Dr. Rehab Hosny Al-Rahmawy

Ingénieure Électricienne en Télécommunications
à l'Autorité Nationale des Médias

Gestion des Risques Cybernétiques
dans le Domaine *Économique*

Introduction:

L'économie mondiale connaît plusieurs changements et transformations dans son entrée dans le monde numérique. Au cours des trente dernières années, la dépendance des gouvernements, des entreprises et des citoyens vis-à-vis d'Internet et des technologies de l'information et de la communication s'est considérablement accrue, formant un cyberespace qui reflète les données et les économies des États, mais sous la forme d'informations numériques très sensibles, simulant la réalité économique de ceux-ci, en particulier les pays qui se sont fortement immergés dans le travail informatisé, et se sont engagés dans la modernité de l'information, ce qui en a fait une arène pour la cybercriminalité, et ce conflit s'est répercuté sur la sphère économique avec le contrôle, la manipulation de son contenu. Les pays qui ont produit cette technologie sont devenus les plus exposés aux risques cybernétiques, ainsi qu'à la difficulté d'adhérer aux exigences du maintien de leur sécurité nationale.

De nombreux pays et leurs institutions et entreprises sont confrontés à des risques cybernétiques affectent le domaine économique de l'État, ce qui les a amenés à partager un certain niveau de responsabilité dans la gestion de ces risques, de sorte que les pays et les entreprises doivent d'abord se rendre compte que leur stratégie et leur programme numériques doivent être basés sur une approche disciplinée pour faire face et comment gérer les risques cybernétiques. L'inaction et l'incapacité à prendre les mesures appropriées les exposent à de grands risques. La cybermenace augmente également en raison de la disponibilité d'un marché pour les logiciels malveillants, les outils, les services illicites et les données sensibles qui ne sont pas accessible au public (et abordable). La sécurisation des données est devenue un enjeu majeur pour la sphère économique, cependant, la plupart des organisations n'ont pas pris de mesures pour améliorer leurs compétences en cybersécurité.

La transformation rapide vers une économie numérique mondiale entraîne une augmentation des cyberattaques de jour en jour et devient plus complexe et influente, ce qui nous oblige à affronter et à gérer ces risques cybernétiques afin que nous puissions formuler une nouvelle réalité économique numérique sécurisée, qui renforce l'importance pour les pays de bien sécuriser leurs systèmes et entités et de travailler à gérer les risques cybernétiques dans le domaine économique pour atteindre la sécurité nationale par une méthode administrative pour faire face à ces risques cybernétiques. De nombreuses institutions et organisations souffrent de l'incapacité administrative à répondre aux risques cybernétiques, d'où cette étude qui vise à éclairer la façon de gérer les risques cybernétiques dans le domaine économique.

Problème d'étude :

Le problème de l'étude est l'identification des risques cybernétiques et leurs effets négatifs sur la

sphère économique des pays et de leurs institutions et organisations, d'autant plus que de nombreux pays recherchent actuellement la transformation numérique, qui a été un domaine de cyber percées et de vulnérabilité aux cyberattaques qui nécessitent la gestion de ces risques cybernétiques afin de ne pas entraîner de pertes dans la sphère économique des pays, leurs institutions et organisations économiques et à la sécurité nationale.

L'importance de l'étude :

L'importance de l'étude vient du point de vue de la menace posée par les risques cybernétiques au domaine économique des pays, de leurs institutions et des organisations qui menacent leur sécurité nationale, en particulier avec la transformation des gouvernements à l'économie numérique, les risques cybernétiques ont émergé pour menacer ces réalisations, et donc il est nécessaire de faire la lumière sur ces risques cybernétiques, et leur impact sur le domaine économique des pays, et comment gérer leurs risques cybernétiques pour les pays, et au sein des organisations et des institutions, pour atteindre la sécurité nationale des pays.

Objectif de l'étude :

Aboutir à une proposition de stratégie de gestion des risques cybernétiques dans le domaine économique des pays.

Méthodologie de l'étude :

L'approche descriptive et analytique a été suivie pour analyser comment gérer les risques cybernétiques pour le domaine économique, et déterminer l'impact de ses risques sur le domaine économique des pays, des institutions et des organisations, afin de tenter de répondre à la question principale de cette étude, à savoir :

Comment les pays peuvent-ils gérer les risques cybernétiques dans le domaine économique pour eux-mêmes et pour leurs organisations et institutions afin d'assurer la sécurité nationale?

Dans l'ordre de ce qui précède, cette étude sur la gestion des risques cybernétiques dans le domaine économique s'articule autour de cinq axes :

Le premier axe: le cadre théorique et conceptuel de l'étude..

Le deuxième axe : l'impact des risques cybernétiques sur le champ économique.

Le troisième axe : les procédures de gestion des risques cybernétiques dans le domaine économique.

Quatrième thème : Les principales caractéristiques d'une proposition de stratégie de gestion des risques cybernétiques dans le domaine économique.

Le premier axe :
Cadre théorique et conceptuel de l'étude

Premièrement : La notion des risques cybernétiques :

Les risques cybernétiques désignent les risques opérationnels liés aux actifs et aux technologies de l'information qui entraînent des conséquences qui affectent la confidentialité, la disponibilité ou l'intégrité de l'information ou des systèmes d'information. Par rapport aux catégories de risques couvertes par l'assurance. Les risques cybernétiques sont cohérents en termes de caractéristiques et de responsabilité, avec des risques de biens et de responsabilité, ainsi que des risques catastrophiques et opérationnels(1).

Deuxièmement : la classification des risques cybernétiques :

Les risques cybernétiques dans le domaine économique sont classés en deux types : les risques procéduraux et les risques techniques comme suit :

1- Risques procéduraux :

A- Responsabilité : L'absence d'un organisme chargé du cyberespace et de la protection de l'information.

B- Classification : L'absence de classification des informations, sur la base de laquelle les informations sont classées en fonction de leur importance.

C- Politiques stratégiques : L'absence de politiques et de stratégies dans le cyberespace, ou l'absence de mise en œuvre intégrale si elles sont disponibles.

D- Les cadres humains : le manque de compétences et de cadres nationaux formés et l'absence de sensibilisation à la cybersécurité dans les couches de la société(2).

Risques techniques :

A- Perte : Il s'agit de la perte d'informations résultant de leur effacement ou de leur endommagement.

B- Destruction et sabotage : Il s'agit de la destruction et du sabotage d'informations par quelque moyen que ce soit en raison de parties internes ou externes et dont le but est d'empêcher définitivement l'accès à l'information.

C- Fuite : Il s'agit de la fuite d'informations provenant de la principale source de préservation.

D- Changement : Il s'agit de la modification des données dans le but de les falsifier ou de

communiquer de fausses informations qui saboteraient les informations.

E. Brouillage : Il s'agit du blocage temporaire de l'accès à l'information.

F- Obsolescence : C'est l'absence de mise à jour de l'information pendant un certain temps, qui conduit à réduire la valeur de l'information et à donner des résultats inexacts [3].

Troisièmement : La relation entre la cybersécurité et l'économie :

La relation entre l'économie et la cybersécurité s'est entremêlée dans le processus de transformation numérique auquel de nombreux gouvernements vont s'attaquer pour saisir les capacités de la quatrième révolution industrielle. La question de la lutte contre les risques cybernétiques est devenue un enjeu particulier dans le domaine économique à l'ère numérique des enjeux émergents. De nouveaux intérêts et menaces liés à la cybersécurité sont apparus avec l'utilisation croissante du cyberespace, de la prestation de services et de l'accumulation de richesse, ainsi que les répercussions négatives de l'absence ou de la faiblesse de la cybersécurité sur l'économie, en particulier l'économie numérique.

Cela s'inscrit dans le cadre de la relation directe qui combine les deux dimensions, et de son impact sur les taux de confiance dans l'environnement numérique, l'offre numérique, la demande numérique et l'infrastructure de l'information. En particulier avec l'augmentation des risques cybernétiques dans l'environnement numérique, et en même temps le renforcement du rôle de l'économie numérique dans la croissance économique, ce qui a incité les pays à augmenter les dépenses dans le domaine de la cyberdéfense et à allouer des ressources dans le budget général de l'État ou dans son budget pour la sécurité et la défense, à la lumière des défis renouvelés posés par les processus de transformation numérique. Et ses applications économiques, qui ont conduit à un changement quantitatif et qualitatif des éléments de la richesse et des ressources économiques et des fondements de l'offre et de la demande.

La perspective économique de la cybersécurité confirme que les acteurs des gouvernements, des entreprises ou des utilisateurs ont des exigences et des intérêts de sécurité différents selon la nature de l'utilisation, et que ce conflit d'intérêts et d'intérêts doit être soumis à des normes d'autocontrôle, que ce soit en surveillant certains ou en prenant des réactions basées sur des incitations qui déplacent les motivations de chaque partie [4].

Quatrièmement : Gestion des risques cybernétiques :

La gestion des risques cybernétiques est généralement introduite sous la forme d'un processus, et les étapes comprennent les éléments suivants :

Identification, analyse, évaluation, surveillance et audit des risques.

La gestion des risques comprend l'application d'une méthode logique et systématique pour identifier, analyser, évaluer, traiter et surveiller les risques de manière à permettre aux organisations de réduire les pertes et de maximiser les gains. La gestion des risques peut être appliquée à de nombreux niveaux de l'organisation ; elle peut être appliquée aux niveaux stratégique et opérationnel[5].

Il est essentiel d'établir une voie pour gérer les risques émergents et réagir rapidement et efficacement afin d'assurer une intervention simplifiée et de veiller à ce que tout risque potentiel soit atténué autant que possible, et à ce que les stratégies d'intervention et les processus de gestion soient mis en œuvre de manière proactive[6]. Les processus de gestion des risques sont menés selon les étapes suivantes :

1- Identifier les risques cybernétiques :

L'organisation identifie les risques cybernétiques potentiels qui peuvent avoir une incidence négative sur un processus ou un projet particulier qu'elle entreprend, l'environnement commercial et les facteurs contributifs qui peuvent causer des risques cybernétiques et les causes profondes des risques cybernétiques doivent être identifiés, et ses risques sont décrits et l'objectif de ses risques et des menaces auxquels l'organisation est confrontée doit être déterminé. L'évaluation proactive s'appuie sur des données pertinentes, des tendances et des événements actuels[7], et les risques peuvent être cernés à partir de diverses sources comme suit :

A- Échange d'idées avec du personnel opérationnel expérimenté.

B- Elaboration de scénarios de risques.

C- Programmes d'analyse de données.

D. Enquêtes de sécurité et examens de la sécurité dans le contrôle des procédés.

E- Compte rendu d'enquêtes sur les accidents.

F- Les facteurs organisationnels, tels que les politiques de l'institution, de l'organisation ou de l'entreprise en matière de recrutement et de formation, la rémunération et l'allocation des ressources.

G- Les facteurs de l'environnement opérationnel, tels que le bruit et les vibrations ambiants,

la température, l'éclairage et l'équipement de protection, les facteurs humains tels que les conditions médicales, les limites de la performance humaine et l'interface homme-machine.

H- Les facteurs de conformité réglementaire tels que l'applicabilité des règlements et l'approbation de l'équipement, du personnel et des procédures.

- Outils d'identification des risques cybernétiques potentiels :

Listes de contrôle, enquêtes, inspections personnelles et opinions d'experts qui dépendent de la conscience de l'expert et de l'ampleur du risque, et de la méthode de circulation des idées, dans le sens de faire une combinaison de ce qui précède pour obtenir les meilleurs résultats, et parmi les moyens d'identifier les risques, il y a aussi le brainstorming - SWOT - questionnaires sur les risques - ateliers - analyse des risques - évaluation des risques - politiques de traitement des risques - surveillance et suivi des risques(8) Présent dans le Forum.

2- Analyse des risques cybernétiques :

L'analyse des risques est la prochaine étape du processus de gestion des risques, mais elle peut également être la première étape s'il y a des risques identifiés par d'autres moyens que l'évaluation des risques, et l'objectif principal de l'analyse des risques est l'évaluation, une fois que des types spécifiques de risques sont identifiés, l'organisation détermine sa classification, ses priorités, ses contrôles et ses niveaux de risque, puis la probabilité de leur occurrence ainsi que leurs conséquences. L'objectif de l'analyse de ces risques est d'accroître la compréhension de chaque cas spécifique de risque et de la manière dont il peut affecter les objectifs stratégiques de l'organisation.

Les cinq (9) étapes du processus d'analyse des risques peuvent être illustrées comme suit :

A- Une description claire des risques :

Il devrait y avoir une brève déclaration décrivant ce que sont les risques cybernétiques et comment ils pourraient affecter l'atteinte des objectifs, et l'équipe d'examen des risques devrait s'entendre sur l'étendue du risque, puis décrire le scénario de risque, en précisant à quoi ressemble l'événement à risque potentiel.

B- Causes des risques :

« Pourquoi ce danger se produit-il ?» Outre les causes directes du risque, nous devons également bien comprendre les causes profondes et les principaux facteurs afin de réduire efficacement la probabilité de risque.

C- Contrôles préventifs :

Une fois que nous avons compris les causes profondes, nous devons nous mettre d'accord sur les contrôles qui existent déjà et qui aident à réduire la probabilité que ces causes ou facteurs se produisent, et déterminer des contrôles supplémentaires que nous pouvons mettre en place pour réduire davantage la probabilité ; les organisations qui suivent une stratégie proactive de gestion des risques pour la sécurité croient qu'elles peuvent réduire les risques cybernétiques en cernant les vulnérabilités et en prenant des mesures pour réduire les conséquences négatives des risques émergents.

D. Conséquences des risques :

L'identification de ces conséquences potentielles à l'avance aide à élaborer des plans d'urgence en cas de danger.

E- Commandes d'inclinaison :

- Quels contrôles devraient être appliqués pour aider à minimiser l'impact des conséquences ?
- Quels contrôles supplémentaires peuvent être mis en place pour réduire davantage l'impact ?

3- Évaluation des risques cybernétiques :

Le service concerné met en œuvre des procédures d'évaluation des risques cybernétiques au minimum dans les cas suivants :

A- Dans les premières étapes des projets techniques.

B- Avant d'opérer un changement fondamental dans la structure technique.

C- Lors de l'intention d'obtenir les services d'un tiers.

D- Lors de la planification et avant le lancement de nouveaux produits et services techniques.

L'évaluation des risques comprend :

Menace et vulnérabilité, ainsi qu'en analysant et en tenant compte des facteurs atténuants applicables(10), le volet évaluation des risques a pour objectif de recenser :

A- Menaces contre les organisations, c'est-à-dire les opérations, les biens, les individus ou les menaces dirigées par les organisations contre d'autres organisations.

B- Faiblesses à l'intérieur et à l'extérieur des organisations.

C. Dommages causés (c.-à-d. effets préjudiciables) qui peuvent survenir compte tenu de la probabilité de menaces.

D. La probabilité de dommages.

Le praticien analyse les risques cybernétiques pour déterminer la probabilité que les événements de menace et les conditions vulnérables entraînent des

effets négatifs sur l'origine du système, et de même, le praticien analyse la valeur d'impact et calcule le risque d'exposition à l'aide de la méthodologie spécifiée dans la stratégie de risque d'entreprise, telle que (probabilité de risque x impact du risque). Par conséquent, l'analyse des causes profondes (en pensant aux événements précédents qui ont déjà conduit à un événement). Il aide à examiner les conséquences potentielles d'événements futurs et à documenter la séquence des résultats qui peuvent survenir après le début d'un événement de menace, et bien que le jugement d'un expert soit précieux pour estimer les facteurs de risque, une façon de réduire la subjectivité est de compléter ce jugement à l'aide de modèles de simulation(11) .

Les risques cybernétiques devraient être réévalués et mis à jour comme suit :

A- Périodiquement pour toutes les informations et tous les actifs techniques, et au moins une fois par an pour les systèmes sensibles.

B- Après qu'un incident de cybersécurité a porté atteinte à l'intégrité, à la disponibilité et à la confidentialité des informations et des actifs techniques.

C. Après avoir obtenu des résultats d'audit importants ou des informations proactives.

D. En cas de modification des informations et des moyens techniques.

Le processus d'évaluation des risques cybernétiques devrait couvrir :

A- Analyse des risques cybernétiques: Le (Département Cybersécurité) doit évaluer la probabilité d'occurrence des risques et menaces et des effets qui en découlent, et utiliser les résultats de cette évaluation pour déterminer le niveau général de ces risques. Le (Département Cybersécurité) doit adopter une méthodologie quantitative ou qualitative pour effectuer l'analyse des risques.

B- Évaluation des risques cybernétiques: Le (département concerné par la cybersécurité) doit estimer l'ampleur des risques cyber conformément aux critères d'évaluation des risques institutionnels approuvés au « nom de l'entité » et déterminer les modalités de traitement de ceux-ci en fonction de la priorité (12).

4- Aborder ou répondre aux risques cyber :

La réponse aux risques cybernétiques consiste à déterminer et à évaluer un ensemble d'options pour traiter et évaluer ses risques, ainsi qu'à préparer et à mettre en œuvre des plans de remédiation des risques, y compris l'évitement, la réduction de la probabilité d'occurrence, la minimisation des conséquences, le transfert et la conservation des risques(13).

La Direction de la cybersécurité doit déterminer les options pour faire face aux risques cybernétiques selon les étapes suivantes :

A- Traitement ou réduction des risques : Aborder ou réduire le degré de risque par l'application des contrôles de sécurité nécessaires pour réduire la possibilité d'occurrence ou d'impact, ou les deux, qui aident à contenir et à maintenir les risques à des niveaux acceptables.

B- Éviter les risques : Se débarrasser du risque en évitant de perpétuer la source du danger en faisant ce qui suit :

- Partage ou transfert des risques : partager les risques avec un tiers qui a le potentiel de mieux gérer les risques, ou assurer les informations et les actifs techniques en cas d'exposition aux risques cybernétiques.
- Tolérance au risque : Le niveau de risque est acceptable, mais doit être surveillé en permanence en cas de changement.

Les options de réponse au risque cybernétique comprennent : la tolérance et sont appropriées seulement lorsqu'elles sont acceptables lorsque la perte ou le dommage est survenu/conservé, traité/réduit au minimum et transporté (et sont basées sur la fourniture d'une orientation aux personnes sur la façon de s'assurer qu'aucune perte ne se produit, mais dépend des personnes qui suivent des systèmes de travail sûrs bien établis), la résiliation et l'évitement (par la mise en œuvre de contrôles préventifs appropriés). La réaction aux risques est plus critiquée comme étant un leadership correctif à ce jour que préventif, comme dans le format suivant.

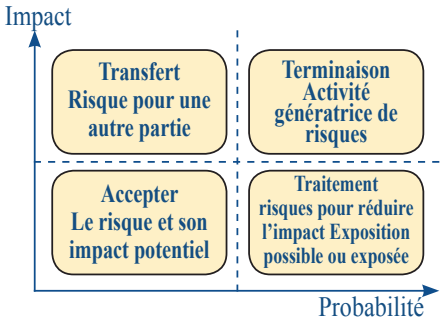

Schéma illustrant les options de réponse aux risques (14)

Au cours de cette étape, l'organisation évalue les risques cybernétiques les mieux notés, les traite de manière positive et élabore un plan d'atténuation à l'aide de contrôles de risque spécifiques, et ces plans comprennent des opérations d'atténuation des risques, des tactiques de prévention des risques et des plans d'urgence en cas de risque (15).

5- Suivi des risques cybernétiques :

Il fait partie du plan d'atténuation basé sur le suivi de tous les risques cybernétiques, de la surveillance et du suivi continu des risques cybernétiques ,en plus de l'examen du processus complet de gestion des risques et de sa mise à jour en fonction des situations différentes et changeantes, et les risques sont examinés sur une base trimestrielle, de l'identification des nouveaux risques et des changements existants, de la mise à jour du registre des risques et de l'évaluation des mesures prises par les détenteurs de risques pour gérer les risques et corriger les performances inappropriées [16].

Afin de surveiller les risques cybernétiques, le département Cybersécurité doit préparer et tenir à jour un registre des risques pour documenter les résultats du processus de gestion des risques cybernétiques, à condition qu'il comprenne au minimum les informations suivantes :

A. Le processus d'identification des risques.
B. Étendue du risque.
C. Le responsable ou le détenteur du risque.
D. Une description des risques, y compris leurs causes et effets.
E. Analyse des risques montrant leurs effets et leur échelle de temps.
F. L'évaluation et la classification des risques qui comprennent la probabilité, l'ampleur et la classification globale des risques s'ils se produisent.
G. Le plan de gestion des risques comprend la procédure à suivre pour les traiter, la personne qui en est responsable et leur calendrier.
H. Description du danger résiduel.
I. Le département Cybersécurité recueille les éléments de preuve relatifs à l'état des risques cybernétiques et les examine périodiquement.

6- Niveau de risques cybernétiques acceptable:

Cela se fait comme suit :

A- Les critères d'acceptation et de documentation des risques cybernétiques doivent être déterminés, en fonction du niveau de risque, et du coût de la prise en charge du risque par rapport à son impact, en déterminant l'ampleur de l'impact du risque, où chaque risque [17] est classé dans l'un des cas suivants:
- Les risques ayant un impact significatif, et des actions et des plans doivent être élaborés pour y faire face.
- Les risques ayant un impact significatif, qui doivent être étudiés et planifiés.
- Les risques d'impact moyen, qui peuvent être pris en compte.
- Risques à faible impact, pour lesquels aucun plan spécifique n'est requis.
- Risques à très faible impact, pour lesquels des plans spécifiques ne nécessitent pas l'élaboration de plans spécifiques.

B-Des contrôles supplémentaires devraient être mis en œuvre afin de ramener le risque à un niveau acceptable si le risque restant ne satisfait pas aux critères d'appétence au risque.

C- En cas de dépassement des critères d'appétit pour le risque, le titulaire de l'autorité doit être invité à prendre les actions ou les décisions nécessaires.

D- Les procédures de gestion des risques de cybersécurité devraient être mises à jour à intervalles réguliers (ou en cas de modification des exigences législatives et réglementaires et des normes connexes).

E- La politique de gestion des risques liés à la cybersécurité devrait être révisée annuellement.

7- La surveillance des risques cybernétiques :

Elle repose sur la surveillance des nouveaux risques et des réalisations continues à ajouter au processus de gestion des risques cybernétiques en permanence [18].

L'objectif du volet contrôle des risques est le suivant :

A-Déterminer l'efficacité continue des réponses aux risques (conformément au cadre réglementaire de gestion des risques).

B- Identifier les changements qui affectent les risques et les environnements dans lesquels les systèmes fonctionnent.

C-Vérifier que les réponses aux risques prévues sont mises en œuvre et que les lois, les directives, les règlements, les politiques, les normes et les lignes directrices sont respectés[19]

Le deuxième axe

L'impact des risques cybernétiques sur le champ économique :

La relation entre sécurité et technologie s'est accrue, les intérêts stratégiques de l'État étant de plus en plus exposés aux risques cybernétiques et même menacés de transformer le cyberespace d'un intermédiaire et d'une source de nouveaux outils pour les conflits internationaux[20].

Les risques cybernétiques plus importants pour le domaine économique sont les suivants :

1- Manipuler l'information d'un système particulier, la déformer ou la détruire, que ce soit par piratage ou propagation de virus.

2- Les délits de droit commun qui utilisent Internet, pour le vol, la fraude, l'usurpation

d'identité, la violation de la propriété intellectuelle et autres.

3- Les crimes qui entrent dans le cadre du crime organisé, qui menacent la sécurité des individus et des États, tels que le blanchiment d'argent et le terrorisme...etc., comme les menaces de sécurité du système de ransomware, un outil criminel qui s'est répandu en ligne depuis plusieurs années, ne cessant d'évoluer et impliquant à la fois les individus et les économies au niveau individuel.

4- Les risques des technologies intelligentes telles que les crypto-monnaies qui peuvent conduire à l'effondrement de l'économie, facilitant la commission de crimes car ils sont difficiles à suivre car ils sont cryptés et facilitent le processus de blanchiment d'argent, ainsi que l'utilisation de l'ingénierie sociale qui est un des moyens de connaître les comptes bancaires de la cible elle-même(21) .

5- Les cyberattaques peuvent viser l'arrêt complet d'Internet dans le pays cible, ce qui entraîne l'arrêt des transactions bancaires, des transactions e-gouvernementales et le vol des numéros et des détails de carte de crédit qui sont commercialisés en ligne, ce qui entraîne la perturbation du flux d'argent dans le pays, et donc la cessation des secteurs les plus importants du pays tels que l'industrie et d'autres secteurs de l'État. Il est possible que les transactions échouent en raison de la rétention de liquidités, et que les familles et les entreprises perdent leur capacité à accéder aux dépôts et aux paiements, et dans un scénario aussi grave, les investisseurs et les déposants réclament leur argent ou tentent d'annuler leurs comptes ou d'autres services et produits qu'ils utilisent habituellement.

6- Les outils de piratage sont maintenant moins chers, plus accessibles et plus puissants, ce qui permet aux pirates ayant des compétences limitées d'infliger davantage de dommages contre une petite partie du coût précédent, et l'expansion des services mobiles (la seule plateforme technologique disponible pour beaucoup) augmente les possibilités de piratage, et les attaquants ciblent des entreprises grandes et petites, des pays riches et pauvres et travaillent au-delà des frontières. La lutte contre la cybercriminalité et la réduction de ses risques doivent donc être une responsabilité partagée entre les pays et au sein des pays(22).

7- Des acteurs individuels peuvent lancer des cyberattaques pour voler de l'argent sur des comptes bancaires individuels. Des États rivaux et des adversaires idéologiques peuvent viser à obtenir des données classifiées, provoquer des perturbations dans les systèmes financiers et provoquer la panique parmi les citoyens.

En raison de l'exposition du système économique des pays à de tels risques, il devait y avoir une sécurité nationale économique, car c'est le secteur de la sécurité le plus vulnérable aux cyberattaques, en raison de la transformation de l'économie mondiale vers une économie numérique basée sur les technologies de l'information, et donc l'exposition de ce système à de tels risques peut entraîner d'énormes pertes économiques et nationales, ce qui affecte la réalisation de la sécurité nationale de l'État, ce qui nécessite un travail sur la gestion des risques cybernétiques dans le domaine économique(23).

Troisième thème

Procédures de gestion des risques cybernétiques dans le domaine économique

Premièrement : Procédures techniques :

Les sources d'informations sensibles peuvent être protégées contre les cybers dangers en les gardant hors de vue ou à l'abri des regards des agresseurs en suivant les procédures suivantes :

1- Protection physique : comprend les éléments suivants :

A- La cybercensure qui ne donne pas la possibilité d'y accéder (hackers).

B- Des caméras de surveillance et de surveillance qui sont placées à différents endroits du bâtiment.

C- Une sécurité renforcée qui ne permet pas d'accéder à l'information.

2- Cryptage : Il se fait en mélangeant des informations numériques, de sorte qu'elles ne peuvent être réorganisées qu'à l'aide d'une clé spécifique, et les informations mélangées sont complètement incompréhensibles pour la personne qui n'a pas cette clé, et ce processus de mélange est connu sous le nom de cryptage, tandis que le processus de retour du message crypté à sa position d'origine est connu sous le nom de décodage et de renvoi.

3- Protection par composants : Cette méthode offre une protection presque complète contre le virus, en utilisant des appareils sans la mémoire utilisée, et les disques optiques peuvent être utilisés pour stocker des programmes de manière permanente, et ces disques sont en lecture seule, et ne peuvent pas y être écrits, ainsi que le stockage des systèmes d'exploitation sur ces disques, car cela leur fournit une protection contre les virus.

4- Nomination : L'une des méthodes utilisées par de nombreux partis pour se dissimuler derrière cela est ce qu'on appelle la nomination, qui est un moyen d'obtenir des informations sélectionnées à partir d'informations confidentielles sans divulguer les informations confidentielles elles-mêmes.

5- Contrôler l'élimination des déchets d'information : Cette procédure doit être appliquée avec précision et soin pour éviter les risques cybernétiques car il existe des programmes et des méthodes par lesquels des données peuvent être récupérées à partir de supports de stockage après balayage [24].

Deuxièmement : Procédures administratives:

Tous les pays insistent sur la préservation de leurs informations et leur protection contre le vol et le sabotage, et cette attention les a obligés à prendre, en plus des mesures techniques, certaines procédures administratives dans leurs centres, agences de leur personnel, et certaines de ces procédures sont les suivantes :

1- Définir les responsabilités : La responsabilité d'assurer la protection de l'information et d'éviter les risques cybernétiques incombe à trois parties importantes : le directeur des systèmes d'information, le responsable de la cybersécurité comme suit :

A- Chef de l'information : Applique strictement les procédures de sécurité pour assurer la confidentialité des informations de l'installation, et a la capacité d'effacer toutes les informations qu'il veut, d'établir des instructions d'utilisation et de donner l'autorité.

B- Responsable de la cybersécurité : Sa tâche est de contrôler le contenu du centre et est également responsable des dispositifs de cryptage.

C- Agent de cybersécurité : Responsable de la sélection et de l'examen des programmes, et de s'assurer qu'ils sont exempts de virus ou de cryptages pouvant profiter à l'ennemi ou aux falsifiant.

2- Déterminer les pouvoirs : L'une des difficultés auxquelles est confrontée la protection de l'information est l'accès des personnes de l'intérieur ou de l'extérieur de l'installation aux centres d'information, de sorte que les pouvoirs doivent être déterminés pour les personnes autorisées à accéder et à utiliser les informations et les bases de données, ainsi que l'établissement de règles qui déterminent les personnes ou les groupes qui ont accès à un certain type d'information. Cela nécessite de diviser les fichiers au sein du réseau informatique en certaines sections, afin que personne ne puisse accéder à une section non autorisée, et cela aide beaucoup à protéger les informations contre L'arrivée des saboteurs.

3- Protection des individus : Les travailleurs des centres d'information sont exposés à des attaques orchestrées par l'ennemi afin de paralyser leur capacité à protéger leurs informations, et il est donc nécessaire de protéger ces individus et de les immuniser contre les idées et les procédures de guerre psychologique menées par l'ennemi, et de consolider leur adhésion à leurs principes.

4- Maintenance du matériel : Les agents de maintenance du fabricant, ou ceux qui installent le système en continu, doivent être surveillés lorsqu'ils sont autorisés à accéder aux centres d'information pendant la maintenance, et ce problème est surmonté en remplaçant les travailleurs de maintenance de l'entreprise par des membres de l'installation qui sont formés pour effectuer des travaux de maintenance[25].

Quatrième thème

Les principales caractéristiques d'une proposition de stratégie de gestion des risques cyber dans le domaine économique :

Objectif de la stratégie proposée :

Assurer une croissance économique sûre en Égypte et la protéger de tout risques cybernétiques.

Piliers de la stratégie proposée :

La stratégie proposée repose sur plusieurs piliers Parmi les plus importants, citons :

1- Permettre aux entreprises internationales dans ce domaine d'entrer sur le marché égyptien et de fournir de nombreux services avancés.

2- L'Égypte se classe quatrième parmi les pays du Moyen-Orient et d'Afrique du Nord et 23e au niveau mondial en cybersécurité sur 182 pays avec un score de 95,45 sur 100.

3- Création du Conseil suprême pour la cybersécurité et du Centre Egy Cert pour la réponse aux urgences Internet et informatiques.

4- Adhésion de l'Égypte à certaines fédérations internationales et organismes concernés par la cybersécurité.

5- La cohésion et la préparation des forces armées et leur adoption de l'approche des armées électroniques modernes afin de faire face à la menace de la sécurité égyptienne développée et dépendante du cyberespace.

6- Réglementer la Banque centrale d'Égypte pour qu'elle utilise les monnaies numériques et empêche leur circulation.

7- Opérer un changement de nature de l'environnement des affaires pour tous les

secteurs économiques, alors que la demande de technologie d'assurance pour la cybersécurité contre les risques cybernétiques a doublé.

Déterminants de la stratégie proposée :

La stratégie proposée repose sur plusieurs déterminants Parmi les plus importants, citons :

1- La transition vers l'économie numérique est devenue un moyen d'aider davantage en matière de piratage et de cyberattaque.
2- L'augmentation relative du coût de l'application significative des techniques de sécurité des systèmes d'information et du cyberespace.
3- La difficulté d'appliquer les contrôles de sécurité des systèmes d'information et du cyberespace en raison de la faible culture de la cybersécurité chez certains travailleurs de certains secteurs, notamment financier et bancaire.
4- La nécessité d'un mécanisme de contrôle clair sur tous les secteurs, en particulier les banques et les sociétés financières, pour s'assurer qu'il existe des contrôles et des politiques pour atteindre la cybersécurité et gérer ses risques.
5- Le sous-développement, l'ignorance, l'analphabétisme et les pressions de la croissance qui pèsent sur les épaules de la société à travers la pauvreté, l'analphabétisme et la criminalité, qui limitent tous les possibilités de transition vers la société de l'information et de la cybersociété, de sorte que des structures économiques doivent être développées pour que les sociétés puissent entrer facilement dans la société de l'information et de la cybersociété.
6- Le manque de compétences au niveau de certains dirigeants d'entreprise en raison du manque de qualification et de la migration des cerveaux a posé un défi majeur.

Les politiques exécutives les plus importantes de la stratégie proposée :

Premièrement : Aux niveaux régional et international :

1- Formuler une stratégie internationale et arabe commune pour faire face à l'escalade des cybermenaces, renforcer la cybersécurité et coopérer dans les domaines de la lutte contre les risques cybernétiques, afin qu'elle soit formulée en coopération et coordination par les centres d'études et les institutions officielles concernées.
2- Activer la technologie de signature numérique pour protéger les fonds des banques et des institutions.
3- Utiliser l'IA face aux cybermenaces, là où l'IA est actuellement confrontée à l'IA.
4- Développer des programmes de protection électronique pour faire face aux cyberattaques, et à cette fin, des partenariats ont été établis entre les pays et le secteur privé dans chaque pays pour développer les infrastructures.
5- Préparer des programmes de sensibilisation à la cybersécurité qui sont présentés et diffusés de manière claire et simplifiée auprès du grand public.
6- Reconsidérer les règles juridiques internationales qui régissent ce type de guerre, et la nécessité de développer un consensus international à cet égard.
7- La nécessité pour les États de s'assurer que leurs systèmes, entités, rapports d'incidents cybernétiques et participation effective à l'information sont bien sécurisés afin d'améliorer la capacité des autorités du monde entier à gérer efficacement les incidents. Le modèle de déclaration des incidents et de partage des connaissances élaboré par le Conseil de stabilité financière est une étape importante pour améliorer la cybersécurité
8- Développer les capacités préventives : Les économies en développement et les pays à faible revenu devraient être aidés à renforcer la stabilité financière et à soutenir l'inclusion financière, en veillant à ce que la technologie soit utilisée de manière à préserver la sécurité et la sûreté contre les cyber-risques.

Deuxièmement : Au niveau local :

1- La mise en place d'un centre de sécurité cyberéconomique pour traiter rapidement tout problème économique, et c'est différent d'un département de cybersécurité, mais cette administration est liée à ce centre, et cela est dû à l'importance du domaine économique, car c'est un domaine sensible qui peut affecter le reste de l'État.
2- Sensibilisation économique et culture de sécurité pour les hommes d'affaires et les investisseurs afin de faire face à tous les cyber-risques représentés par l'extorsion et les intrusions, et comment faire face à ces situations.
3- Activer l'Internet à haut débit, car il joue un rôle majeur dans le développement économique.
4- Partenariat entre les secteurs public et privé en matière d'échange d'informations sur les différents risques cyber.
5- Éradiquer l'analphabétisme dans les technologies financières et diffuser la conscience numérique dans la société.
6- Affectation de structures de cybersécurité, comme stipulé à l'article 14 de la Convention de Budapest sur les crimes informatiques, qui permet une réponse rapide à toute attaque informatique

7- Développer des stratégies d'intervention où le système financier doit être en mesure de reprendre ses opérations rapidement.
8- Activer la stratégie de cyberdissuasion, où le coût des cyberattaques et leur risque doit être réduit grâce à des mesures de dissuasion efficaces.
9. Utiliser les médias tels que la télévision et la radio pour sensibiliser à la protection des données personnelles.
10- La mise en place d'un organisme national indépendant de réglementation de l'Internet, y compris une plateforme de sécurité Internet avec une vaste quantité de simulation d'informations et de ressources ; Pour aider la communauté et promouvoir la responsabilité et la flexibilité en ligne pour construire une culture positive. Sa mission est de promouvoir la sécurité numérique en promouvant une culture positive autour de la citoyenneté numérique, qui comprend également un système intensif de plaintes pour aider la communauté ; Si le site de médias sociaux ne respecte pas les normes contenues dans le Code de pratique. La personne peut s'adresser au commissaire à la sécurité numérique, qui peut guider le site de médias sociaux pour qu'il se conforme aux normes du Code tout en sensibilisant le public à la cybersécurité en adoptant des mesures de prévention proactive.

Résumé:

L'étude a abordé le problème des risques cybernétiques dans la sphère économique, en particu-lier pour les entreprises et les organisations dans les États, et répondu à une question impor-tante de savoir comment les États peuvent gérer leurs risques cybernétiques et ceux de leurs organisations dans la sphère économique ? L'étude a mis en évidence les actions et politiques nécessaires pour gérer les risques cybernétiques dans le domaine économique. L'étude s'est conclue par les résultats suivants :

1- Le développement rapide de la technologie a contribué à augmenter la taille des cyber-risques pour les pays, car il révèle des faiblesses plus grandes, des outils moins chers et plus faciles pour les attaquants, et bien que certaines sociétés financières et organismes de réglementation soient devenus plus conscients et préparés aux cyberattaques, les lacunes en matière de cybersécurité sont encore importantes et représentent toujours un défi pour les institutions et les pays.

2- Le nombre de cyberattaques a augmenté au cours des deux dernières décennies, pour devenir l'une des méthodes et tactiques les plus importantes adoptées entre les parties en conflit à travers le monde, en raison de leur faible coût et des pertes qui peuvent résulter de la partie attaquante par rapport à l'étendue des dommages et des dégâts possibles causés à l'adversaire en les employant.

3- Il existe de nombreuses procédures techniques et administratives pour faire face et gérer les risques et les cyberattaques dans le cyberespace et y faire face.

L'engagement d'appliquer et d'activer le plus grand nombre d'entre eux peut être très utile pour faire face à ces attaques et même travailler à gérer leurs risques cybernétiques avant qu'elles ne se produisent.

4- Nous constatons que la sécurité des pays n'est plus seulement liée à leur protection contre les risques et les attaques militaires, mais s'est étendue et élargie pour inclure la nécessité de protéger leurs communautés, leurs installations et infrastructures vitales, en particulier économiques, contre l'exposition aux risques cybernétiques

5- La nécessité d'un engagement organisationnel des institutions pour gérer les cyber-risques, car la simple existence d'un désir sans politiques et procédures bien étudiées ne suffit pas à créer une culture contre les risques cybernétiques.

6- Il est devenu nécessaire de travailler à la réduction de ces risques informatiques en établissant des procédures et des politiques qui protègent les données économiques dans les pays. Par conséquent, un système de gestion des risques cybernétiques au sein des organisations et institutions de l'État demeure la solution pour protéger les secteurs économiques et financiers contre le piratage et la pénétration des données. Il est donc nécessaire de travailler sur la gestion des risques cybernétiques dans le domaine économique pour protéger et réaliser la sécurité nationale des États.

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) صـلاح حيدر عبد الواحد، حروب الفضـاء الإلكتروني: دراسة فى مفهومها وخصائصـها 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 المؤسسـى لجامعة الأقصـى بقطاع غزة، رسالة ماجستير، كلية الاقتصاد والعلوم الإدارية، الجامعة الإسلامية، ٢٠٢٠، غزة، ص ٦٨.

(٩) أحمـد الخيـاط، تصـور مقترح لتطويـر إدارة الأعمال فى ضـوء مدخـل إدارة المخاطر بمؤسسـات الأعمال الكويتيـة، 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) صـليحة محمدى، الارهـاب الإلكترونى والأمن القومـى للدول: نمط جديد وتهديـدات مختلفة، المجلة الجزائريـة 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.

Gestion des Risques Cybernétiques dans le Domaine Économique

■ *Dr / Rehab Hosny El Rahmawy*
Ingénieure Électricienne en Télécommunications
à l'Autorité Nationale des Médias

Résumé:

L'aspect cybernétique est étroitement lié à l'économie, en particulier après l'expansion de l'utilisation des technologies de l'information et de la communication, et fait donc l'objet d'une attention prioritaire en raison de son impact le plus important sur l'amélioration du reste des capacités des forces globales de l'État et affecte les capacités des individus et du pays à tous les niveaux.

L'étude visait à aborder un sujet qui est l'un des sujets modernes et très importants, car il représente la nouvelle apparence des guerres futures à travers l'utilisation du cyberespace comme moyen de cyberattaque pour contrôler l'économie des pays à l'aide d'un ensemble de logiciels, et des virus destructeurs comme armes cyber stratégiques résultant de leurs orientations stratégiques, et comme un moyen de détruire l'infrastructure économique de l'État, puis d'affecter la sécurité nationale de l'État cible, ce qui a rendu nécessaire de travailler sur la gestion de ces risques cybernétiques dans le domaine économique de l'État. La problématique de l'étude apparaît dans l'identification des risques cybernétiques et de leurs effets négatifs sur le champ économique des pays et des institutions et organisations. L'importance de l'étude réside dans la clarification de l'impact des risques cybernétiques sur le domaine économique des pays et de la manière de les gérer au sein de leurs organisations et institutions, pour atteindre la sécurité nationale.

L'étude a conclu à plusieurs résultats, notamment qu'il existe de nombreuses procédures techniques et administratives pour faire face et gérer les risques et les cyberattaques dans le cyberespace et y faire face. L'engagement d'en appliquer le plus grand nombre peut être très utile pour faire face à ces attaques et même travailler à gérer leurs risques cybernétiques avant qu'elles ne se produisent.

Mots-clés: 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