity risk estimation: The cybersecurity management team should estimate the magnitude of cybersecurity risks in accordance with the institutional risk assessment standards adopted in "name of entity" and determine how to deal with them according to priority [12].

4. Cybersecurity Risk Treatment or Response:

Cybersecurity risk response involves identifying a set of risk treatment options, evaluating them, preparing risk treatment plans, and implementing them. These options include risk avoidance, reducing the likelihood of occurrence, reducing the consequences, transferring risk, and retaining risk[13].

The cybersecurity management team should identify cybersecurity risk treatment options according to the following steps:

A- Risk treatment or reduction: Treat or reduce the severity of the risk by applying the necessary security controls to reduce the likelihood of occurrence or impact, or both, which helps contain risks and keep them within acceptable levels.

B- Risk avoidance: Eliminate the risk by avoiding the continuation of the risk source by doing the following:

- Sharing or transferring risks: Sharing risks with a third party that has the capabilities to deal with risks more effectively, or insuring information and technology assets in the event of exposure to cybersecurity risks.
- Accepting and bearing risks: The risk level is acceptable but must be continuously monitored in case of change.

Cybersecurity risk response options include: tolerance, which is only appropriate when it can be accepted when the loss or damage has occurred / retention, treatment / reduction, transfer (and is based on giving people directions on how to make sure there is no loss, but relies on people who follow established safe working systems) and termination and avoidance (by implementing appropriate preventive controls). Risk response is criticized as being more corrective than preventive, as shown in the following figure.

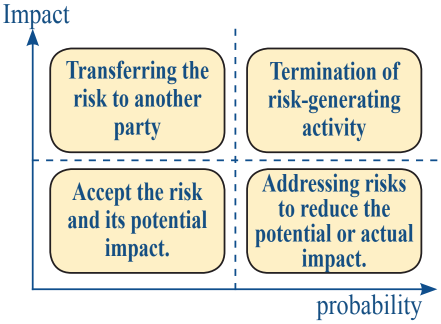
Impact
Transferring the risk to another party
Termination of risk-generating activity
Accept the risk and its potential impact.
Addressing risks to reduce the potential or actual impact.
probability

Figure illustrating risk response options [14].

During this step, the organization assesses the highest-rated cybersecurity risks, deals with them proactively, and develops a plan to mitigate them using specific risk controls. These plans include risk mitigation processes, risk prevention tactics, and emergency plans in case of risks [15].

5- Cybersecurity Risk Monitoring:

It is part of the mitigation plan that involves monitoring all cybersecurity risks from monitoring, tracking new and existing ones on an ongoing basis, as well as reviewing and updating the comprehensive risk management process according to different and changing situations. Risks are reviewed quarterly to identify new risks and existing changes, update the risk register, and assess the actions taken by risk owners to manage risks and correct improper performance [16].

To monitor cybersecurity risks, the cybersecurity management team must prepare and maintain a risk register to document the outputs of the cybersecurity risk management process, which must include at a minimum the following information:

A- Risk identification process.

B- Risk scope.

C- Risk owner or responsible person.

D- Description of the risks, including their causes and effects.

E- Risk analysis that explains the impacts of the risks and their time horizon.

F- Risk assessment and classification that includes the probability and size of the risks and their overall classification in case of occurrence.

G- Risk treatment plan that includes the risk treatment procedure, the person responsible for it, and its timeline.

H- Description of the residual risk.

I- The cybersecurity management team must periodically collect and review evidence related to the state of cybersecurity risks.

6. Acceptable Level of Cybersecurity Risk:

This is done as follows:

A- Cybersecurity risk acceptance criteria must be identified and documented, according to the risk level, the cost of risk treatment versus its impact, by determining the extent of the impact of the risk, where each risk is classified[17] into one of the following cases:

- Risks with a significant impact, and procedures and plans must be put in place to address them.
- Risks with a major impact, which require study and planning.
- Risks with a medium impact, which can be taken into account.
- Risks with a low impact, which do not require specific plans.
- Risks with a very low impact, which do not require specific plans.

B- Additional controls must be implemented to reduce the risk to an acceptable level if the residual risk does not meet the risk acceptance criteria.

C- If the risk acceptance criteria are exceeded, escalation to the competent authority is made to take the necessary actions or decisions.

D- Cybersecurity risk management procedures must be updated at planned intervals (or in the event of changes in legal, regulatory, and related standards).

E- Annual review of the cybersecurity risk management policy.

7. Cybersecurity Risk Monitoring:

It is based on continuous monitoring of new risks and what has been achieved to be added to the cybersecurity risk management process on an ongoing basis [18].

The purpose of the risk monitoring component is as follows:

A- To determine the ongoing effectiveness of risk responses (in accordance with the organizational risk framework).

B- To identify changes that affect the risks and the environments in which systems operate.

C- To verify that planned risk responses have been implemented and that they comply with laws, directives, regulations, policies, standards, and guidelines [19].

Axis 2: Impact of cybersecurity risks on the economic field

The relationship between security and technology has increased, and with it the potential for state strategic interests to be exposed to cybersecurity risks, and even threatened to transform cyberspace into a medium and source of new tools for international conflict [20].

The most prominent cybersecurity risks to the economic field include the following:

1. Manipulating, distorting, or destroying information in a specific system, whether through hacking or spreading viruses.
2. Ordinary crimes that use the Internet for theft, fraud, identity theft, intellectual property infringement, and more.
3. Organized crime, which threatens the security of individuals and states, such as money laundering and terrorism, etc., such as security threats related to the ransomware system, which is a criminal tool that has spread over the Internet for several years, continues to evolve and includes both individuals and economies at the individual level.
4. Risks of intelligent technologies such as digital currencies that could lead to economic collapse and facilitate the commission of crimes as they are difficult to track because they are encrypted and facilitate money laundering, as well as the use of social engineering, which is one of the

means of fraud in knowing the bank accounts from the targeted individual himself [21].

5. Cyberattacks may target the complete shutdown of the Internet in the targeted country, which leads to the suspension of bank transactions, e-government transactions, and the theft of credit card numbers and details that are used for shopping online, which results in the disruption of the flow of money in the country, and consequently the suspension of the most important sectors in the country, such as industry and other sectors of the state, and transactions may fail due to the imprisonment of liquidity, and families and companies lose their ability to access deposits and payments, and in such a severe scenario, investors and depositors may demand their money or try to cancel their accounts or other services and products that they use regularly.
6. Hacking tools are now less expensive, easier, and more powerful, allowing hackers with limited skills to inflict more damage for a fraction of the previous cost. The expansion of mobile-based services (which is the only technological platform available to many) increases hacking opportunities. Attackers target large and small institutions, rich and poor countries, and operate across borders, so fighting cybercrime and reducing its risks must be a shared responsibility across and within countries [22].
7. Individuals may launch cyberattacks to steal money from individual bank accounts, as well as competing countries and ideological opponents may aim to obtain sensitive data and cause disruptions to financial systems and panic among citizens.

Due to the exposure of the economic system in countries to such risks, there must be national economic security, as it is one of the most vulnerable security sectors to cyberattacks, given the transformation of the global economy into a digital economy that relies on information technology, and therefore exposing such a system to such risks It may cause huge economic and national losses affecting the achievement of national security, which necessitates working on managing cybersecurity risks in the economic field [24].

Axis 3: Cybersecurity Risk Management Procedures in the Economic Field

First: Technical Procedures:

Sensitive information resources can be protected from cybersecurity threats by keeping them out of sight or out of the eyes of attackers by following these procedures:

1- Physical protection: This includes the following:

A- Cybersecurity surveillance that does not allow hackers access.

B- Surveillance cameras that are placed in different parts of the building.

C- Tight security that does not allow any access to information.

2- Encryption: This is done by mixing digital information so that it can only be rearranged using a specific key. The mixed information is completely incomprehensible to someone who does not have this key. This mixing process is called encryption, and the process of returning the encrypted message to its original state is called decryption and return.

3- Protection through components: This method provides almost complete protection against viruses by using devices without the used memory. Optical discs can also be used to permanently store programs, and these discs are read-only and cannot be written to. Operating systems can also be stored on these discs, which protects them from viruses.

4- Filtering: One of the methods that many parties resort to in order to cover up is what is known as filtering, which is a way to obtain selected information from secret information without revealing the secret information itself.

5- Monitoring the disposal of information waste: This procedure must be applied accurately and carefully to avoid cybersecurity risks because there are programs, methods, and ways that can be used to recover data from storage media after it has been erased [24].

Second: Administrative Procedures:

All countries are emphasizing the preservation and protection of their information from theft and sabotage. This keenness has forced them to take, in addition to technical procedures, some administrative procedures in their centers and devices, and on the workers. Some of these procedures are as follows:

1- Defining responsibilities: The responsibility for protecting information and avoiding cybersecurity threats lies with three important parties, namely: the Head of Information, the Cybersecurity Manager, and the Cybersecurity Officer, as follows:

A- Head of Information: Implements security procedures accurately to ensure the confidentiality of the establishment's information, has the ability to delete any information he wants, and set usage instructions and give authorization.

B- Cybersecurity Manager: His task is to control the contents of the center and is also responsible for encryption devices.

C- Cybersecurity Officer: Responsible for selecting and examining programs, making sure they are free of viruses or encryptions that can be exploited by the enemy or pranksters.

2- Defining powers: One of the difficulties facing the protection of information is the access of people from inside or outside the establishment to information centers. Therefore, the powers must be defined for the persons authorized to access and use information and databases, as well as setting rules that specify the persons or groups that have the right to access a specific type of information. This requires dividing the files within the computer network into specific sections, so that no one can access a section that is not authorized for them, and this helps a lot in protecting information from the reach of saboteurs.

3- Protecting individuals: Workers in information centers are exposed to deliberate attacks by the enemy in order to paralyze their ability to protect their information. Therefore, these individuals must be protected and fortified against the ideas and procedures of psychological warfare waged by the enemy, and their adherence to their principles must be consolidated.

4- Device maintenance: Maintenance workers from the manufacturing company or the company that installs the system must be continuously monitored when they are allowed access to information centers during maintenance. This problem is overcome by replacing the company's maintenance workers with individuals from the establishment who are trained to perform maintenance work [25].

Axis 4: Key Features of a Proposed Cybersecurity Risk Management Strategy in the Economic Field:

Objective of the Proposed Strategy:

Achieving secure economic growth in Egypt and protecting it from any cybersecurity threats.

Pillars of the Proposed Strategy:

The proposed strategy is based on several pillars, the most important of which are:

1- Allowing global companies in this field to enter the Egyptian market and provide a variety of advanced services.

2- Egypt ranks fourth among Middle East and North Africa countries and 23rd globally in cybersecurity among 182 countries with a score of 95.45 out of 100.

3- Establishment of the Supreme Council for Cybersecurity and the Egypt CERT Center to respond to Internet and computer emergencies.

4- Egypt's membership in some international unions and bodies specialized in cybersecurity.

5- Cohesion and readiness of the armed forces and their adoption of the approach of modern electronic armies in order to confront the newly emerging Egyptian security threat that relies on cyberspace.

6- The Central Bank of Egypt regulating the use of digital currencies and preventing their trading.

7- Bringing about a change in the nature of the business environment for all economic sectors, as the demand for cybersecurity insurance technology against cybersecurity risks has doubled.

Determinants of the Proposed Strategy:

The proposed strategy is based on several determinants, the most important of which are:

1- The shift to the digital economy has become a means that helps more in hacking and cyberattacks.

2- The relative increase in the cost of applying information systems and cyberspace security technologies noticeably.

3- The difficulty of applying information systems and cyberspace security controls due to the weak cybersecurity culture among some workers in some sectors, especially the financial and banking sectors.

4- The need for a clear monitoring mechanism for all sectors, especially banks and financial companies, to ensure that there are controls and policies in place to achieve cybersecurity and manage its risks.

5- Backwardness, ignorance, and illiteracy, and the growth pressures that lie on the shoulders of society in terms of poverty, illiteracy, and crime all limit the opportunities for transition to the information and cyber society. Therefore, economic infrastructure must develop so that societies can easily enter the information and cyber society.

6- The shortage of competencies at the level of some administrative leaders due to lack of training and brain drain posed a major challenge.

Key Executive Policies of the Proposed Strategy:

First: On the Regional and International Level:

1- Formulate a joint international and Arab strategy to confront the escalation of cyber threats, strengthen cybersecurity, and cooperate in the fields of combating cyber risks, so that it is formulated in cooperation and coordination by research centers and official institutions concerned.

2- Activate digital signature technology to protect the funds of banks and institutions.

3- Use artificial intelligence to confront cyber threats, as there is now artificial intelligence that confronts artificial intelligence.

4- Develop electronic protection programs to counter cyberattacks. In this context, partnerships have been formed between countries and the private sector in each country to develop the infrastructure.

5- Prepare awareness programs about cybersecurity that are presented and broadcast in a clear and simplified way to the general public.

6- Review the international legal rules that regulate this type of war, and the need to formulate international consensus in this regard.

7- It is necessary for countries to work to secure their systems and entities well, report cyber incidents, and effectively share information, in order to enhance the ability of authorities around the world to effectively manage incidents, as the incident reporting and knowledge-sharing model that the Financial Stability Board (The Financial Stability Board) is working on is an important step to strengthen cybersecurity.

8- Develop preventive capabilities: Developing economies and low-income countries should be assisted in strengthening financial stability and supporting financial inclusion by ensuring that technology is used in a way that preserves security and safety against cyber threats.

Second: On the Local Level:

1- Establish an economic cybersecurity center to deal quickly with any economic problem. This is different from cybersecurity management, but this management is linked to this center. This is due to the importance of the economic field, as it is a sensitive field that can affect the rest of the country's fields.

2- Economic awareness and security culture for businessmen and investors to face any cyber threats, such as blackmail and hacking operations, and how to deal with these situations.

3- Activate high-speed internet, as it plays a major role in economic development.

4- Partnership between the public and private sectors in the exchange of information about various cyber threats.

5- Eliminate financial technology illiteracy and spread digital awareness in society.

6- Allocate structures for cyber deterrence, which is what Article 14 of the Budapest Convention on Cybercrime stipulated, as it allows for a quick response to any cyber attack.

7- Develop response strategies, as the financial system must be able to quickly resume operations.

8- Activate the cyber deterrence strategy, as the cost of cyberattacks must be reduced and their risk minimized through effective deterrent measures.

9- Use media such as television and radio to raise awareness about the protection of personal data.

10- Establish an authority, which is an independent national regulatory body for the Internet, which includes an online security platform with a huge amount of simulated information and resources; to help the community and promote online responsibility, flexibility to build a positive culture, and its mission is to promote digital safety by strengthening the positive culture around digital citizenship. Its tasks also include containing an intensive complaints system to help the community; So if a social media site does not comply with the standards set out in the Code of Practice, individuals can resort to the Digital Safety Commissioner, who can direct the social media site to comply with the standards set out in the Code. With raising public awareness about cybersecurity by adopting proactive prevention efforts.

Conclusion:

The study addressed the problem of cybersecurity risks in the economic field, especially for institutions and organizations in countries. It answered an important question: How can countries manage cybersecurity risks for themselves and their organizations and institutions in the economic field? The study pointed to the procedures and policies required to manage cybersecurity risks in the economic field. The study concluded with the following results:

1- The rapid development of technology has contributed to an increase in the volume of cybersecurity risks facing countries, as it reveals greater weaknesses, cheaper and easier tools for attackers, and while some financial companies and regulatory bodies have become more aware and prepared for cyberattacks, cybersecurity gaps remain large and continue to pose a challenge to institutions and countries.

2- The number of cyberattacks has increased over the past two decades, to the point where it has become one of the most important means and tactics adopted by the conflicting parties around the world, due to its low cost and the losses that may result for the attacking party compared to the extent of what can be achieved and inflicted on the opponent through its employment.

3- There are many technical and administrative procedures available to confront, manage, and combat cybersecurity risks and attacks in cyberspace, and that adhering to the application and activation of as much as possible of them can be a great help in countering these attacks and even working to manage their cybersecurity risks before they occur.

4- We find that the security of countries is no longer related only to protecting them from military risks and attacks, but has expanded and widened to include the need to protect their societies, vital facilities, infrastructure, and especially the economy from exposure to cybersecurity risks.

5- The need for regulatory compliance of institutions in managing cybersecurity risks; as mere desire without well-studied policies and procedures is not enough to create a culture of anti-cybersecurity risks.

6- It has become necessary to work to reduce these cybersecurity risks by putting in place procedures and policies that protect economic data in countries. Accordingly, following an administrative system for managing cybersecurity risks within the organizations and institutions in the state is the solution for protecting the economic and financial sectors from piracy and data breaches. Therefore, it has become necessary to work to manage cybersecurity risks in the economic field to protect and achieve national security for countries.

References:

(1) Cebula, J.J. and L.R. Young, A taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, 2020, Pennsylvania, P 75.

(٢) صــلاح حيدر عبد الواحد، حروب الفضــاء الإلكتروني: دراسة فى مفهومها وخصائصــها وسبل مواجهتها، ٢٠٢١، جامعة الشرق الأوسط، عمان، ص ٥٨.

(٣) المرجع السابق، ص٦٠.

(4) ISOC, Unleashing the potential of the internet for ASEAN economies. https://www.internetsociety.org/sites/default/files/ASEAN_ISOC_Digital_Economy_Report_Full_0.pdf, (5 mars 2023).

(5) Authority, C. A. S., Safety management systems, Canberra, ACT, Australia, 2002, P 45.

(6) Sityata, I., Botha, L., & Dubihlela, J., Risk Management Practices, Version 5, South African Universities, 2021, South African, p 195.

(7) Pest Management Regulatory Agency Health Canada, A Framework for Risk Assessment and Risk Management of Pest Control Products, PMRA Guidance Document, Canada, 2021, p 112.

(٨) عمر النجار، أثر إدارة المخاطر على التميز المؤسســى لجامعة الأقصــى بقطاع غزة، رسالة ماجستير، كلية الاقتصاد والعلوم الإدارية، الجامعة الإسلامية، ٢٠٢٠، غزة، ص ٦٨.

(٩) أحمــد الخيــاط، تصــور مقترح لتطويــر إدارة الأعمال فى ضــوء مدخــل إدارة المخاطر بمؤسســات الأعمال الكويتيــة، المجلة العلمية للاقتصاد والتجارة، كلية التجارة، جامعة عين شمس، ٢٠٢٠، القاهرة، ص ٢٨.

(١٠) المرجع السابق، ص ٢٩.

(11) Quinn, S., Ivy, N., Barrett, M., Feldman, L., Witte, G., & Gardner, R., Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management, National Institute of Standards and Technology, 2021, p.p 52-53.

Enterprise Risk Management, National Institute of Standards and Technology, 2021, p.p 52-53.

(12) Hopkin, PFundamentals of risk management: understanding, evaluating and implementing effective risk management, Kogan Publishers, 2020, London, p135.

(13) Cybersecurity Risk Management: Why it is needed and How to proceed. https://www.azeusconvene.com, (10 Mars 2023).

(14) Maphorisa, Leadership and the risk management Conundrum in Batswana Country, 24 (1) Mosennodi Journal, 2021, Botswana, p. 17

(15) Buganová, K., & Šimíčková, J., Risk management in traditional and agile project management, Transportation Research Procedia, Version 40, 2021, p.p 986-993.

(١٦)سارة محمد حسين، إجراءات مقترحة لإدارة المخاطر السيبرانية، العدد الرابع والثلاثون، مجلة الإدارة التربوية، ٢٠٢٢، القاهرة، ص ٣٥.

(17) Aven, T., Risk assessment and risk management: Review of recent advances on their foundation, European Journal of Operational Research, 2016, p.p 1-13.

(18) Centers for Medicare & Medicaid Services Information Security and Privacy Group, Version 3, Risk Management Handbook, 2021, Chapter 14, p195.

(19) Ibid, p. 195.

(٢٠) سارة محمد حسين، مرجع سابق، ص ٦٥.

(٢١) مروة فتحى السيد بغدادى، اقتصاديات الأمن السيبرانى، مجلة البحوث القانونية والاقتصادية، العدد ٧٦، يونيو ٢٠٢١، القاهرة، ص١٦.

(٢٢) المرجع السابق، ص١٧.

(٢٣) صــليحة محمدى، الارهــاب الإلكترونى والأمن القومــى للدول: نمط جديد وتهديــدات مختلفة، المجلة الجزائريــة للأمن والتنمية، ٢٠٢٠، الجزائر، ص٦٧.

(٢٤) نبيل حشاد، إدارة المخاطر السيبرانية بالمصارف، العدد ٢٨٨ ، مجلة اتحاد المصارف العربية ، ٢٠٠٤، ص ٣٥.

(25) Khan, M. A., & Malaika, M., Risk Management Fintech and Cybersecurity, International Monetary Fund, 2021, p.p 87 - 90.

Cyber Risks Management in the Economic Field

■ *Dr / Rehab Hosny El Rahmawy*

Communications Electrical Engineer at the National Media Authority

Abstract:

This study explores the critical relationship between the cyber domain and the economy, heightened by the widespread adoption of information technology. The cyber realm's significance lies in its capacity to bolster a nation's comprehensive state capabilities and affect individuals and the nation across all levels.

The research investigates the emerging trend of cyber warfare, wherein cyber attacks employing strategic cyber weapons, including destructive programs and viruses, are used to manipulate a nation's economy in alignment with the aggressor's strategic objectives. These attacks aim to disrupt the economic infrastructure of the target state, jeopardizing its national security. Therefore, the study emphasizes the need to proactively manage cyber risks within a nation's economic sphere.

The study's central challenge is identifying and mitigating cyber risks' adverse impact on a nation's economic entities and institutions. Its significance lies in understanding how these risks affect a nation's economic landscape and proposing strategies for proactive risk management to ensure national security.

The study concludes that various technical and administrative measures are available to counter and manage cyber risks and attacks. Adherence to these measures can effectively thwart cyber attacks and proactively manage cyber risks before they materialize, safeguarding a nation's economic security.

Keywords: Cyber space, Cyber Risks, Economic field

إدارة المخاطر السيبرانية فى المجال الاقتصادى

■ د/ رحاب حسنى الرحماوى

مهندسة كهرباء اتصالات بالهيئة الوطنية للإعلام

المستخلص :

يرتبط الجانب السيبرانى ارتباطًا وثيقًا بالاقتصاد، خاصة بعد التوسع فى استخدام تقنيات المعلومات والاتصالات، ولذلك يأخذ الأولوية فى الاهتمام لما له التأثير الأكبر على تعزيز باقى قدرات قوى الدولة الشاملة ويؤثر فى مقدرات الأفراد والوطن على جميع المستويات.

فقد هدفت الدراسة إلى معالجة موضوع يُعد من الموضوعات الحديثة والبالغة الأهمية حيث تمثل المظهر الجديد لحروب المستقبل من خلال استخدام الفضاء السيبرانى كوسيلة للهجوم السيبرانى للسيطرة على اقتصاد الدول باستخدام مجموعة من البرمجيات، والفيروسات المدمرة كأسلحة استراتيجية سيبرانية ناتجة عن توجهاتهم الاستراتيجية، وكوسيلة لتدمير البنية التحتية الاقتصادية للدولة، ومن ثم التأثير على الأمن القومى للدولة المستهدفة، مما جعل هناك ضرورة للعمل على إدارة هذه المخاطر السيبرانية فى المجال الاقتصادى للدولة، ولذلك تظهر مشكلة الدراسة فى تحديد المخاطر السيبرانية وآثارها السلبية على المجال الاقتصادى للدول وللمؤسسات والمنظمات بها. تأتى أهمية الدراسة فى توضيح تأثير المخاطر السيبرانية على المجال الاقتصادى للدول وكيفية إدارة مخاطرها السيبرانية داخل المنظمات والمؤسسات لها، لتحقيق الأمن القومى.

وقد خلُصت الدراسة إلى عدة نتائج منها أنَّ هناك العديد من الإجراءات الفنية والإدارية المتاحة لمجابهة وإدارة المخاطر والهجمات السيبرانية فى الفضاء السيبرانى والتصدى لها، وأن الالتزام بتطبيق أكبر قدر منها يمكن أن يكون معينًا إلى حد بعيد فى التصدى لهذه الهجمات بل والعمل على إدارة مخاطرها السيبرانية قبل حدوثها.

الكلمات المفتاحية : الفضاء السيبرانى، المخاطر السيبرانية، المجال الاقتصادى