REVIEW OF INTERNATIONAL GEOGRAPHICAL EDUCATION

ISSN: 2146-0353 • © RIGEO • 11(4), WINTER, 2021

www.rigeo.org

Research Article

Requirements of Formulating a National Strategy for Developing the Cybersecurity System in Iraq According to GCI.v4(2019) Index

Yasin Salman Saadoun Al-Wasiti[1]
College of Administration and Economics - Universityof Baghdad/Iraq

Firas Raheem Younis Alazzawi[2]
College of Administration and Economics - University of Baghdad/Iraq
Firas.alazzawi@coadec.uobaghdad.edu.iq

Abstract

The present study aims to present a proposed realistic and comprehensive cyber strategy for the Communications Directorate for the next five years (2022-2026) based on the extent of application and documentation of cybersecurity measures in the Directorate and the scientific bases formulating the strategy. The present study is significant in that it provides an accurate diagnosis of the capabilities of the cyber directorate in terms of strengths and weaknesses in its internal environment and the opportunities and threats that surround it in the external environment, based on the results of the assessment of the reality of cybersecurity according to the global Cybersecurity index, which provides a strong basis for building its strategic direction Which is expressed by its vision, mission, and realistic strategic objectives. The researcher adopted the case study method for its objectivity and being the closest and best method to prove the research problem and provide objective and realistic treatments for it. As for the field of application of the present study, it is represented by the Communications Directorate due to its great importance and its close relationship to the communications system in Iraq and national Cybersecurity, in addition to the fact that it has not been subjected to testing the extent to which Cybersecurity measures are applied and documented before. The checklist was used according to the Global Cybersecurity Index (GCI.v42019). In order to measure the extent of the application and documentation of cybersecurity measures in the Directorate, personal observation and interviews were used as tools for data collection. The SWOT matrix was adopted to analyze the internal and external environment factors.

Keywords

Cybersecurity, Strategy Formulation, SWOT Matrix, Cybersecurity Strategy.

To cite this article: Al-Wasiti, Y, S, S. and Alazzawi, F, R, Y. (2021) Requirements of Formulating a National Strategy for Developing the Cybersecurity System in Iraq According to GCI.v4(2019) Index. *Review of International Geographical Education (RIGEO), 11(4), 49-71. doi: 10.33403/rigeo. 800625*

Submitted: 20-03-2021 • **Revised:** 15-04-2021 • **Accepted:** 25-05-2021

Introduction

Planning in general and strategic planning helps organizations achieve two important outcomes represented by clear decisions about the goal and strategy and commitment to those decisions. It is a process that is designed to support leaders in being intentional, i.e., knowing where to go rather than reactive. Simply put, it is a management tool, and as with any management tool, it is used for one purpose only, which is to help the organization do more systematic work (Allison & Kaye, 2015). Strategic planning is embodied in a set of concepts, procedures, and tools that are designed to assist leaders and managers in these tasks. Strategic planning can be defined as an organized effort to produce the key decisions and actions that shape and direct what an organization or other entity is, what it does, and why it does it. In the past forty years, strategic planning has become a standard part of management thinking and practice in the business world. In the past twenty years, strategic planning has become the standard practice for large public and non-profit organizations (Bryson & Alston, 2011). The purpose of strategic management is to exploit and create new and different opportunities for tomorrow. In contrast, long-range planning attempts to improve today's trends for tomorrow (David & David, 2015).

By developing and implementing a national Cybersecurity strategy, a country can improve the security of its digital infrastructure and ultimately contribute to the realization of its broader socio-economic aspirations. National leaders must follow a strategy on the opportunities and risks to their countries due to the digital environment. They must also have a clear vision of the digital future they aspire to (ITU., 2018). Cybersecurity is a process with a special focus on protecting confidentiality, integrity, and the availability (CIA) of digital information assets in all economic, industrial, health, and other fields, against any threat that may arise from the exposure of these assets to penetration using the Internet (von Solms & von Solms, 2018). Large and complex infrastructures are easy to manage using computers, popular operating systems, applications, and network protocols. However, this convenience comes at a price. Communication is now way ahead of security. This makes the Internet and Internet users vulnerable to attacks (Geers, 2011). Hence, the present study seeks to employ strategic planning in the aspect of Cybersecurity to identify the requirements of formulating a national Cybersecurity strategy in Iraq through the use of the Global Cybersecurity Index of 2019-2020 by identifying strengths, weaknesses, opportunities, and threats through the SWOT matrix according to the level of application and documentation of Cybersecurity measures and their volume and categorizing them according to their priority into strategic issues that embody the most important challenges facing Iraqi national security in its implementation of the national Cybersecurity strategy based on the results of the matrix above analysis in order to create a strategic direction represented by a vision, mission, and strategic objectives for the future period in light of the appropriate strategic option with the real capabilities of the directorate. In the end, a set of executive programs will be presented. The researcher proposes these programs to address the most important strategic issues facing the directorate in Cybersecurity.

Literature Review

Cybersecurity

The Commission of Enhancing National Cybersecurity (CENC) defines Cybersecurity as the process of protecting information and information systems by preventing, detecting, and responding to unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (FAS, 2018). The French government defines it in the National Defense and Security Strategies as the desired state of an information system in which it can withstand events from cyberspace that are likely to jeopardize the availability, integrity, or confidentiality of the data stored, processed, or transmitted and the related services provided by these systems. Cybersecurity uses information systems security techniques based on combating cybercrime and creating an electronic defense (Maurer & Morgus, 2014). Cybersecurity is also defined as the state of protection against the criminal or unauthorized use of electronic data or the actions are taken to achieve this (Brookson et al., 2015). The United Kingdom's National Cybersecurity Strategy states that cybersecurity refers to protecting information systems, hardware, software, and infrastructure associated with them and the data on them and the services they provide from unauthorized access, harm, or misuse. This

includes damage caused intentionally by the system operator, or by mistake, as a result of not following security procedures" (Rashid et al., 2018). ITU defines Cybersecurity as a set of tools, policies, security concepts, security guarantees, guidelines, and approaches of Cybersecurity, risk management, procedures, training, best practices, assurance, and techniques that can be used to protect the cyber environment, organization, and user assets. Enterprise and user assets include connected computing devices, personnel, infrastructure, applications, services, communications systems, and the sum of information transmitted and/or stored in the electronic environment. Cybersecurity strives to ensure that the security characteristics of the organization and user assets are achieved and maintained against relevant security risks in the overall electronic environment" (Prasad & Rohokale, 2020).

Based on the definitions above, the two researchers define cybersecurity as the activities that are desired to achieve the availability, integrity, and confidentiality of data in cyberspace and to protect users in the country from the risks of attacks, data and information breaches by targeting the national information infrastructure, through the adoption of a national strategy Cybersecurity that includes means of defense against attacks. The most important thing is to search for gaps in the country's information infrastructure and address them before they become a point of attraction for attackers".

Strategy Formulation

Drucker (1954) defines strategy through five short questions represented by our business? Who is the customer? what is the value to the customer? what will our business be? Moreover, what should it be? The basic consideration of strategy is the matching of management's vision, company capabilities, and customers' needs and desires through a series of options with long-term survival and profitability as goals (Webster Jr, 2009). Alfred Chandler defines strategy as the identification of the basic long-term goals and objectives of the organization, adopting courses of action, and allocating resources to implement these Objectives (Nickols, 2016). The strategy usually includes two main processes: formulation and implementation. Formulation involves analyzing the environment or situation, making a diagnosis, and developing indicative policies. It includes activities such as strategic planning and strategic thinking. Implementation refers to the action plans taken to achieve the goals set by the guiding policy (Barad, 2018). Strategic planning in its simplest form is the practice of a systematic and integrated approach to policymaking that considers the context, resources and long-term. It has its origins in the military decision-making process. It has also been more rigorously developed in business than public sector planning (Dimitriou & Thompson, 2007). The main difference between strategic and tactical planning is that strategic planning usually involves thinking and making decisions that affect the organization. Tactical planning usually involves thinking and making decisions that affect a part of the organization (such as a specific functional group or department) (Simerson, 2011). Therefore, before beginning strategic planning, organizations must have made clear their mission and vision, and define their core policies in order to determine the path through strategic plan between the current situation of the business and the situation that is required to be achieved, helps the business to determine its goals and objectives. Decisions to achieve these goals and objectives involve a long-term and future perspective (BÜTÜNER, 2016). Formulation of strategy in organizations is an ongoing process.

Specific dilemmas within the company or in the corporate environment may increase the awareness of members of the organization about the strategy and allow analysts to think of strategy formulation as an intentional process built on certain bad decisions. However, strategy implicitly shapes all the time. The study of the strategy formulation process includes analyzes of both discrete and identifiable decision events and the pathways leading to decision events and their outcomes, along with the links between successive decisions over time (Pettigrew, 1977). The rational model describes strategy formulation as a set of Actions: Defining the current strategy, analyzing the environment, resources and gaps, identifying and evaluating strategy options, strategic choice and implementation (Narayanan & Fahey, 1982).(Wheelen, Hunger, Hoffman, & Bamford, 2018) state that Strategy formulation, often referred to as strategic planning or long-range planning is concerned with developing a mission in the company, its objectives, strategies and policies. It begins with the analysis of the situation: the process of finding a strategic fit between external opportunities and internal strengths while working around external threats and internal weaknesses (Wheelen et al., 2018). According to(QUINN, Mintzberg, & James, 1995), strategy formulation includes defining the company's vision, mission and determining Attainable

 goals, developing strategies, and setting policy guidelines (Mbulwa & Kinyua, 2020). In conclusion,the two researchers describe the strategy formulation process as the process of creating the finalstrategy document through the process of environmental monitoring and analysis, and establishing the strategic direction represented by the vision, mission, values, objectives and identifying the most important issues facing the organization in order to overcome them with strategic options and facilitating the process of selecting the best alternatives that ensure the survival of the organization.

Data analysis

Analysis Of Application-Level Data and Documentation of Cybersecurity Measures

A set of mechanisms for analyzing the gaps achieved by implementing the Global Cybersecurity Index (GCI.v4:2019) will be reviewed and documented. The analysis of the measures of the above index measures will be addressed to identify their causes within the research sample.

The Graph of Matching Ratios

Based on the checklists that have been achieved, which showed the level of application and documentation of the measures of the Global Cybersecurity Index (GCI.v42019), the results of the weighted adjusted arithmetic mean and the percentage of matching of the main measures of the Global Cybersecurity Index will be shown as in Table (1).

Table (1)
Summary of Conformance and Documentation Level Results for the Measures of the Global Cybersecurity Index (GCI.v4:2019) in Communications Directorate

No	Headlines of Measures by Indicator (GCI.v4:2019) Measures	Calendar Scores For actual application and authentication		
		Grade achieve 1	Percentage achieved%	Gap ratio per measure%
1	Legal measures	0.45	8%	92%
2	Technical measures	1.3	20%	80%
3	Regulatory measures	0.5	8%	92%
4	Capacity development	1.2	20%	80%
5	Cooperative measures	3	50%	50%
Total results of the achieved calendar		6.45	106	394
Maximum application and full documentation of measures		6	100	100
Total assumed application and full documentation		30	500	500
Amount of gap in application and documentation of total measures		23.55	394	106
The proportion of total results			21.2%	78.8%

Source: The two researchers based on the data analysis.

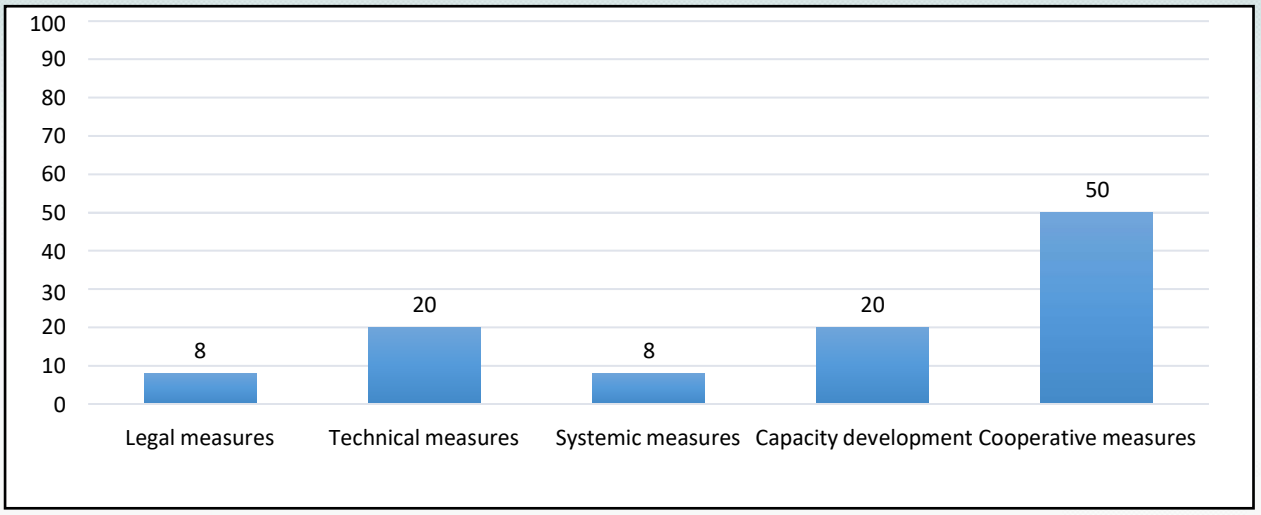

Figure (1) The total level of application and documentation of cybersecurity measures according to the Global Cybersecurity Index.

From Figure (1), it is noticed that the percentage of application and documentation of all measures was under half. However, the gap for each requirement prevented the application and complete documentation of the measures of the global Cybersecurity index.

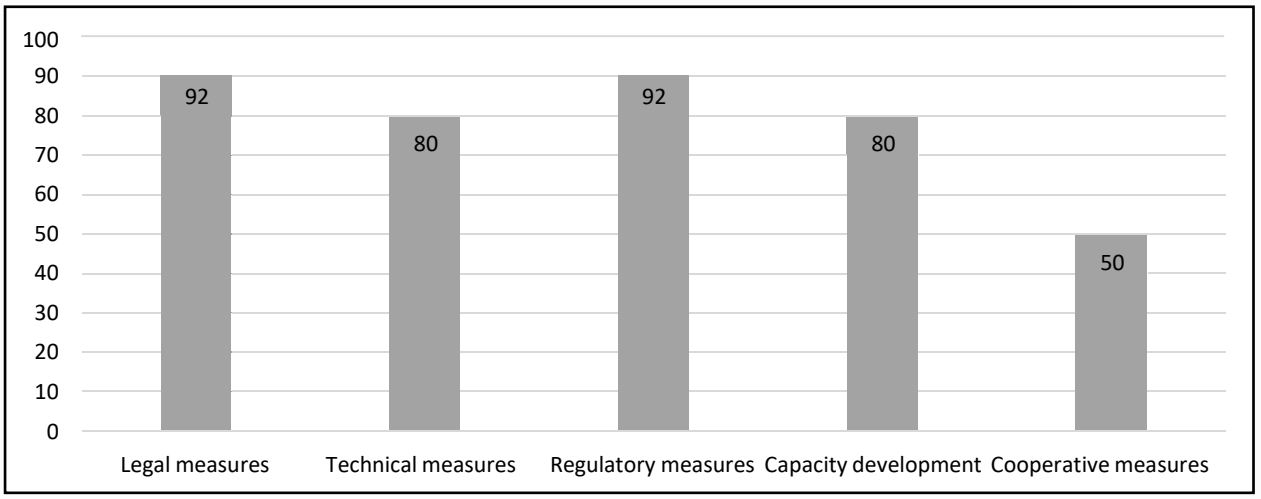

Figure (2) The amount of application gaps in the Global Cybersecurity Index (GCIv.4:2019) in the surveyed directorate

From Figure (2), it is clear that the highest gap is the (legal and organizational measures) gap witha percentage of (92%) whereas, (cooperative measures) gap is the lowest at a percentage of (50%).

Using The Pareto Chart to Analyze the Results

The Pareto chart is the tool that enables the administration to distinguish between factors with a high impact and the least impact. It is also defined as (80:20) analysis, i.e., the most influential minority versus the non-influential majority. There is a set of procedures that must be completed on the data table for the checklists to prepare the data for Pareto analysis. They are as follows: Collecting the results of the checklists and for each of the basic measures of the indicator. Extracting the modified percentage using the law (part/whole * 100). Extracting the cumulative percentage. Arranging the results in ascending order. Drawing the chart. Through all the procedures above, the results are as shown in Table (2).

Table (2)
Configuring Checklist Results for Pareto Analysis

No	Measures	Gap Ratio%	Adjusted percentage	Cumulative percentage
1	Legal measures	92	23.45	23.35
2	Regulatory measures	92	23.35	46.6
3	Technical measures	80	20.30	67
4	Capacity development	80	20.30	87.3
5	Cooperative measures	50	12.69	100
Total		394	100%	

Source: The two researchers based on the results of the checklists.

Pareto analysis displays the level of gaps in terms of identifying the most influential minority. Both legal and regulatory measures appeared at a rate of (92%), which is the gap that must start to be reduced. This will help achieve (46.7%) of the global Cybersecurity index. It is followed by the technical and capacity development measures by (80%). It ends with cooperative measures by (50%), which got the least gap. Thus, the gap is reduced until all the measures of the Global Cybersecurity Index GCI are applied (100%).

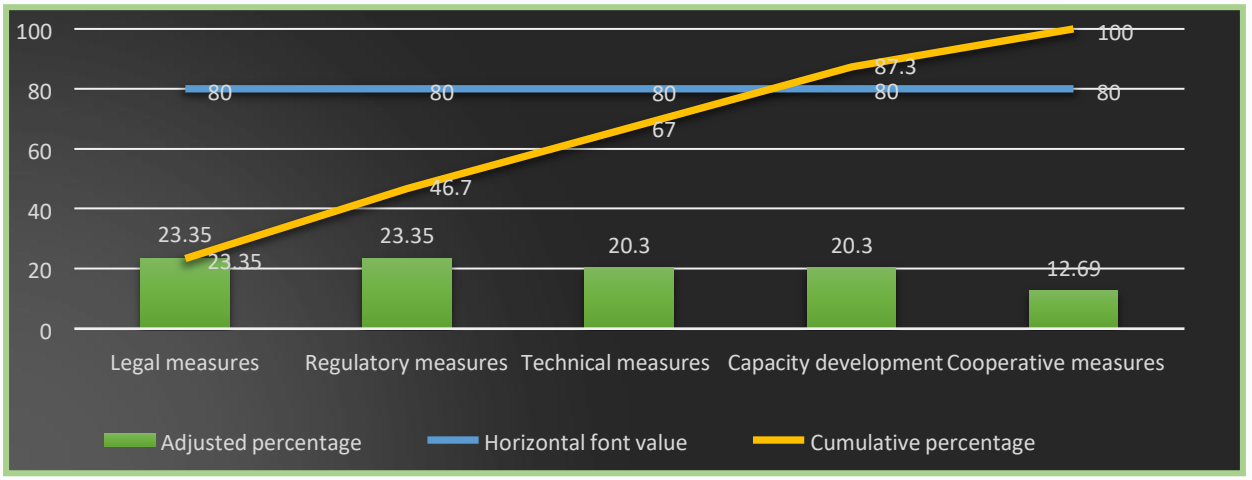

Figure (3) Pareto analysis of the level of the main gaps for the measures of the Global Cybersecurity Index (GCI.v4: 2019) in terms of identifying the most influential minority in the Telecommunications Directorate

It is noted from Figure (3) that the highest gap was achieved in legal and regulatory measures (23.35%) for both of them in relati1on to the total gaps. The lowest gap was achieved with cooperative measures (12.69%).

Graphical Representation of Gap Ratios

The Cause-Effect Diagram, which is called the Ishikawa Diagram and the Fishbone Diagram due to its shape, was used to analyze in detail the gaps of Cybersecurity measures in implementing and documenting the measures of the Global Cybersecurity Index (GCI.v4:2019) in the Communications Directorate. This scheme aims to indicate the possible causes of the problem and elicit details in completing this analysis through brainstorming to identify the main and subsidiary reasons causing the gaps in the application and documentation of the Global Cybersecurity Index (GCI.v4:2019).

Table (3)
Some Possible Main and Secondary Causes of the Global Cybersecurity Index Gap (GCIv.4:2019).

No	Major Reasons	Minor Reasons
1	Weak application of legal measures	Not issuing the law of communications and information, the law of cyber-crime and the law of personal data protection Lack of periodical update of laws
2	Weak application of technical measures	Uredines of electronic infrastructure Lack of modern technical equipment
3	Weak application of regulatory measures	The national Cybersecurity strategy has not yet been approved
4	Weak application of capacity development	Lack of periodic and continuous awareness campaigns for cybersecurity for all age groups lack of academic specializations under the name of Cybersecurity explicitly so far Lack of educational curricula on Cybersecurity in primary and secondary education
5	Weak application of cooperative measures	The lack of international cooperative agreements for Cybersecurity Lack of agreements aimed at developing cyber capabilities Lack of participation in international cyber activities

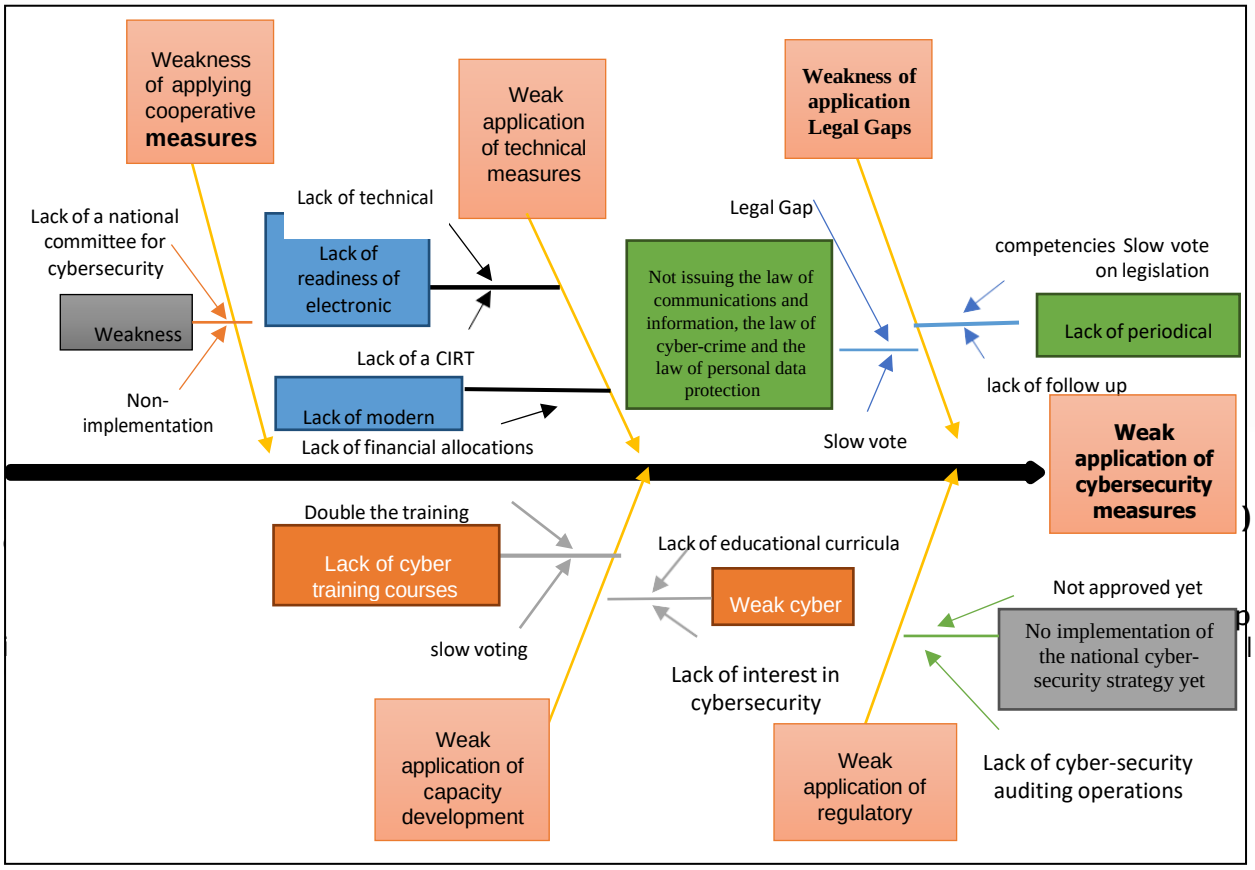

Figure (5)

(SWOT) Matrix to Analyze the Internal, External Environment and Determine the Strategic Options for Communications Directorate

	Strengths	Weaknesses	
Internal environment	1. There is a tendency by the Directorate to introduce appropriate cyber legislation and submit it to the legislature. 2. The Directorate has an efficient technical staff. 3. The Directorate has a direction to participate in the formulation, implementation and evaluation of a national Cybersecurity strategy. 4. The Directorate tends to adopt development programs for Cybersecurity. 5. The Directorate has public-private partnerships.	1. The Information Offences Act, the Communications, Informatics Act and the Personal Data Preservation Act have not yet been adopted. 2. Poor application of child protection procedures on the Internet. 3. The application of controls, instructions to protect personal data and protect privacy in the Directorate has fluctuated. 4. Absence of laws to protect information infrastructure. 5. Lack of a framework for implementing Cybersecurity standards. 6. Weak systematic and periodic evaluation of the information security system. 7. Lack of modern technical equipment. 8. Lack of financial allocations to the technical aspect. 9. National electronic infrastructure is not ready and linked. 10. The need to attract technical competencies to support the cyber system. 11. The proposed national Cybersecurity strategy has not yet been endorsed.	12. The team responsible for cyber coordination relies on speculative information. 13. The lack of a team whose responsibility is to develop cyber capabilities. 14. Absence of Cybersecurity checks. 15. Failure to apply cyberspace risk assessment measures. 16. Weak cyber awareness campaigns. 17. Lack of cyber training courses, training and development programs. 18. Lack of studies and research in Cybersecurity development. 19. Lack of specialized security courses on computer security. 20. Lack of training staff in Cybersecurity. 21. Weak international Cybersecurity cooperation agreements. 22. Weak international cooperation agreements on strengthening the capacity of Cybersecurity professionals. 23. Participation in international Cybersecurity activities fluctuated. 24. Lack of multilateral agreements in the area of Cybersecurity.
External environment	Opportunities	Threats	
	1. Government support in the adoption of the Computer Offences Act. 2. The possibility of attracting legal specialists to develop cyber legislation. 3. The possibility of drawing on the experiences of developed countries in the field of cyber	1. Possible escalation of illegal attacks on devices and data (hacking). 2. The possibility of the attackers falsifying and illegal electronic manipulation. 3. Online abuses against dignity and humanity and threats to community peace. 4. Electronic loopholes are difficult to detect. 5. People's lack of	Power + Opportunity = Options for Evolution and Growth Expansion strategies Vulnerability + opportunities = treatment option (Prevention treatment strategies)

legislation. 4. The possibility of adopting cyberspace as a fourth sovereign space. 5. There is an opportunity to form a national cyber-CIRT response team. 6. The possibility of making use of the technical system of the cyber-developed countries. 7. Financial allocation for technical development supported by the Government. 8. Work to develop a pilot program on electronic threats for the general public. 9. Membership in the Incident Response Forum and Security Teams (FIRST). 10. Developing measures to assess the level of development of Cybersecurity at the national level. 11. Review and make use of States' Cybersecurity strategies. 12. Attracting strategic planning competencies. 13. Establishment of a cyber-development section. 14. Adoption of international measures to assess the level of development of Cybersecurity. 15. The possibility of using twinning programs in Cybersecurity. 16. The possibility of strengthening international cooperation programs in the area of staff development.	awareness of Cybersecurity. 6. The difficulty of managing cyber accidents. 7. The growth and evolution of harmful, malicious programs and applications. 8. Lack of expertise in equipment and software registered by the owners concerned, and poor application of measures to prevent the import of technical equipment for use. 9. The absence of a national industry of equipment, technology and information technology. 10. A lower Cybersecurity index compared to other countries. 11. Regulatory regression at Cybersecurity level. 12. Weak information security system. 13. Increased Cybersecurity risk for lack of evaluation measures. 14. Lack of training and development centers on the cyber side. 15. Lack of government incentives to promote the development of cyber capabilities. 16. Absence of national Cybersecurity industry. 17. Poor support for cyber education programs in education (high-secondary education). 18. Absence of competition in Cybersecurity. 19. Accumulated problems of disestablishment of an independent cyber body so far. 20. The database lacks information on cyber-attacks and threats in all sectors. 21. Marginalization in international Cybersecurity	Force + threats = defense option (Stability and stability strategy) Vulnerability + threats = contraction option (Regression and contraction strategies)

17. Establishment of an international cooperative network for the exchange of security information. 18. Increase in the number of women participating in global cyber seminars and conferences. 19. Increased cooperation with ministries and bodies to raise the level of cyberculture among staff.	partnerships.

By reviewing the above-diagnosed strengths and weaknesses or opportunities and threats, the strategic options provided by the SWOT matrix to the Communications Directorate, and by relying on the direct method in identifying strategic issues presented by (Bryson & Alston, 2011) in his book (Strategic Planning for public and non-profit institutions), the two researchers categorized a set of strategic issues, which represent the most basic challenges that affect the level of Cybersecurity in the directorate and based on the five main measures of the global Cybersecurity index, because the higher the percentage of application of these five measures, the higher the Cybersecurity index. Then. The Directorate achieves its set goals. These issues, their prioritization, and the degree of their importance will be the main pillars on which the two researchers rely when presenting programs to implement the proposed strategy for the Communications Directorate. A special sample of experts and specialists who have high experience and practice in the field of Cybersecurity were surveyed, based on a special form prepared for determining the order of priority for the strategic issues identified by the two researchers as a result of the results that appeared in the test of the extent of application and documentation of Cybersecurity measures in the Directorate. The results are as in table (4).

The Proposed Strategy for Cybersecurity for Communications Directorate

The proposed Cybersecurity strategy for the Communications Directorate will be reviewed according to the findings of the two researchers regarding the extent of the application and documentation of Cybersecurity measures in the directorate in question and the analysis of the gaps that appeared and which were reviewed above. So, all components of the proposed strategy will be closely related to the dimensions of the Cybersecurity index (GCI.v4: 2019), ensuring its use in developing the Cybersecurity system in Iraq by addressing all the gaps; in return, this leads to avoiding the low level of application and documentation of Cybersecurity measures that negatively affect Cybersecurity in the country.

Stages Of the Proposed Cybersecurity Strategy Formulation Process

Stage I: Strategic Environmental Assessment (Strategic Analysis)

In light of what was proven in the first stage of analyzing the environments of the Communications Directorate according to the Global Cybersecurity Index (GCIv.4: 2019), based on the results of the gap analysis that were proven, and through a set of direct interviews that were conducted by the two researchers with the relevant specialists In the various areas of work and activities of the Communications Directorate in order to explain the results that were adopted when measuring the extent of the application of Cybersecurity measures in the Directorate, a set of factors were. The factors express the strengths or weaknesses in the Communications Directorate, mentioning the opportunities and threats faced by the Directorate itself. The two researchers classified the factors according to the measures of the Global Cybersecurity Index (GCIv.4: 2019), and through the application of the (SWOT) matrix. For all the factors of strength, weakness, opportunities, and threats, the possible strategic options for the Communications Directorate were

identified, which will be analyzed and evaluated at the strategic selection stage in order to determine the appropriate strategic option in light of the strengths and weaknesses surrounding the directorate and the opportunities and threats provided by the external environment. Figure (5) represents the environmental analysis according to the (SWOT) matrix and the strategic options it provides to the Directorate.

Table (4)
Prioritization of the strategic issues of Communications Directorate

No	Strategic issue	Priority rating
1	Legal measures: Legislation is a critical measure to provide a coordinated framework for entities to prepare themselves for a common legislative and regulatory base, whether about the prohibition of specific criminal acts or the imposition of minimum regulatory requirements. The legal environment can be measured based on legal institutions and effective frameworks that deal with Cybersecurity and cybercrime.	High
2	Technical measures: Without adequate technical measures and capabilities to detect and deal with incidents, the Member States and their affiliated entities remain vulnerable to cyber risks that could limit the benefits arising from the adoption of information about digital technologies. Therefore, Member States need to have the ability to develop strategies Defining acceptable minimum-security standards and certification programs for software applications and systems. Technical measures can be measured based on technical institutions and frameworks dealing with Cybersecurity that the Member States have endorsed or developed.	High
3	Organizational measures: Organizational and procedural measures are necessary for the proper implementation of any national initiative. The member state must define a broad strategic goal with a comprehensive plan for implementation, follow-up, and measurement. Structures along the lines of national agencies have to be established to implement the strategy and assess the success or failure of the plan. Organizational structures can be measured based on the presence and number of institutions and strategies that regulate the development of Cybersecurity at the national level.	High
4	Capacity development measures: Capacity building is an inherent component of legal, technical, and regulatory measures. An understanding of technology, risks, and repercussions would help in developing the best legislation, policies, strategies, and regulation for the different roles and responsibilities. This field of study is often approached from a technological perspective. There are also many economic, social, and political implications for this field. Any capacity-building framework for advancing Cybersecurity should include awareness-raising and resource-providing activities.	High
5	Cooperative Measures: Cybersecurity needs input from all sectors and disciplines, which is why it must be addressed through a multi-stakeholder approach, promoting cooperation, dialogue, and coordination, and enabling a more holistic field of Cybersecurity implementation. It is difficult to better exchange information between different disciplines and within private sector operators.	Medium

Stage Two: Strategic Direction

Based on what was proven in the first stage, and according to the priority of the strategic issues identified by the two researchers, the proposed strategic direction of the Communications Directorate for the future stage will be presented according to the following components of the strategic direction:

Vision:

The Communications Directorate does not have a written strategic vision or a declared and planned strategic direction that reflects what it wants to achieve. Therefore, the two researchers sought to provide a clear, comprehensive, and feasible vision to facilitate its delivery and reception to implement it in light of its general framework. It is represented by a smart directorate that supports development to ensure a reliable, secure, and protected national cyberspace.
The following criteria were taken into account when drafting it:

a. It Is viable, ambitious, and it expands the future work of the Directorate.
b. It involves a considerable level of flexibility to change policies according to the position of the Directorate in the future.

The Mission:

The message must express the philosophy of the directorate and the purpose of its existence. Who are we? what do we distinguish us? What is our business? and what do we want to be in the future? Were all taken into consideration. It considered the extent to which the mission conforms to the directorate's goals and values and flexibility in responding to environmental changes.
We, the Communications Directorate, are distinguished by an excellent, experienced and highly skilled technical staff. We work to maintain the electronic security of citizens and state institutions in public and private sectors from penetration and tampering. We seek to plan for the development of the Cybersecurity system in the country, which preserves the sovereignty of the country and the economic, financial, social, health, and educational systems in partnership with all stakeholders.

Values:

In order to achieve the vision and mission of the organization, ensure the implementation of works, and avoid deviation of the decision from the ethical system, the Communications Directorate adopts the following values as a motivator and guide for the behavior of the administration and employees in the performance of work and decision-making:
a. Belonging and citizenship; Deepening belongs to the homeland.
b. Honesty; Professionalism and sincerity when performing business.
c. Justice; Equality when dealing with citizens.
d. Cooperation; Encouraging participatory teamwork that affects the efficiency and effectiveness of the directorate's environment.
e. Creativity and development; Excellence in work performance and sustainable development.

Main Objectives;

These are the optimal broad objectives that the Communications Directorate seeks to achieve and maintain. These goals reflect the desire and purpose of the Directorate in its practices and activities. The two researchers review the following basic goals of the Communications Directorate within the proposed strategy:
a. Enhancing and developing the capabilities of human and administrative resources in order to achieve the optimal investment of human capital.
b. Applying the information security and protection system to provide a safe work environment and achieve occupational safety.
c. Using the latest global technology in the field of Cybersecurity.
d. Maintaining the electronic security of the citizen from blackmail, hacking, and forgery.
e. Building the citizen's confidence in Iraqi cyberspace regarding confidentiality, safety, and availability.

Strategic Objectives;

By the prioritization of the strategic issues that have been achieved as in Table (5), which expressed the most important challenges facing the Communications Directorate in light of its surrounding internal and external environmental conditions, the two researchers formulated the strategic objectives of the Directorate. In line with the vision, mission, and proposed values, the

two researchers classified these goals according to the strategic issues that were previously identified as follows:

Table (5)
Strategic issues and strategic objectives of the Communications Directorate

No	Strategic Issues	Strategic Objectives
1	Legal measures	• Adopting a substantive law on cybercrime. • Adopting Cybersecurity regulations. • Voting on a law that considers Iraqi cyberspace to be a sovereign space. • Establishing a legal committee to follow up with the legislative authority.
2	Technical measures	• Creating and supporting National Incident Response Teams - CERT/CSIRT/CIRT • Linking response teams with sectoral teams distributed over the health and financial sectors, public utilities and emergency services. • Establishing a national framework for implementing Cybersecurity standards. • Protecting children online.
3	Regulatory measures	• Creating a national strategy for Cybersecurity. • Determining the agency that is responsible for implementing the strategy. • Adopting recognized standards in order to measure the development of Cybersecurity. • Adopting the Cybersecurity risk assessment program.
4	Capacity development measures	• Increasing the number of courses and the number of trainees for Cybersecurity professionals. • Developing educational programs or academic curricula to train skills and professions related to Cybersecurity such as code analysts, digital forensics experts, incident responders, security architects, and penetration testers. • Reviewing research and development programs in the field of Cybersecurity. • Supporting the national Cybersecurity industry.
5	Cooperative measures	• Establishing bilateral agreements with advanced cyber countries. • Participating in international forums. • Establishing partnerships between the public and private sectors. • Creating internal partnerships between agencies.

The Third Stage: Strategic Option

Referring to the SWOT Matrix Figure (5), it is noticed that it provided a set of strategic options that the Communications Directorate can pursue for the upcoming future phase as follows:

The SO Growth and Expansion Strategy:

Strategies for this option are based on the approach of exploiting the opportunities and strengths provided by the two environments and successfully and optimally employing those opportunities in order to support, improve, and expand the business and raise the level of the directorate's performance. It is noticed from Figure (5), which is represented by the SWOT matrix, that the Communications Directorate possesses some of the strengths within its internal environment. On the other hand, there are a set of opportunities provided by the external environment that the Directorate can invest in for the growth and expansion of its field of business and development for the better. Accordingly, there are two options of growth and expansion strategies for the Directorate: Adopting a development strategy for its current business and services or adopting a growth and expansion strategy in its business and services in other new areas. However, in light of the threats surrounding the external environment and the weaknesses belonging to the directorate, the two researchers believe that both options are not appropriate for the

directorate's situation and should be overlooked because they affect the directorate's performance negatively. Thus, they hamper the directorate's performance of its tasks and services.

Remedial strategy WO:

The treatment or transformation strategy is based on many opportunities in the external environment and the elements of weakness in the internal environment. It is usually adopted in order to reduce the impact of the factors of weakness by investing the opportunity provided by the external environment in order to ensure the continuity of work and performance and provide Services through improvement and overcoming the problems that the directorate suffers from. All this requires the formulation of strategies that include setting priorities that address these weaknesses based on the opportunities provided by the external environment. As this option is the most appropriate as a result of the environmental survey that was diagnosed through the SWOT matrix of the directorate's conditions, the two researchers believe that the directorate should exploit and invest the most important opportunities provided by its external environment in order to set and determine the priorities that aim to provide a real treatment for weaknesses, with focusing the attention on the size of the threats surrounding the directorate from the external environment to avoid them or reduce their impact by taking into account the opportunities and strengths of the directorate.

Defense Strategy (Stability and Constancy) ST:

This type of strategy helps maintain the current situation and what has been achieved by investing the strengths of the Directorate and employing them to face external threats, which leads to maintaining the achievements made by the Directorate. However, given the directorate's various work and tasks, which are closely related to technological development and keeping pace with changes in order to maintain the city's electronic security, especially in light of the weaknesses that the directorate suffers from, the two researchers believe that this option does not serve what is planned to achieve. This means that this option does not serve the achievement of the goals and objectives planned by the Directorate and does not keep pace with what may be required to be done in the future.

The TW retreat and contraction strategy:

This option depends on the retreat and withdrawal or contraction strategies. In other words, the directorate surrenders to the restrictions imposed by the weaknesses and threats surrounding it due to the negative impact they have on the directorate's activities, which leads to that the Directorate retreats and stops performing its tasks efficiently and effectively. Accordingly, the directorate's option is to adopt regressive strategies, which may be restructuring the directorate, adopting a strategy of reducing human resources or canceling some works and services. From the two researchers' point of view, this strategic option is not possible to adopt. This is due to the sensitive nature of the directorate's work and its responsibility towards society and the state because adopting such a type of strategy reflects the complete collapse of the state system and the deterioration of its public institutions.

Based on what has been analyzed and evaluated for the alternatives to the strategic options mentioned above and from the two researchers' point of view, the second option is the best and most appropriate of the other strategic options available to the Communications Directorate, represented by adopting remedial and preventive strategies because of the weaknesses it faces in its internal environment and by exploiting them optimally as well as by exploiting the strengths and the excellent opportunities provided by the external environment, which can be invested in confronting potential external threats in the future in a way that ensures correcting its procedures, sustaining its activities and work, and providing the best possible services to society in the next future stage, which leads to achieving the objectives of the Directorate and the objectives of the parties benefiting from the services it provides.

Table (6)
Strategic Case Programs of Legal Measures

Body / Vertical Section: Legal Strategic Issue One: Legal Measures Priority: high					
Time horizon	**2022**	**2023**	**2024**	**2025**	**2026**
Completion rate	**25%**	**55%**	**7%**	**7%**	**6%**

Strategic goals: • Adoption of substantive law on cybercrime. • Adoption of cybersecurity regulations. • Vote on a law that considers Iraqi cyberspace to be a sovereign space. • Establishing a legal committee to follow up with the legislative authority.		Obstacles and limitations: • Lack of effective follow-up by stakeholders. • The slow vote on laws by the legislative authority. • There are some legal gaps in some legislation due to continuous change and innovation in laws and decisions.
No	Software	Measures
1	Program to reformulate the legal framework for cybercrime	• Reviewing the legal basis for international legislation, instructions and norms related to cybercrime. • Working on diagnosing contradictions and overlaps in legal texts and identifying outdated ones that need to be updated. • Reconsidering the texts of the legal articles on information crimes in a way that does not restrict freedom of expression. • Work on proposing and drafting legal amendments that would address the cases diagnosed in the two paragraphs mentioned above, and submit them to the legislative authority for approval and acquire a sober legal form.
2	Cyber Security Legislation Program	• Forming a stakeholder committee consisting of specialists and consisting of international and criminal law experts and information engineering experts in order to identify the most important items and texts related to Cybersecurity. • Submitting proposals for the legislation of the cybersecurity law to the legislative authority to ratify it and acquire a solid legal form. • Proposing a law that states that Iraqi cyberspace is a sovereign space. • Coordination with the Ministry of Justice and the Supreme Judicial Council to allocate a judge to look into cybersecurity issues to ensure their speedy completion and resolution.
The executing agency	**Follow-up**	**Success indicators**
• Legal Department + Information Technology Department	Planning and Follow-up	• Existence of an ideal legal framework for information crimes. • Existence of a Cybersecurity law that preserves the country's electronic sovereignty.

Table (7)
Strategic Issue Programs: Technical Measures

Body/Vertical Section: IT Strategic Issue Two: Technical Measures Priority: high					
Time horizon	**2022**	**2023**	**2024**	**2025**	**2026**
Completion rate	**25%**	**55%**	**7%**	**7%**	**6%**

Strategic goals:	**Obstacles and limitations:**
• Creation and support of the National Incident Response Team - CERT/CSIRT/CIRT. • Linking response teams with sectorial teams distributed over the health and financial sectors, public utilities and emergency services. • Establishing a national framework for implementing cybersecurity standards. • Protecting children online.	• Weak financial allocations to modernize the technical system. • Some technical issues that appear during the update process. • Lack of qualified technical staff for this type of business. • Limitations imposed by the International Telecommunication Union.

No	Software	Measures
1	Technical qualification program	• Using modern information technology devices and preparing specialized personnel for that. • Create a CERT/CSIRT/CIRT cyber or computer incident response team. • Directing the private and public sector to adopt a sectorial CERT team linked to the national team. • Adopt a global framework for the implementation of Cybersecurity standards, including but not limited to those set by the International Organization for Standardization (ISO), the International Telecommunication Union (ITU), and the IETF-Internet Engineering Task Force.
2	Information and communications network security program	• Working to improve the Cybersecurity situation by enhancing awareness and building human resources capabilities. • Reducing spam and malicious software, ways to mitigate them, and regulatory aspects. • Protecting children through cyberspace and providing a hotline for that.
3	Program for obtaining the latest technical equipment	• Preparing a purchase order that includes all the main needs of technical equipment to meet the development process of the cybersecurity system.

The executing agency	Follow-up	Success indicators
• IT Department + Human Resources + Procurement Committee	Planning and Follow-up	• The existence of a technical system qualified for cyber work. • Ensure confidentiality, integrity and availability of information. • Availability of modern technical devices and equipment.

Table (8)
Strategic Issue Programs: Organizational Measures

Organization / Vertical Section: Planning and Follow-up
Strategic Issue Three: Regulatory Measures
Priority: high

Time horizon	**2022**	**2023**	**2024**	**2025**	**2026**
Completion rate	**25%**	**55%**	**7%**	**7%**	**6%**

strategic goals:

- Create a national strategy for cybersecurity.
- Determine the agency responsible for implementing the strategy.
- Adopting recognized standards in order to measure the development of cybersecurity.
- Adopting the Cybersecurity risk assessment program.

Obstacles and limitations:

- lack of planning disciplines.
- lack of planning oversight.
- There is no approved national Cybersecurity strategy.
- Overlapping cyber powers and responsibilities.

No	**Software**	**Measures**
1	Program for the Formation of a National Cyber Strategic Planning Team	• Identify the Planning Group, including its stakeholders, expertise and practice, to address strategic issues and identify priorities. • Work to train and equip the team before proceeding. • Mapping the way, the team works (defining the planning area). • Promote the distribution of planning responsibilities among the various members with their specialties damaged. • Participation of decision-makers, stakeholders and those responsible for formulating annual plans and identifying their views and proposals.
2	National Cybersecurity strategic document writing program and responsible agency	• environmental analysis of the reality of Cybersecurity throughout Iraq, and identification of the main weaknesses and strengths in the internal environment, opportunities and threats in the external environment. • Formulation of the National Cyber Strategic Direction (vision, message and organizational values). • strategic selection and identification of the main strategic issues of cybersecurity at the national level, the development of binding programs for their implementation and related budgets and procedures, and the development of an effective mechanism for monitoring and evaluating the stages of implementation of such plans in order to diagnose and avoid major deviations and errors and ways of addressing them. • Develop an advisory agency responsible for the implementation of this strategy.
3	Cybersecurity Metrics Program	• The adoption of officially recognized national and sectorial assessment practices in measuring the development of Cybersecurity. • The adoption of Cybersecurity risk assessment strategies is an example of this (ISO/IEC 27004).

The executing agency	Follow-up	Success indicators
• IT Department + Human Resources + Planning and Follow-up	Planning and Follow-up	• Having an efficient strategic planning team. • A strategic Cybersecurity plans. • Having a comeback or agency overseeing

	the execution. • some practices measure the evolution of Cybersecurity.

Table (9)
Strategic Issue Programs: Capacity Development Measures

Body/Vertical Section: Training and Development Fourth Strategic Issue: Capacity Development Measures Priority: high					
Time horizon	**2022**	**2023**	**2024**	**2025**	**2026**
Completion rate	**25%**	**55%**	**7%**	**7%**	**6%**
Strategic goals: • Increasing the number of courses and the number of trainees for cybersecurity professionals. • Develop educational programs or academic curricula to train skills and professions related to cybersecurity, such as (code analysts, digital forensics experts, incident responders, security architects, and penetration testers). • Reviewing research and development programs in the field of cybersecurity. • Supporting the national cybersecurity industry.			**Obstacles and limitations:** • Lack of necessary financial allocations. • Weakness of training curricula in this specialty. • Lack of trainers with experience and practice. • Volatility in the participation of trainees. • Lack of material and moral privileges for trainers.		
No	**Software**		**Measures**		
1	Capacity Development Program for Cyber Security Professionals		• Determining the job needs annually and the extent to which the current job cadres need training programs in order to work on providing them. • Determining the annual training need, as well as the type and specialization of courses curricula. • The number of specialized courses with modern curricula and some of these courses, to mention but not limited to (code analysts, digital forensics experts, accident responders, security architects, and penetration testers). • Qualifying the incoming trainers according to the latest training standards and focusing on the nomination of aspiring and willing elements to develop and develop their capabilities, which is reflected in the development of overall performance • Attracting external trainers with experience and specialization and using colleges and international training and development centers to organize some specialized training courses. • Activating coexistence activities and scholarships abroad for some distinguished employees in order to learn about the experiences of developed countries in the field of developing cyber capabilities.		

2	Cyber Security Research and Development Program	• Develop training curricula that will increase society's awareness of Cybersecurity. • Investing in national research and development programs in the field of Cybersecurity. • Urging participation in cyber scientific conferences, whether inside or outside Iraq. • Proposing educational curricula to train young people in Cybersecurity-related skills and professions, whether in schools, colleges, universities, or other educational institutions. • Submit research for competition at the directorate level annually.
The executing agency	**Follow-up**	**Success indicators**
Training and development + IT department + HR	Planning and follow-up + training and development	• Existence of a solid program for developing cyber capabilities. • Increasing the number of specialized courses. • Professional and qualified training staff. • Increasing the number of trainees. • Increase the capabilities and skills of employees.

As a result, the Communications Directorate must adopt detailed policy programs with the adoption of a series of procedures in order to achieve each of its organizational goals in line with the strengths and opportunities it possesses and in a manner that ensures the achievement of complete integration and harmony between all those goals to reflect the image of the greater goal or the supreme goal of Achieving the vision and mission of the Communications Directorate. In light of this, a set of strategic programs and some measures to achieve them have been developed through which the strategic objectives of the Communications Directorate are achieved to ensure addressing the strategic issues that were previously classified in light of the diagnosed strengths, weaknesses, opportunities and threats, concerning the most important obstacles that are expected to hurt the course of implementing these programs. In addition, the authorities concerned with implementing these programs and the time frames required for their implementation were identified in order to reflect a planned treatment strategy for the Communications Directorate for the coming future period as follows:

Discussion And Conclusions

The conclusions of the present study are of two levels. The first level is the level of application of the measures of the global Cybersecurity index. The second level is the level of the proposed strategy for Cybersecurity as follows:

First: The Conclusions of The Level of Application of The Measures of The Global Cybersecurity Index GCI.V4:2019 In the Directorate

The Global Cybersecurity Index GCI.v4 is a reliable reference that measures the extent to which countries are committed to Cybersecurity at the global level to raise awareness of the importance and dimensions of this issue because Cybersecurity has wide areas of application at various security, financial, health, social, scientific research, and other levels. The Global Cybersecurity Index GCI.v4 provides a set of measures to measure cyber performance distributed according to its legal, technical, regulatory, capacity development, and cooperative pillars. The level of cyber development for each country is measured according to these measures. These pillars have been adopted in the context of the present study in order to prove the level of application and

documentation of Cybersecurity requirements in the Communications Directorate.

Table (10)
Strategic Issue Programs: Cooperative Measures

Authority / Vertical Section: Planning, Follow-up and Related Sections Fifth Strategic Issue: Cooperative Measures Priority: high					
Time horizon	**2022**	**2023**	**2024**	**2025**	**2026**
Completion rate	**25%**	**55%**	**7%**	**7%**	**6%**

Strategic goals: • Establishment of bilateral agreements with advanced cyber countries. • Participation in international forums. • Establishing partnerships between the public and private sectors. • Create internal partnerships between agencies.	**Obstacles and limitations:** • Weak coordination with international bodies. • Not giving importance to international relations. • Less comprehensive field of Cybersecurity application.
No Software	**Measures**
1 Bilateral Agreement Program	• Formation of a working group for international agreements. • Coordination and conclusion of cooperative agreements with advanced foreign countries in cybersecurity to exchange information, experiences, technology and other resources. • Concluding international agreements on capacity development and coexistence to transfer external experiences to the reality of Cybersecurity in developed countries.
2 Participation program in international forums	• Participation in solid international forums and conventions such as the African Union Convention on Cyber Security and Protection of Personal Data and the Budapest Convention on Cybercrime.
3 Public-Private Partnership Program	• Establishment of public-private cooperative projects for the exchange of information, experience, technology or resources.
4 Inter-agency partnership program	• A formal partnership between the various government agencies (ministries, departments and other public sector institutions) exchange information, experiences, technology and other resources.
Performer / **Follow-up authority**	**Indicators of success**
Training and Development Information Technology Section Human Resources and other specialized sections / Planning and follow-up	• High-level national and international coordination. • Increase in the number of international cooperative conventions. • Public-private partnerships. • Increased number of external courses as a result of cooperative conventions. • An increase in the number of internal courses as a result of cooperative conventions.

The Communications Directorate suffers from a gap in the level of application and documentation of legal measures as a result of the non-voting and ratification of the Law of

Communication and Information, Information Crimes, and Personal Data Protection, which resulted in the difficulty of establishing response mechanisms in the investigation of cybercrime, prosecuting its perpetrators and imposing penalties for non-compliance, violation of the sovereignty of national cyberspace, or violation of the law. The Communications Directorate suffers from a gap in the level of application and documentation of technical measures due to the lack of sufficient financial allocations for the preparation of modern technology devices and equipment, the lack of qualified specialized technical personnel, and the lack of readiness of the national electronic infrastructure, which hampered the process of establishing a national Cybersecurity authority that warns and responds to electronic accidents.

There is a significantly low level of application and documentation of regulatory measures due to the lack of approval of the national strategy for Cybersecurity in Iraq, the failure to adopt measures to assess and measure the level of cyber risks, which negatively affected the process of preparing the national strategy for Cybersecurity at the national and sectoral levels, and the difficulty of determining the agency responsible for implementing, evaluating, and following up the strategy.

The Communications Directorate suffers from a gap in the level of implementation and documentation of capacity development measures that reaches (80%) as a result of the implementation and partial documentation of Cybersecurity awareness campaigns, the weakness of modern training curricula that are specialized in Cybersecurity, and the lack of specialized training personnel and the absence of the national Cybersecurity industry, which led to difficulty in building human and institutional capacities to increase awareness and knowledge of Cybersecurity to develop and support Cyber security professionals. The level of response to implementation and documentation of cooperative measures reached (50%); Because there are partial agreements for cooperation in cybersecurity and participation between the public and private sectors and local companies in the field of Cybersecurity. However, it is necessary to strengthen cooperation in this field in order to develop stronger cyber capabilities in order to deter repeated and continuous threats and reach a better and more professional investigation. It was found that the Directorate has an overall gap in the extent of the application and documentation of Cybersecurity measures at a rate of (78.8%) and an achieved application rate of (21.2%).

Second; The Conclusions of The Proposed Strategy for Cybersecurity

The Communications Directorate has the intention to develop the appropriate cyber legislation and submit it to the legislative authority after evaluating it by legal experts, which has supported the law enforcement process against cybercrime operations and their optimal investigation. The Directorate has an efficient technical staff of programmers, engineers, and designers, who are assigned tasks to complete the work and prepare and design programs that require electronic work to achieve the Directorate's goals to serve the public interest. It turned out that the directorate tends to participate in the formulation, implementation, and evaluation of the national Cybersecurity strategy to meet the requirements of the global Cybersecurity index and the approval of an agency tasked with auditing and reviewing the strategy. It was found that the Directorate intends to adopt internationally and globally accredited programs by the International Telecommunication Union or the ISO organization to develop the Cybersecurity aspect to keep pace with the pace of development in the field of Cybersecurity and progress within the global Cybersecurity index for countries. The Directorate has partnerships with the public and private sectors in information exchange, capacity development, and benefiting from the experiences of attacks and how to address them.

It was found that the Directorate faces obstacles on the legal side due to the lack of approval of the Information Crimes Law, the Communications and Information Law, and the Personal Data Protection Law, which made it difficult to prosecute and investigate the attackers easily. It turned out that the Directorate has a weakness in the technical aspect due to the lack of modern technical devices, the lack of financial allocations to them, and the lack of qualified technical staff, which made it difficult to detect loopholes and respond to cyber incidents and investigate them. There is confusion in the cyber regulatory aspect of the Directorate due to the non-approval of the national Cybersecurity strategy in Iraq and the reliance of the team responsible for cyber coordination on approximate information, which led to the cyber retreat and weakness of the internal information security system. The Directorate does not have cyber awareness campaigns. It also suffers from a lack of training personnel in Cybersecurity and the lack of studies and research

in Cybersecurity development, which negatively affected the development of capabilities, enhancing its electronic capabilities, and spreading cyberculture among members of society.
It was found that the Directorate has limited agreements in the field of international cyber cooperation and limited participation in international cyber activities, which led to the absence of the element of international competition, the accumulation of problems in this field, and the lack of insight into the experiences of other countries to solve such problems. It is clear that the Directorate has opportunities for the external environment that supports legal legislation for Cybersecurity through continued government support in approving communications and information laws, the cybercrime law and the personal data preservation law, as well as benefiting from the experiences of developed countries in the field of cyber legislation, as well as recognizing that the Iraqi cyberspace is a sovereign space.
There are opportunities for the Directorate to enable it to benefit from the technical experiences of countries in the field of Cybersecurity by allocating funds to develop the technical aspect, setting up an indicative program on cyber threats, and raising people's awareness of how to deal with them. The directorate has opportunities to develop regulatory measures by adopting a national Cybersecurity strategy by reviewing countries' Cybersecurity strategies and using them in evaluating the current strategy before approving it, as well as identifying an agency that is responsible for following up and evaluating the strategy. In addition, there is an opportunity to attract competencies specialized in strategic planning and adopting international measures to assess the level of development of Cybersecurity.
It was found that the Directorate has opportunities in the field of supporting the development of cyber capabilities as a result of the continuous wheel of cyber progress in the world, which allowed the Directorate to attract local and external training competencies that are specialized in Cybersecurity, the possibility of instructing higher education institutions to increase scientific research activities in the cyber side, as well as planning the development of educational curricula in the field of Cyber security. The Directorate has opportunities in the external environment that enable it to increase cooperation in the field of Cybersecurity through establishing local, regional, and global partnerships in the field of exchanging non-sensitive information, exchanging security information, as well as developing cyber capabilities and benefiting from experiences in this field, which contributes to the development of the national Cybersecurity system. The directorate faces challenges on the legal level as there is a possibility of an increase in the number of cyber-attacks from phishing, forgery, hacking, and abuse through social media platforms without any deterrent position due to the reluctance to introduce and vote on legal legislation.
On the technical level, it was found that threats are facing the Directorate in the external environment represented by the difficulty of detecting loopholes and how to deal with them, as well as the lack of community awareness in the field of Cybersecurity, which caused many gaps that are difficult to address. There are also challenges in the speed of development of malicious programs and how to implement procedures to prevent the import of prohibited devices in the technical aspect and the absence of the national industry of technical devices.
Organizational challenges are facing the directorate represented by the organizational decline at the cyber level, the weakness of the information security system, and the possibility of increasing Cybersecurity risks as a result of not adopting Cybersecurity assessment criteria. On the side of developing cyber capabilities, the Directorate faces challenges, represented by the lack of cyber training staff, as well as the lack of government incentives to encourage the development of cyber capabilities, and most importantly, the weak support for cyber educational programs in primary, secondary, and higher education, which resulted in the absence of the national Cybersecurity industry. The directorate faces threats in the cooperative pillar represented by the accumulation of cyber problems, the lack of an independent cyber body to take care of this, challenges at the level of international competition in the field of Cybersecurity, and the lack of a database of information related to cyber-attacks and threats in all sectors, as well as lack of international participation.

References

Allison, M., & Kaye, J. (2015). *Strategic Planning for Nonprofit Organizations: A Practical Guide for Dynamic Times* (3rd ed.): John Wiley & Sons.

Barad, M. (2018). Definitions of strategies *Strategies and Techniques for Quality and Flexibility* (pp. 3-4): Springer.

Brookson, C., Cadzow, S., Eckmaier, R., Eschweiler, J., Gerber, B., Guarino, A., . . . Górniak, S. (2015). Definition of Cybersecurity-Gaps and overlaps in standardisation. *Heraklion, ENISA*.

Bryson, J. M., & Alston, F. K. (2011). *Creating your strategic plan: A workbook for public and nonprofit organizations* (3rd ed. Vol. 3): John Wiley & Sons.

BÜTÜNER, H. (2016). *Case Studies in Strategic Planning.*: Taylor & Francis Group, LLC, NW.

David, F., & David, F. (2015). Strategic Management Concepts and Cases 15th ed. Harlow (15th ed.): United Kingdom: Pearson Prentice Hall.

Dimitriou, H. T., & Thompson, R. (2007). Strategic thought and regional planning: the importance of context *Strategic Planning for Regional Development in the UK* (pp. 92-116): Routledge.

Drucker, P. F. (1954). *The practice of management: A study of the most important function in America society*: Harper & Brothers.

FAS, F. O. A. S. (2018). Cybersecurity. from https://fas.org/

Geers, K. (2011). *Strategic cyber security*: Kenneth Geers.

ITU. (2018). Guide to developing a national cybersecurity strategy - strategic engagement in cybersecurity. *Geneva, Switzerland: International Telecommunication Union*.

Maurer, T., & Morgus, R. (2014). *Compilation of existing cybersecurity and information security related definitions*: Federal Department of Foreign Affairs, Switzerland

Mbulwa, J., & Kinyua, G. (2020). The Role Of Strategy Formulation On Service Delivery: A Perspective Of Turkana County In Kenya. *International Journal of Innovative Research and Advanced Studies, 8*(3), 8.

Narayanan, V. K., & Fahey, L. (1982). The micro-politics of strategy formulation. *Academy of Management Review, 7*(1), 25-34. doi: https://doi.org/10.5465/amr.1982.4285432

Nickols, F. (2016). Strategy, strategic management, strategic planning and strategic thinking. *Management Journal, 1*(1), 4-7.

Pettigrew, A. M. (1977). STRATEGY FORMULATION AS A POLITICAL PROCESS. *International studies of management & organization, 7*(2), 78-87.

Prasad, R., & Rohokale, V. (2020). *Cyber Security: The Lifeline of Information and Communication Technology* (1 ed.): Springer.

QUINN, J. B., Mintzberg, H., & James, R. (1995). The strategy concept. *The Strategy Process, European edn. London: Prentice Hall*.

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. *IEEE Security & Privacy, 16*(3), 96-102. doi: https://doi.org/10.1109/MSP.2018.2701150

Simerson, B. K. (2011). *Strategic planning: A practical guide to strategy formulation and execution*: Abc-clio.

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security, 26*(1), 2-9. doi: 10.1108/ICS-04-2017-0025

Webster Jr, F. E. (2009). Marketing IS management: the wisdom of Peter Drucker. *Journal of the Academy of Marketing Science, 37*(1), 20-27. doi: https://doi.org/10.1007/s11747-008-0102-4

Wheelen, T. L., Hunger, D. J., Hoffman, A. N., & Bamford, C. E. (2018). *Strategic management and business policy : globalization, innovation and sustainability*.