Dr. Asmaa Jaber Mehran
Professeure adjointe de sociologie criminelle
Faculté des Lettres - Université d'Assiout

Répercussions et Risques Sociaux des Crimes et des Attaques Cybernétiques Contre la Sécurité Numérique et les Mécanismes de Lutte à la lumière de la vision de l'Égypte 2030

Introduction:

Les résultats d'une étude exploratoire menée par l'Organisation de coopération et de développement économiques (OCDE) sur l'économie numérique ont révélé que les gouvernements ont classé la sécurité à la deuxième place et la confidentialité à la troisième place parmi 31 domaines politiques prioritaires. Dans le même ordre d'idées, les consommateurs accordent une importance croissante à la confidentialité dans l'environnement numérique. En effet, les résultats d'une étude menée par CIGI-IPSOS en 2014 auprès des internautes de 24 pays sur la sécurité et la confiance en ligne ont montré que 64% des participants étaient plus préoccupés par la confidentialité qu'ils ne l'étaient auparavant (1).

Malgré la difficulté de sa quantification, les incidents de sécurité semblent se multiplier en termes de complexité, de fréquence et d'impact(2). Au cours des dix dernières années, les activités vitales ont été de plus en plus exposées aux menaces de sécurité numérique, une tendance accélérée par la transformation numérique actuelle. Les avantages attendus des villes intelligentes, des réseaux énergétiques renforcés numériquement et des soins de santé orientent l'adoption et l'exploitation de technologies comme le big data, l'intelligence artificielle, l'Internet des objets et les réseaux 5G. Bien que ces technologies soient émergentes, elles complexifient les écosystèmes numériques qui soutiennent les activités vitales en augmentant la surface d'attaque des opérateurs de ces activités proportionnellement à la quantité croissante de données, d'appareils, de logiciels et d'infrastructures de réseau qu'ils doivent gérer et qui ne peuvent être considérées comme parfaitement sécurisées(3).

La possibilité que des incidents de sécurité numérique entraînent des dommages matériels n'est plus une hypothèse théorique. Des attaques de sécurité numérique ont détruit des centrifugeuses nucléaires en Iran, causé des dommages matériels considérables dans une aciérie allemande en 2014, et provoqué des pannes de courant en Ukraine en 2015 et 2017. De plus, l'incident NotPetya en 2017 a montré que les cyberattaques pouvaient considérablement perturber les opérations et les chaînes d'approvisionnement pendant plusieurs jours dans des domaines tels que la logistique des conteneurs mondiaux (Maersk) et la production de médicaments (Merck). En 2021, une cyberattaque a contraint la société Colonia Pipeline Company à fermer le plus grand oléoduc des États-Unis pendant six jours, ce qui a entraîné une pénurie de carburant sur la côte est (4).

Problématique de l'étude :

La société s'est déplacée du monde réel au monde virtuel, et la criminalité l'a suivie. Il est

important de considérer l'ampleur des interactions qui se déroulent dans l'espace virtuel, que ce soit au niveau personnel, institutionnel, commercial, des services ou culturel. Il est essentiel de souligner que l'espace numérique a engendré de nouvelles formes de criminalité, appelées cybercriminalité, en créant de nouvelles opportunités pour les criminels. Les cybercriminels ont la possibilité de naviguer sur internet et de commettre des crimes uniques dans cet espace. Ces caractéristiques constituent des clés de transformation et se manifestent par :

1. La mondialisation : qui permet aux criminels de transcender les frontières traditionnelles avec de nouvelles opportunités.
2. Les réseaux distribués : qui ont engendré des opportunités pour créer des victimes.
3. Le panoptisme et le synoptisme: qui permettent aux criminels de humilier leurs victimes à distance.
4. Les traces de données : qui ont créé des opportunités pour le vol d'identité.

D'un autre côté, le nombre de victimes de cybercriminalité est en hausse, en particulier ceux qui subissent des pertes financières, des menaces ou du harcèlement, en raison de l'augmentation du nombre d'utilisateurs d'internet. La cybercriminalité représente un nouveau domaine de recherche en criminologie [5].

De ce qui précède, il ressort que la problématique de l'étude actuelle réside dans la réponse à la question principale :

Quelles sont les conséquences et les risques sociaux des crimes, attaques et menaces cybernétiques sur la sécurité numérique ? Et quels sont les mécanismes de lutte à la lumière de la Vision Égypte 2030 ?

De cette question principale découlent plusieurs questions subsidiaires :

a. Quelles sont les générations d'attaques cybernétiques ?
b. Quelle est la nature et les formes des crimes et attaques cybernétiques ?
c. Quels sont les acteurs menaçant dans l'environnement cybernétique ?
d. Quels sont les risques sociaux des crimes et attaques cybernétiques sur la sécurité numérique ?
e. Quels sont les mécanismes et les efforts de l'État égyptien pour lutter contre les cyberattaques à la lumière de la Vision 2030 ?
f. Quelle est la proposition conceptuelle pour faire face aux risques sociaux des crimes et attaques cybernétiques sur la sécurité numérique en Égypte?

Importance de l'étude :

Importance scientifique :

a. L'importance scientifique de l'étude réside dans sa tentative de mettre en lumière un nouveau domaine dans les sciences sociales, en particulier la sociologie criminelle. Cette étude est, à la connaissance de l'auteure, la première étude arabe à aborder la sécurité numérique d'un point de vue sociologique, et l'on espère qu'elle contribuera à ouvrir de nouvelles perspectives futures dans les études sociologiques.
b. Elle représente un ajout au patrimoine théorique en étudiant un concept nouveau, la sécurité numérique, qui diffère de la sécurité informatique.

Importance pratique :

L'identification des impacts sociaux des crimes et attaques cybernétiques sur la sécurité numérique est importante pour les individus afin de les sensibiliser à leurs risques et à la façon de les contrer. Elle est également importante pour les responsables et les décideurs afin de développer des stratégies de lutte contre ces menaces et de renforcer les capacités défensives et offensives, car elles représentent une menace sérieuse pour l'individu et l'État dans son ensemble.

Objectifs de l'étude :

L'objectif principal de l'étude actuelle est d'examiner les conséquences et les risques sociaux des crimes, attaques et menaces cybernétiques sur la sécurité numérique, et d'identifier les mécanismes de lutte à la lumière de la Vision Égypte 2030. De cet objectif général découlent les objectifs spécifiques suivants :

a. Identifier les générations d'attaques cybernétiques.
b. Déterminer la nature et les formes des crimes et attaques cybernétiques.
c. Identifier les acteurs menaçant dans l'environnement cybernétique.
d. Détecter les risques sociaux des crimes et attaques cybernétiques sur la sécurité numérique.
e. Identifier les mécanismes et les efforts de l'État égyptien pour lutter contre les crimes et attaques cybernétiques à la lumière de la Vision 2030.
f. Développer une proposition conceptuelle pour faire face aux risques sociaux des crimes et attaques cybernétiques sur la sécurité numérique en Égypte.

Méthodologie de l'étude :

L'étude actuelle s'appuiera sur la méthodologie d'analyse des systèmes développée par David Easton pour analyser les phénomènes et les systèmes sociaux en décomposant le phénomène en ses éléments constitutifs comme des entrées. Puis elle étudiera l'influence des facteurs changeants sur ces éléments comme des processus, jusqu'à obtenir les sorties et les comparer aux entrées via ce qu'on appelle la rétroaction, afin d'étudier la relation entre la cause et l'effet (6).

Ainsi, les sujets d'étude seront divisés en fonction de cette méthodologie selon l'ordre suivant :

- ***A. Les entrées :*** qui comprendront les concepts de l'étude tels que (les cybercrimes, les cyberattaques, la sécurité numérique).
- ***B. Les processus :*** qui comprendront l'étude et l'analyse des objectifs liés au sujet de l'étude, qui consistent à identifier les générations de cyberattaques, la nature et les formes des cybercrimes et des cyberattaques, les acteurs de la menace dans l'environnement cybernétique, les risques sociaux des cybercrimes et des cyberattaques sur la sécurité numérique, et les efforts et les mécanismes de l'État égyptien pour faire face aux cybercrimes et aux cyberattaques à la lumière de la Vision 2030.
- ***C. Les sorties :*** comprendront la méthodologie développée à laquelle l'étude tente de parvenir en tant que proposition ou nouvelle méthodologie pour faire face aux risques des cybercrimes et des cyberattaques sur la sécurité numérique.

La perspective sociologique de l'étude de la sécurité numérique:

1-La théorie de la société du risque pour observer les répercussions des cybercrimes sur la sécurité numérique :

Ulrich Beck, sociologue allemand, est le fondateur de cette théorie. Il est le premier à avoir évoqué le concept de risque et de société du risque mondiale. La théorie du risque aborde l'augmentation croissante de l'incertitude généralisée dans le contexte des changements sociétaux. La société industrielle a cédé la place à une société du risque technologique, numérique ou informationnelle, que les penseurs post-modernes qualifient de « monde de la complexité » où les modes de vie stables disparaissent (7).

La société du risque mondiale représente une période historique unique, capable de s'autodétruire technologiquement (8).

Sur cette base, nous constatons que la sécurité numérique est confrontée à de nombreux risques en raison de la révolution numérique que connaît la société, et des évolutions qu'elle a entraînées dans les types de cybercrimes et d'attaques. Ces derniers ont eu pour conséquence la non-préservation de la vie privée culturelle des individus, ainsi que le vol de données numériques d'individus, d'entreprises et d'États (9).

2-Théorie de la structuration pour surveiller les éléments de la sécurité numérique.

On peut considérer la théorie de la structuration chez Anthony Giddens comme une contribution importante à l'élaboration d'une vision théorique pour résoudre un problème social, à savoir le problème de (Structure d'agence)

Étant donné que, selon cette théorie, les pratiques de sécurité numérique et cybernétique constituent l'un des principaux aspects de la formation de la structure sociale, en considérant les questions clés soulevées par Anthony Giddens , à savoir : (10)

A. Le processus de formation de la structure implique une participation active des acteurs et des pratiques quotidiennes réussies.
B. La structure impose des limites à l'action humaine tout en facilitant cette action : c'est la « dualité de la structure ».
C. La structure se forme à la lumière de l'interaction entre les significations, les normes et le pouvoir.
D. La structure se forme à travers la performance habile des membres au sein d'un espace-temps donné.

Par conséquent, il est clair que les acteurs, à savoir les auteurs de crimes et d'attaques cybernétiques, ont un impact négatif sur la structure sociale et la façonnent selon leur propre vision dualiste. En effet, à travers leurs pratiques criminelles répétées, ils constituent une force active dans l'espace numérique car ils possèdent un pouvoir de destruction et agissent selon des croyances spécifiques, utilisant diverses méthodes qui, dans l'ensemble, entraînent une série de risques sociaux préjudiciables à l'individu et à la société tout entière.

L'étude comprend les éléments suivants :

1. Le cadre conceptuel de l'étude.
2. Les générations des cyberattaques.
3. Les types de cybercrimes et de cyberattaques.
4. Les types d'acteurs menaçant dans l'environnement cybernétique (catégories de cybercriminels).
5. Les risques sociaux des cybercrimes et des cyberattaques sur la sécurité numérique.

6.Les mécanismes et les efforts de l'État égyptien pour lutter contre les cybercrimes et les cyberattaques à la lumière de la Vision Égypte 2030.
7.Les critères et le modèle proposés pour faire face aux risques sociaux des cybercrimes et des cyberattaques sur la sécurité numérique en Égypte.
8.Les résultats de l'étude et ses recommandations.

Premièrement :
le cadre conceptuel de l'étude:
1. Concept de cybercriminalité :

La cybercriminalité se limite à un nombre restreint d'actes portant atteinte à la confidentialité des données ou des systèmes informatiques et à l'intégrité de leur disponibilité. Les actes exécutés à l'aide d'ordinateurs dans le but de réaliser des gains personnels ou financiers ou de causer des dommages, y compris les formes de criminalité liées à l'identité et au contenu informatique, relèvent tous d'un concept plus large de cybercriminalité et ne peuvent être facilement adaptés pour s'inscrire dans des définitions juridiques d'un terme général. Cela nécessite de définir et d'identifier les actes fondamentaux constituant une cybercriminalité. Bien que la définition de la cybercriminalité ne soit pas aussi importante pour d'autres objectifs tels que la détermination de la compétence des autorités compétentes en matière d'enquêtes et de coopération internationale, il est préférable de se concentrer sur les preuves électroniques en ce qui concerne tout crime plutôt que de se concentrer sur une structure large et artificielle de la « cybercriminalité » (11).

Au sens large, les cybercrimes (électroniques) désignent « tout comportement illégal utilisant l'ordinateur ou Internet comme outil ou cible, ou les deux. Ce comportement illégal utilise des appareils informatiques tels que les smartphones,les tablettes, les assistants numériques personnels (PDA) et d'autres appareils informatiques autonomes ou connectés comme outil ou cible d'un comportement criminel commis de manière répétée par des personnes ayant un comportement destructeur et criminel pour diverses raisons, notamment la vengeance, l'argent ou l'aventure ». Selon le dictionnaire d'Oxford, le terme cybercriminalité désigne : « les activités criminelles qui sont mises en œuvre à l'aide d'ordinateurs ou d'Internet ». La cybercriminalité est également définie comme « une activité criminelle qui se produit sur ou à l'aide d'appareils, du Web ou de toute autre technologie reconnue ». En conclusion, la cybercriminalité est : « ces types d'actes dont le genre est un crime traditionnel, mais où l'ordinateur est l'objet ou le sujet du comportement qui constitue un crime»(12).

2. Concept de cyberattaque :

Les cyberattaques s'inscrivent dans un contexte plus large, traditionnellement appelé opérations d'information ou opérations informationnelles, qui utilisent de manière intégrée les capacités clés de la guerre électronique, des réseaux psychologiques et informatiques, de la tromperie militaire et des opérations de sécurité, en coordination avec le soutien spécial et les capacités connexes. Les définitions de la cyberattaque ont varié selon les spécialistes juridiques et techniques. L'une des définitions les plus importantes est que les cyberattaques sont : ***« les mesures prises par les États pour pénétrer dans les ordinateurs d'un autre État ou d'autres États afin de causer des dommages ou des perturbations »*** (13).

Les cyberattaques sont également définies comme : « un acte qui compromet les capacités des fonctions du réseau d'information en exploitant des vulnérabilités, ce qui donne à l'attaquant la capacité de manipuler le système. Elles sont également définies comme l'exploitation délibérée de systèmes informatiques et de réseaux technologiques dépendants par le biais de logiciels malveillants»(14).

Nous pouvons distinguer et mettre en évidence les différences entre la cybercriminalité, la cyberguerre et la cyberattaque de la manière suivante :

- ***Cybercriminalité (électronique) :*** Il s'agit d'actions cybernétiques entreprises uniquement par des attaquants non étatiques, et l'action cybernétique est exécutée par un système informatique, ce qui constitue une violation du droit pénal.
- ***Cyberattaque et cyberguerre :*** Le but de la cyberattaque est de détruire et de perturber le fonctionnement d'un réseau informatique, et l'attaque est menée à des fins politiques ou de sécurité. Les effets d'une cyberattaque sont similaires à ceux d'une attaque armée ou d'un acte cybernétique commis dans le cadre d'une attaque armée (15).

3. Concept de sécurité numérique :

Les normes internationales et nationales de sécurité de l'information incluent souvent une définition de la sécurité numérique. Il est à noter qu'il n'existe pas de définition universellement acceptée ou de consensus mondial sur ce que le terme englobe exactement. Dans le contexte des Nations Unies, les inspecteurs ont remarqué qu'aucune orientation à l'échelle du système n'émanait des forums inter-agences concernés ne recommandant à l'unanimité une définition particulière comme étant fiable pour le système,

et que les cadres réglementaires des organisations n'essaient pas de manière systématique d'imposer une définition de la sécurité numérique. Selon l'Union internationale des télécommunications, la sécurité numérique est définie comme : ***« un ensemble d'outils, de politiques, de concepts de sécurité et de garanties de sécurité, de principes directeurs, d'approches de gestion des risques, de procédures, de formation, de meilleures pratiques, d'assurance et de technologies qui peuvent être utilisées pour protéger l'environnement cybernétique et les actifs de l'organisation et des utilisateurs. Les actifs de l'organisation et des utilisateurs comprennent les appareils informatiques interconnectés, les employés, les infrastructures, les applications, les services, les systèmes de communication et l'ensemble des processus transférés ou stockés dans l'environnement cybernétique. La sécurité cybernétique vise à garantir et à préserver les propriétés de sécurité des actifs de l'organisation et des utilisateurs contre les risques de sécurité liés à l'environnement cybernétique. Les objectifs de sécurité généraux sont la disponibilité,l'intégrité qui peut inclure l'authenticité et la non-répudiation, et la confidentialité »*** (16).

L'Agence européenne de sécurité numérique, dans sa première législation adoptée en 2001, a défini la sécurité numérique comme : ***« la capacité d'un système d'information à résister aux tentatives d'intrusion ou aux incidents imprévus visant les données circulant ou stockées dans un cadre harmonisé »*** (17).

Le centre Herodo pour le soutien à l'expression numérique le définit comme suit : ***« la manière d'utiliser Internet efficacement sans être exposé à des menaces, des risques ou une surveillance qui compromettent la confidentialité et la sécurité des informations »*** (18).

Ce qu'il est important de noter concernant le concept de sécurité numérique, c'est qu'il constitue un outil pour unifier la coopération dans la lutte contre les cybercrimes sous toutes leurs formes et pour faire face à leurs risques. Il convient de mentionner que parmi les pays qui ont accordé une importance particulière au concept de sécurité numérique figurent le Royaume-Uni, qui occupe la première place mondiale selon le classement de l'indice mondial de cybersécurité (GCI) publié par l'Union internationale des télécommunications des Nations Unies, puis les États-Unis, et parmi les pays arabes qui ont accordé de l'importance à la sécurité numérique selon le classement, l'Arabie Saoudite arrive en tête, suivie de l'Égypte et du Qatar (19).

Deuxièmement : Les générations des cyberattaques

On peut mentionner ce qui suit (20) **:**

- ***Première génération (1989-1990) :*** À la fin des années 1980, des pirates informatiques ont lancé des attaques virales sur les ordinateurs personnels, ce qui a incité les utilisateurs et les entreprises privées touchées à créer des produits antivirus (AV) axés sur les signatures.

Et voici quelques exemples de cyberattaques de première génération :

- (1982 - ELK Cloner): Le premier virus informatique au monde.

La deuxième génération (1995) : Au milieu des années 1990, les attaques par vers informatiques se sont rapidement propagées sur Internet, ce qui a contraint les entreprises à mettre en place des pare-feu aux frontières de leur infrastructure pour repousser les attaquants.

Et voici quelques exemples de cyberattaques de deuxième génération :

- (Ver Morris - 1988) : Un des premiers vers informatiques, ayant entraîné une condamnation pénale aux États-Unis en vertu de la loi sur la fraude et l'abus informatique.
- (Melissa - 1999) : Le premier virus macro de courrier électronique de masse.

La troisième génération (2005) : Au début du nouveau siècle, les cybercriminels ont commencé à exploiter les vulnérabilités logicielles pouvant affecter les entreprises, marquant ainsi une période de transition où le but des attaquants est passé de la reconnaissance à la recherche de profits, notamment grâce à l'utilisation de botnets pour envoyer du spam.

Et voici quelques exemples de cyberattaques de troisième génération :

- (2000 - I Love You) : Un ver informatique ayant infecté des dizaines de millions d'ordinateurs Windows.
- (2005 - SQL Slammer) : Une attaque par déni de service ayant affecté 75 000 serveurs.

La quatrième génération (2010) : Au cours du premier quart du siècle dernier, il n'y avait aucune indication de l'émergence d'attaques ciblées. Au cours d'une discussion sur l'absence de preuves claires concernant les armes de destruction massive, les citoyens ont été encouragés à adopter le concept d'inconnues inconnues, inventé par l'ancien secrétaire américain à la Défense, Donald Rumsfeld.

Et voici quelques exemples de cyberattaques de quatrième génération :

• (2010 - Stuxnet) : Un logiciel malveillant développé par un État visant les systèmes SCADA des infrastructures critiques, notamment le programme nucléaire iranien.

• (2016 - Dyn) : Pas un virus en soi, mais une attaque par déni de service distribué (DDoS) massive contre un fournisseur DNS majeur.

Cinquième génération (2017) :

C'est en 2017 qu'ont commencé des cyberattaques de grande envergure, largement financées par certains gouvernements,permettant ainsi à de nombreuses entreprises de les mettre en œuvre. La cybercriminalité dispose désormais de ses propres réseaux et de ses propres moyens.

Parmi les exemples d'attaques de cette cinquième vague, on peut citer :

• (2017 - Wannacry) : Une attaque massive par rançongiciel ayant affecté 200 000 ordinateurs dans 150 pays.

Troisièmement :

Typologies des cybercrimes et des cyberattaques :

1. Typologies des cybercrimes :

La cybercriminalité est devenue l'une des menaces criminelles connaissant la croissance la plus rapide. Il est extrêmement difficile d'évaluer l'ampleur de ces activités criminelles.

Parmi les actes classés comme cybercrimes, on peut citer [21] :

- Atteinte aux données informatiques.
- Atteinte aux systèmes informatiques.
- Mauvaise utilisation des équipements ou des logiciels informatiques.
- Crimes financiers.
- Exploitation sexuelle d'enfants.
- Atteinte à la propriété intellectuelle des œuvres numériques.
- Fraudes aux cartes bancaires et aux monnaies électroniques.
- Atteintes aux données personnelles.
- Crimes racistes et crimes contre l'humanité commis à l'aide de moyens informatiques.
- Crimes liés aux jeux d'argent et au trafic de drogues commis à l'aide de moyens informatiques.
- Crimes informatiques contre l'État et la sécurité publique.
- Crimes de chiffrement de données.

2. Typologies des attaques cybernétiques :

Les attaques cybernétiques peuvent être classées dans les catégories suivantes [22] :

A. Attaques contre les réseaux :

Ce sont des attaques qui ciblent les sites web ou les applications web. En voici quelques exemples :

- Injections : Cela inclut les injections SQL, XML, de code et de journal, qui consistent à injecter des données dans une application web pour la manipuler et obtenir les informations souhaitées.
- Usurpation d'identité DNS : L'attaquant redirige le trafic vers un faux serveur.
- Phishing : Cela inclut le spear phishing (ciblage ciblé), le whaling (ciblage de hautes personnalités), le smishing (par SMS), le vishing (par téléphone) et le phishing par e-mail. Il existe également le SEO poisoning qui consiste à manipuler les résultats de recherche.
- Attaques par déni de service (DoS/DDoS) : Ces attaques visent à rendre un service indisponible en saturant le système de requêtes.
- Attaques de l'homme du milieu (Man-in-the-Middle) : L'attaquant s'interpose entre deux parties communicantes pour intercepter et éventuellement modifier les données. Cela inclut l'écoute clandestine sur les réseaux Wi-Fi,l'interception d'e-mails ou de protocoles SSL, et l'usurpation d'adresses IP, HTTPS ou DNS.

B. Attaques basées sur les systèmes :

Ces attaques visent à compromettre un ordinateur ou un réseau. En voici quelques exemples :

- Virus : Programme malveillant qui se réplique et se propage.
- Vers : Programme malveillant qui se réplique de manière autonome.
- Cheval de Troie : Programme malveillant dissimulé dans un logiciel légitime.
- Porte dérobée : Mécanisme permettant un accès non autorisé à un système.
- Botnets : Réseau d'ordinateurs infectés contrôlés à distance.

Analyse de la traduction :

- Précision technique : La traduction utilise des termes techniques précis pour décrire les différents types d'attaques.
- Clarté et concisité : Les explications sont claires et concises, facilitant la compréhension.
- Structure logique : La classification des attaques en deux catégories (réseau et système) est logique et facilite la compréhension.

De plus, la stratégie nationale de cybersécurité égyptienne (2023-2027) a révélé une augmentation significative du nombre de cyberattaques ces dernières années. Ces attaques ont entraîné des pertes économiques considérables à l'échelle mondiale, représentant un fardeau important pour les budgets nationaux. Outre ces pertes financières, les cyberattaques peuvent également entraîner l'interruption de services essentiels et porter atteinte à la réputation des entreprises et des individus.

La stratégie a également mis en évidence la diversité des sources de menaces cybernétiques, qui incluent la cybercriminalité, la cyberguerre, le terrorisme, les menaces internes et les menaces provenant d'acteurs non étatiques [23] :

- Cybercriminalité (Crime Cyber) :

La cybercriminalité est principalement responsable du développement et de la propagation de logiciels malveillants dans le but de générer des profits, de pirater des systèmes pour voler, endommager ou altérer des données ou des réseaux. Ces attaques sont devenues de plus en plus virulentes et se sont répandues à l'échelle mondiale, comme en témoigne l'utilisation croissante des rançongiciels et des attaques par déni de service (DDoS) à des fins de diffamation ou d'extorsion.

- Cyberguerre (Cyber War) :

Il s'agit de menaces perpétrées par des États ou des groupes soutenus par des États, visant à infiltrer des secteurs critiques d'autres pays, tels que l'énergie, les télécommunications et les banques, dans le but d'espionner, d'obtenir des gains politiques et stratégiques, ou simplement de saboter. Il convient de noter que de nombreux pays ont ouvertement déclaré posséder des capacités d'attaque cybernétique à des fins de défense.

- Terrorisme (Terrorism) :

Bien que les capacités cybernétiques des terroristes soient encore limitées, on s'attend à ce qu'elles augmentent considérablement dans les prochaines années, ce qui en fait une menace potentielle majeure.

- Menaces internes (Insiders) :

Avec l'utilisation croissante des technologies de l'information au sein des organisations, les risques liés aux employés autorisés à utiliser ces systèmes augmentent, que ce soit intentionnellement ou non. Ces employés peuvent représenter une menace pour les organisations en volant des données sensibles, entraînant ainsi des pertes financières importantes ou en endommageant la réputation de l'entreprise. Les employés peuvent également exposer involontairement les données sensibles de l'organisation à des risques en tombant victimes de certaines cyberattaques telles que le phishing ou l'ingénierie sociale.

- Hackers amateurs (Kiddies Script) :

Il s'agit d'individus ayant des compétences limitées en matière de cybersécurité mais utilisant des logiciels préconfigurés dotés de capacités destructrices élevées s'ils trouvent des vulnérabilités dans les systèmes d'information des organisations.

Quatrièmement :
Types d'acteurs menaçant dans l'environnement cybernétique (Catégories de cyberattaquants):

Les principaux types d'acteurs menaçant dans l'environnement cybernétique sont les suivants [24]:

- **Hackers :** Individus ou groupes qui pénètrent dans les réseaux pour causer des perturbations, des dommages ou du chaos, par simple désir de reconnaissance ou de défi.
- **Hacktivistes :** Ils ont des motivations spécifiques et considèrent leur activité comme une forme de désobéissance civile ou un moyen d'expression politique ou idéologique.
- **Cybercriminels :** Acteurs engagés dans des activités criminelles facilitées par le cyberespace (fraudes, vols,extorsions, etc.) à l'aide d'outils informatiques ou dans des activités criminelles dépendant du cyberespace, telles que la propagation de virus ou de logiciels malveillants, et d'autres activités qui ne peuvent être commises que par des moyens informatiques.
- **Espions industriels :** Sous-catégorie du groupe criminel, leurs objectifs sont spécifiques : obtenir des secrets commerciaux, extorquer des fonds pour des raisons économiques ou saboter la concurrence.
- **États ou groupes soutenus par des États:** Acteurs très sophistiqués et bien financés, dont les activités sont généralement difficiles à détecter, à suivre ou à attribuer. Ils peuvent poursuivre des objectifs complexes, souvent indirects et obscurs, et sont directement utilisés par des entités gouvernementales ou militaires ou financés indirectement par celles-ci.
- **Initiés :** Acteurs qui, en raison de leurs relations contractuelles avec l'organisation concernée, ne sont pas considérés comme des acteurs externes, mais qui l'exposent à des risques depuis l'intérieur. Cette catégorie peut inclure des employés mécontents, des employés mal formés, des fournisseurs de services sous-

traitants mal formés,ainsi que d'autres parties prenantes.

Cinquièmement : Les risques sociaux des cybercrimes et des cyberattaques sur la sécurité numérique :

Les cybercrimes ont causé des dommages aux citoyens, aux entreprises et aux gouvernements de diverses manières, telles que la perte d'informations commerciales sensibles, la perte de confiance des clients, la perte de propriété individuelle, les pertes commerciales, etc. Le Centre d'études stratégiques et internationales a indiqué que le coût annuel supporté par l'économie mondiale en raison des cybercrimes dépasse les 400 milliards de dollars, et que les impacts des cybercrimes augmenteront progressivement avec le développement des activités commerciales en ligne, et avec la connexion d'un nombre croissant d'entreprises et de clients dans le monde à Internet.

La cybercriminalité entraîne également une baisse du taux d'emploi dans les pays développés. Des recherches ont révélé que les pertes dues à la cybercriminalité peuvent affecter jusqu'à 200 000 emplois aux États-Unis, soit environ un tiers de la baisse de l'emploi. En outre, 3 000 entreprises aux États-Unis ont été piratées en 2014. Le Brésil a subi des pertes de 1,4 milliard de dollars en raison des dommages causés par les cyberattaques, car plus de 45 % des Brésiliens utilisent Internet.En 2013, la France a perdu 5,19 millions de dollars en raison des cyberattaques et a fait face à 1900 cyberattaques depuis les attentats terroristes de 2014. Près de 91 % des entreprises et 31 % des ménages au Royaume-Uni ont accès à Internet,et le coût estimé des cybercrimes au Royaume-Uni est d'environ 27 milliards de dollars (25).

t sur cette base, le rapport de l'Union internationale des télécommunications (UIT) de 2010 sur les dimensions sociales de la sécurité numérique a souligné que la révolution numérique a transformé les pratiques commerciales et le fonctionnement des gouvernements. La mondialisation et les progrès technologiques ont affaibli les infrastructures, les rendant ainsi des cibles potentielles pour des attaques terroristes. Les pays sont confrontés à des risques réels, et les criminels exploitent les vulnérabilités des systèmes d'information pour perturber les infrastructures et les ressources essentielles, menaçant ainsi la sécurité nationale (26).

Les principaux risques sociaux des cybercrimes et des cyberattaques sur la sécurité numérique sont les suivants :

1. Augmentation des taux de criminalité nouvelle et des pertes qui en résultent :

Le 23 décembre 2015, des hackers ont attaqué le réseau électrique ukrainien et ont désactivé à distance les systèmes de contrôle utilisés dans les sous-stations électriques, laissant des personnes et la partie occidentale du pays sans électricité pendant plusieurs heures. Le Service de sécurité ukrainien (SBU) a blâmé le gouvernement russe pour cette cyberattaque,une accusation qui a été soutenue plus tard par une analyse de programmes malveillants réalisée par des entreprises de sécurité informatique privées. Cette cyberattaque en Ukraine a été le premier cas publiquement reconnu d'une cyberattaque ayant réussi à provoquer une coupure de courant. Ce n'est qu'un exemple parmi des milliers d'activités cybernétiques, dont la plupart sont menées parallèlement aux combats physiques en Ukraine (27).

Étant donné que les consommateurs dépendent de plus en plus des ordinateurs, des réseaux et des informations qu'ils utilisent pour les stocker et les conserver, le risque d'être victime de cybercrimes est élevé. Les résultats d'enquêtes ont montré que jusqu'à 80 % des entreprises interrogées ont reconnu des pertes financières dues à des violations informatiques, estimées à 450 millions de dollars, et près de 10 % des fraudes financières. Les nouvelles attaques affectant la confidentialité, l'intégrité et la disponibilité des systèmes informatiques peuvent varier de vols d'informations d'identification personnelle à des attaques par déni de service (28).

Conformément à ce qui a été mentionné, au cours des quinze dernières années, de nombreux problèmes ont affecté la transition de la sécurité de l'information à la sécurité numérique : l'augmentation des menaces internes (telles que les fuites de données de WikiLeaks, les violations de données et les activités malveillantes internes), les technologies émergentes, en particulier les technologies numériques externes qui permettent la connectivité, les technologies cognitives, l'intelligence artificielle, la technologie mobile, les médias sociaux, etc., et l'augmentation des menaces externes telles que les logiciels malveillants, les ransomwares, les violations de données, les appareils interconnectés et les appareils IoT, la cyberguerre et les attaques soutenues par l'État. Par exemple, le Pew Research Center a estimé que les coûts directs d'une violation de données en 2017 s'élevaient à 3,62 millions de dollars américains(29).

Ce n'est pas tout, car les commissariats de police de tout le pays ont indiqué avoir reçu un nombre

croissant de plaintes pour fraude et vol en col blanc ces dernières années. Cette situation coïncide avec la tendance nationale résultant de l'utilisation accrue de l'informatique et du commerce en ligne. En 2004, la cybercriminalité a généré des revenus supérieurs à ceux du trafic de drogue, et l'on s'attend à ce qu'elle se développe davantage avec l'expansion de l'utilisation des technologies dans les pays en développement. Les résultats de 2011 ont montré que plus de 74 millions de personnes aux États-Unis avaient été victimes de cybercrimes en 2010, et que ces activités criminelles avaient entraîné des pertes financières estimées à 32 milliards de dollars. De plus, 69% des adultes connectés à Internet ont été victimes de cybercrimes, ce qui représente environ un million de victimes par jour. Beaucoup de gens pensent que la cybercriminalité se limite aux crimes liés aux affaires en ligne (30).

2. Cible des secteurs vitaux :

Le rançongiciel WannaCry a affecté de nombreux services à travers le monde, tels que les services de santé nationaux au Royaume-Uni. Renault a dû arrêter la production dans ses usines en France, Deutsche Bahn a rencontré des difficultés pour afficher les horaires des trains dans les gares, et le trafic de conteneurs de Maersk a été considérablement perturbé à l'échelle mondiale, etc.(31).

Parmi les exemples d'attaques cybernétiques dévastatrices, on peut citer la célèbre cyberattaque sur le pipeline colonial en 2021, qui a directement entraîné l'arrêt de l'approvisionnement en gaz à travers les États-Unis. Dans la nuit du 9 septembre 2020, une attaque par rançongiciel a touché les systèmes de l'hôpital universitaire de Düsseldorf, un grand hôpital du sud de Düsseldorf. Les rançongiciels sont un type de logiciel malveillant qui empêche les utilisateurs d'accéder à leurs fichiers, souvent en chiffrant les données jusqu'au paiement d'une rançon. L'attaque s'étant propagée à travers le réseau informatique de l'hôpital, trente serveurs ont été chiffrés et rendus inutilisables, rendant difficile l'accès aux données des patients. De nombreux équipements médicaux connectés au Wi-Fi sont devenus inaccessibles, et l'hôpital a dû suspendre les opérations pendant plusieurs semaines le temps de réparer les systèmes endommagés. Parallèlement, les pirates ont exigé une rançon considérable pour restaurer l'accès aux systèmes informatiques verrouillés. Après avoir alerté la police, les criminels ont indiqué que l'attaque s'était propagée involontairement à l'hôpital local (32).

"Il est clair d'après ce qui précède que les cybercrimes et les cyberattaques ciblent directement les systèmes et les secteurs vitaux des États afin de les extorquer et d'atteindre des objectifs spécifiques."

3. Destruction des infrastructures et atteinte à la sécurité nationale:

La cyberguerre ne se limite pas aux équipements et systèmes militaires. Elle cible également les infrastructures critiques d'une société, notamment les réseaux intelligents, les réseaux de surveillance et de contrôle (SCADA) qui permettent à ces infrastructures de fonctionner et de se défendre. Par conséquent, un conflit cybernétique peut avoir des conséquences mettant en danger des vies si les infrastructures de l'information sont compromises. Le rapport UIT-2017 du Congrès mondial du développement des télécommunications souligne la nécessité d'une infrastructure de communication et de technologies de l'information sûre et fiable. Il insiste également sur le besoin de renforcer le développement des infrastructures et des services, notamment en construisant la confiance et la sécurité dans l'utilisation des communications et des technologies de l'information. Une infrastructure habilitante et renforcée, ainsi que des politiques favorables, sont essentielles pour une développement durable des communications et des technologies de l'information. Les sociétés subissent des pertes économiques et sociales considérables si leurs réseaux de communication ou leurs autres infrastructures sont attaqués ou endommagés. L'évolution technologique amplifiera ces pertes en l'absence d'une attention suffisante accordée à la sécurité et aux infrastructures (33).

Un des documents de référence pour comprendre l'impact des attaques sur les infrastructures sur les sociétés est le rapport sur les bombardements stratégiques mené par les États-Unis pendant et après la Seconde Guerre mondiale. Les États-Unis et la Grande-Bretagne ont lancé des milliers de bombardiers lourds qui ont largué des millions de tonnes d'explosifs sur l'Allemagne, dans le but de paralyser ses infrastructures, de détruire son appareil industriel et de briser la volonté de la population de poursuivre la guerre. Les premiers théoriciens de la guerre aérienne avaient prédit qu'un tel assaut paralyserait l'ennemi. Avec l'intensification des bombardements, les Allemands n'ont pas pu empêcher le déclin et l'effondrement de leur économie (34).

4. Vol d'identité numérique et données personnelles :

Le vol d'identité numérique est l'un des crimes les plus dangereux qui menacent les utilisateurs

d'Internet et l'avenir des services en ligne. Les données personnelles d'un utilisateur peuvent être volées dans le but d'usurper son identité, de s'approprier ses biens et son argent, ou de l'impliquer dans des transactions suspectes ou illégales. Le voleur d'identité utilise généralement des informations déjà disponibles en ligne, en particulier sur les sites et réseaux sociaux professionnels ouverts, les bases de données et les informations nationales, les réseaux de services gouvernementaux, les services de sécurité sociale, les sites de commerce électronique, les marchés virtuels, les réseaux de paiement électronique, les distributeurs automatiques de billets et les bourses. De plus, les outils et systèmes utilisés pour effectuer des transactions électroniques peuvent être volés ou sabotés, ce qui représente un risque important pour les intérêts des utilisateurs et l'avenir des services en ligne. Des attaques à grande échelle peuvent affecter le secteur financier national dans son ensemble. Les données privées des institutions publiques et des entreprises sont également susceptibles d'être volées, entraînant des pertes financières et immatérielles considérables, ainsi qu'une atteinte à leur réputation, la perte de clients et d'actifs immatériels, ce qui peut nuire à l'économie nationale dans son ensemble (35).

6. Mécanismes et efforts de l'État égyptien pour lutter contre la cybercriminalité et les cyberattaques dans le cadre de la Vision Égypte 2030 :

L'indice de la cybersécurité (GCI) publié par l'Union internationale des télécommunications a classé l'Égypte au 23ème rang mondial sur 193 pays. L'Égypte s'est également classée première au monde en termes de compétitivité des secteurs de l'internet et de la téléphonie en 2021, selon l'Indice de la connaissance mondiale. De plus, l'Égypte a progressé de trois places dans l'indice de préparation du gouvernement à l'intelligence artificielle publié par le groupe d'Oxford, atteignant la 62ème place en 2022 contre la 65ème en 2021 (36).

Les mécanismes et les efforts de l'État égyptien dans le domaine de la cybersécurité et sa capacité à lutter contre la cybercriminalité et les cyberattaques peuvent être résumés comme suit :

1. Législation nationale égyptienne :

- **Constitution égyptienne :** L'article 31 de la Constitution égyptienne, tel que modifié le 23 avril 2019, stipule que :"L'espace informationnel est une partie essentielle du système économique et de la sécurité nationale. L'État s'engage à prendre les mesures nécessaires pour le préserver conformément à la loi" (37).
- **Loi sur la lutte contre la cybercriminalité (Loi n° 175 de 2018) :** Pour la première fois, la loi criminalise les "pratiques cybernétiques illégales" telles que la création de sites Web incitant au terrorisme, la falsification numérique, etc. Selon cette loi, la peine est déterminée en fonction de la gravité et de la nature du crime. Dans le cas de cybercrimes, des peines sévères sont imposées en raison des graves conséquences de ces crimes sur la sécurité nationale, en plus des autres peines liées aux infractions de piratage informatique, de falsification, etc. (38).
- **Loi n° 94 de 2015 sur la lutte contre le terrorisme :** C'est une loi complète pour lutter contre le terrorisme et son financement, tant sur le plan matériel que procédural. Elle a abordé les axes nécessaires à la lutte juridique contre le terrorisme avec des procédures efficaces et des sanctions dissuasives. Les dispositions de cette loi sont inspirées des résolutions du Conseil de sécurité et des instruments et accords internationaux et régionaux en matière de lutte contre le terrorisme. Elle prévoit également de punir la tentative de commettre un crime terroriste ou l'incitation à le commettre de la même peine que celle prévue pour le crime achevé, sans que l'incitation n'entraîne d'effets. Le législateur a réglementé les contrôles de gel des avoirs et d'interdiction d'en disposer, et a imposé la création de tribunaux spécialisés pour connaître des délits et des crimes, des appels et des recours en cassation dans les affaires de terrorisme(39).

2. Intervention stratégique :

A. Stratégie nationale d'intelligence artificielle: L'Égypte a lancé une stratégie nationale d'intelligence artificielle visant à utiliser cette technologie pour soutenir la réalisation des objectifs de développement durable, ainsi que pour jouer un rôle clé dans la facilitation de la coopération régionale dans les régions africaine et arabe, et pour consolider la position de l'Égypte en tant qu'acteur international actif dans ce domaine. Cela s'inscrit dans le cadre du désir de l'Égypte d'interagir avec les données de l'ère numérique où les nouveautés technologiques se succèdent chaque jour (40).

B. Stratégie nationale de cybersécurité (2017-2021) : Le Conseil suprême de la cybersécurité, rattaché à la présidence du Conseil des ministres et présidé par le ministre des Communications et des Technologies de l'information, a lancé la stratégie nationale de cybersécurité (2017-2021). L'objectif

stratégique est de faire face aux cybermenaces, de renforcer la confiance dans les infrastructures des communications et de l'information et leurs applications et services dans tous les secteurs vitaux et de les sécuriser afin de créer un environnement numérique sûr et fiable pour la société égyptienne dans toute sa diversité, dans le cadre des efforts de l'État pour soutenir la sécurité nationale et le développement de la société égyptienne [41].

C. Stratégie du cloud computing gouvernemental: La stratégie du cloud computing gouvernemental vise à améliorer l'efficacité et la performance du gouvernement. Elle permet d'optimiser la valeur en augmentant l'efficacité opérationnelle et en répondant plus rapidement aux besoins complexes. Le modèle de cloud computing soutient les agences gouvernementales qui ont besoin de fournir des services très rapides, fiables et innovants malgré les contraintes de ressources [42].

D. Lancement de la stratégie nationale quinquennale de cybersécurité (2023-2027): Le Conseil suprême de la cybersécurité, rattaché à la présidence du Conseil des ministres et présidé par le ministre des Communications et des Technologies de l'information, a lancé la stratégie nationale quinquennale de cybersécurité (2023-2027). L'importance d'une stratégie nationale de cybersécurité réside dans deux points essentiels : premièrement, faire face aux incidents cybernétiques qui ont augmenté en nombre et en provenance, et deuxièmement, créer des opportunités pour le marché égyptien en développant des ressources humaines et en développant une industrie nationale qui contribue à augmenter le produit intérieur brut (PIB) [43].

3. Création de centres nationaux et de conseils spécialisés :

A. Centre national de préparation aux urgences informatiques et réseautiques : Créé en 2009, ce centre a pour objectif de faire face aux cyberattaques et autres menaces cybernétiques. Il fournit un soutien technique et sur le terrain aux secteurs public et financier, et présente des rapports techniques aux autorités compétentes pour protéger les infrastructures nationales d'information critiques, en particulier dans les secteurs des technologies de l'information et des communications et des services financiers. Une équipe spécialisée de haut niveau surveille en permanence la cybersécurité et répond aux incidents, analyse les données forensiques numériques et analyse les logiciels malveillants et l'ingénierie inverse. Son objectif principal est de renforcer la sécurité des infrastructures de communication et d'information égyptiennes en prenant des mesures proactives, en collectant et en analysant les informations relatives aux incidents de sécurité, en coordonnant et en médiatisant entre les parties concernées pour résoudre ces incidents de sécurité et en coopérant au niveau international avec les différentes équipes chargées de répondre aux urgences informatiques et réseautiques dans d'autres pays [44].

B. Centre égyptien de réponse aux urgences informatiques (CERT): L'Autorité nationale de régulation des télécommunications a créé le Centre égyptien de réponse aux urgences informatiques (CERT) en avril 2009. Il est composé d'une équipe de seize spécialistes et fournit un support technique 24 heures sur 24 pour protéger les infrastructures d'information critiques. Depuis 2012, le centre fournit un soutien à divers organismes des secteurs des technologies de l'information et des communications, des services bancaires et gouvernementaux afin de les aider à faire face aux menaces de cybersécurité, notamment les attaques par déni de service. La mission principale du CERT égyptien est de fournir un système d'alerte précoce contre les logiciels malveillants et les cyberattaques à grande échelle contre les infrastructures d'information critiques égyptiennes [45].

C. Création du Conseil supérieur de la sécurité des infrastructures de communication et de l'information (Conseil supérieur de la cybersécurité) : Créé le 16 décembre 2014, il a pour mission de protéger et de sécuriser les infrastructures des communications et des technologies de l'information. Le Conseil supérieur de la cybersécurité a pour objectif d'élaborer des plans stratégiques pour faire face aux cyberattaques, ainsi que de superviser la mise en œuvre des stratégies nationales de lutte contre les menaces cybernétiques. Cette stratégie est mise à jour régulièrement. En outre, le bureau exécutif et le secrétariat technique du Conseil supérieur de la cybersécurité ont été créés. Ils sont chargés de superviser la mise en œuvre des travaux du Conseil et des plans qu'il approuve, conformément aux stratégies et politiques définies. Le secrétariat technique du Conseil est chargé d'effectuer les travaux et les études techniques demandés par le Conseil et son bureau exécutif, d'organiser et de lancer des campagnes nationales de sensibilisation aux risques des menaces cybernétiques dans les différents secteurs, et d'organiser des ateliers et des cours de sensibilisation à la cybersécurité au niveau sectoriel et d'élaborer des spécifications pour des systèmes d'échange d'informations sécurisés concernant la sécurisation des infrastructures d'information de l'État [46].

7. Critères et modèle proposés pour faire face aux risques sociaux des cybercrimes et des cyberattaques sur la sécurité numérique en Égypte :

1. Critères proposés pour faire face aux risques sociaux des cybercrimes et des cyberattaques sur la sécurité numérique :

Premier critère : Élaboration de lois et de réglementations sur la cybersécurité : La lutte contre les cybercrimes et les menaces cybernétiques nécessite l'établissement de bases légales couvrant tous les types de cybercrimes et de menaces persistantes, ainsi que l'élaboration de lois et de réglementations garantissant la protection des droits des individus dans l'espace numérique et la sécurisation de leurs données personnelles,en sensibilisant sur le fait de ne pas partager d'informations personnelles. Il est également nécessaire de renforcer la coopération entre les forces de l'ordre et les appareils judiciaires aux niveaux national et international, et que les lois protègent les enfants et les jeunes dans l'espace numérique.

Deuxième critère : Sensibilisation de la société : La lutte contre les cybercrimes et les menaces cybernétiques nécessite des programmes et des approches suffisants pour sensibiliser les citoyens de tous les horizons et l'implication de la société civile dans leur dynamique.

Troisième critère : Renforcement des partenariats : Avec les secteurs public et privé, les institutions et les organisations internationales, et les parties prenantes.

Quatrième critère : Renforcement des capacités : En élaborant et en mettant en œuvre des programmes de formation reconnus par les universités et les instituts agréés, et en renforçant les capacités des différentes organisations pour exercer leurs fonctions dans le domaine de la cybersécurité, des transactions électroniques et de la transformation numérique.

Cinquième critère : Un environnement propice à la cybersécurité : Il repose sur l'encouragement de la recherche scientifique et de l'innovation dans le domaine de la cybersécurité et de la protection des réseaux et des systèmes d'information, ainsi que sur le renforcement des compétences et la qualification des compétences nationales dans le domaine de la sécurité de l'information et des cybercrimes.

Sixième critère : Mise en place de méthodes pour sécuriser le système de sécurité numérique : Celui-ci doit se concentrer sur trois piliers fondamentaux :

- La prévention des attaques et des menaces cybernétiques : en utilisant des pare-feu et des logiciels de sécurité pour lutter contre les virus, les vers et les logiciels malveillants.
- La détection et la récupération : la détection rapide des menaces et des vulnérabilités et la mise à jour des systèmes.
- La rapidité de réaction : si des attaques sont détectées et non contrées, la détection n'a plus de valeur ni d'importance, il faut donc disposer de capacités de riposte et de défense prêtes à faire face aux différentes attaques.

Septième critère : Innovation et investissement: La lutte contre les risques numériques tels que la cybercriminalité, le terrorisme et les cyberattaques nécessite d'attirer et de former des ressources humaines qualifiées, de renforcer l'innovation et l'investissement et d'exceller dans le domaine de la cybersécurité, en se concentrant sur le développement des infrastructures numériques afin de contribuer à la réalisation de la Vision Égypte 2030.

2. Modèle proposé pour développer et renforcer les systèmes de sécurité numérique et de sécurité de l'information pour faire face aux cybercrimes et aux cyberattaques :

A. Approches pour faire face aux cybercrimes et aux cyberattaques, notamment : * Gouvernance * Sensibilisation des individus * Application de la loi * Coopération internationale * Formation et renforcement des capacités * Soutien à la recherche, au développement et à l'innovation

B. Partenaires pour faire face aux cybercrimes et aux cyberattaques (parties prenantes) : * Organisations gouvernementales * Secteur privé * Organisations internationales * Milieux académiques

C. Outils pour faire face aux cybercrimes et aux cyberattaques : * Conférences * Séminaires * Forums * Commissions * Ateliers * Programmes * Campagnes * Réunions * Accords internationaux

D. Enjeux ciblés : * Cybercriminalité * Cyberattaques * Logiciels malveillants * Cyberterrorisme * Cyberguerre * Cyberespionnage * Cybervandalisme * Intelligence artificielle * Internet des objets * Ingénierie sociale * Blockchain * Résilience cybernétique * Informatique quantique * Biohacking * Fausses identités * Attaques par appareils * Perte de confidentialité

E. Cibles : Au niveau individuel : * Enfants * Étudiants universitaires * Employés * Jeunes victimes de cybercrimes * Jeunes victimes de cyberattaques * Jeunes cybercriminels Au niveau

des États : * Pays où les taux de cybercriminalité sont élevés * Pays victimes de cyberattaques * Pays victimes de cyberterrorisme * Pays victimes de crimes d'ingénierie sociale

F. Résultats visés : * Établir les meilleures pratiques en matière de sécurité numérique et de cybersécurité et leurs contrôles de sécurité et techniques. * Réduire l'impact des risques, des attaques et des cybercrimes. * Améliorer les capacités de gestion des incidents numériques et de sécurité. * Construire un cadre réglementaire pour protéger les technologies actuelles et émergentes. * Détecter les cyberattaques et renforcer les méthodes de récupération après incident.

8. Résultats de l'étude et propositions :

1. Résultats :

L'étude a abouti à plusieurs résultats et recommandations que l'on peut résumer comme suit:

- Il existe un certain nombre de définitions nationales et internationales des termes cybersécurité, sécurité numérique et cybercriminalité. Les concepts évoluent constamment en raison des développements technologiques et des nouvelles technologies, ainsi que des changements dans les systèmes de communication et les technologies de l'information. Il est très difficile de donner une définition exhaustive de la sécurité numérique en raison de sa nouveauté d'une part, et des différences d'interprétation entre les chercheurs d'autre part.
- La sécurité numérique est une nécessité urgente imposée par le développement technologique et le processus de transformation numérique pour garantir la sécurité et la protection des informations et des technologies de l'information et de la communication.
- Il est difficile de recenser les types de cybercrimes et de cyberattaques, car les criminels utilisent des techniques et des méthodes liées aux progrès technologiques qui changent de plus en plus rapidement.
- Les résultats de l'étude ont montré que les auteurs de cyberattaques exploitent les vulnérabilités connues des individus, des organisations et des États, ce qui entraîne une faible capacité à classer les dommages et une augmentation des risques qui en résultent, ainsi qu'une difficulté à déterminer précisément les coûts directs et indirects qui en découlent.
- Les résultats ont montré que les cybercrimes et les cyberattaques ont un impact extrêmement grave sur le tissu social des pays, car ce sont des crimes transfrontaliers qui ciblent les infrastructures et les activités sociales liées aux individus et à la société dans son ensemble.
- Les cybercrimes et les cyberattaques constituent une menace grave et croissante, et les coûts de lutte contre les effets qui en résultent et de leur découverte sont très élevés pour les États car ils dépendent entièrement de la technologie et des technologies modernes et avancées.
- Les cybercrimes et les cyberattaques sapent la confiance des individus dans les gouvernements car ils sont capables de causer des dommages considérables, ce qui oblige le gouvernement à protéger ses citoyens contre une nouvelle génération de cyberattaques.
- Les résultats ont montré que la plupart des pays du monde ont été victimes de nombreux cybercrimes et cyberattaques qui ont ciblé des secteurs vitaux de la société, et ont donc adopté diverses lois afin de surmonter les menaces et les dangers qui en résultent.
- Les résultats ont montré que l'Égypte est l'un des premiers pays à avoir adopté des lois et des réglementations,à avoir créé des centres et des conseils spécialisés, et à avoir élaboré de nombreuses stratégies comprenant divers programmes stratégiques différents, et à avoir organisé des conférences afin de protéger le pays contre les risques de cybercrimes et de cyberattaques, et pour créer un environnement numérique sûr et fiable pour la société égyptienne dans toute sa diversité.

2. Propositions :

À la lumière des résultats, l'étude propose ce qui suit :

1. Sensibilisation du public: La lutte contre les cybercrimes et les menaces cybernétiques nécessite de fournir davantage de connaissances et de sensibilisation aux utilisateurs d'Internet et des réseaux sociaux afin d'éviter les incidents et les dommages cybernétiques directs et indirects auxquels ils peuvent être exposés ou victimes, et de réduire les coûts supportés par l'État pour y faire face.
2. Mise en œuvre de stratégies, de lois et de politiques de sécurité numérique: Car elles sont un moyen d'assurer la sécurité nationale de l'Égypte et de diffuser une culture de la sécurité numérique parmi les différents segments de la société, en l'intégrant dans les différents plans et stratégies à tous les niveaux régionaux et internationaux, afin d'assurer la sécurité

cybernétique et la sécurité de l'information en ligne avec les changements rapides.

3. Les universités, les instituts et les différentes organisations doivent s'intéresser au développement d'un programme de cybersécurité et à son enseignement, afin qu'il devienne une exigence universitaire, afin de disposer de l'expertise scientifique et technique nécessaire pour faire face aux attaques et aux menaces cybernétiques évolutives et changeantes.
4. Les décideurs politiques, les universitaires et les spécialistes doivent réfléchir aux meilleurs moyens de mettre en œuvre le concept de gestion des risques liés à la protection de la vie privée et des données et des informations contre les menaces potentielles.
5. La confiance est essentielle dans l'environnement numérique et dans le développement de stratégies de protection de la vie privée et de lutte contre les vulnérabilités et les nouvelles menaces émergentes, et de faire face aux risques de sécurité et aux problèmes de confidentialité, il faut donc prêter attention à l'éthique de la construction de la confiance car elle affecte l'environnement numérique.
6. Les décideurs doivent traiter les risques de sécurité numérique comme une menace pour la sécurité politique, économique, sociale et technologique.
7. Les stratégies nationales visant à assurer la sécurité numérique doivent refléter la vision de la société et renforcer la protection de la vie privée dans l'espace numérique qui repose sur les données comme élément fondamental.
8. Les stratégies de sécurité numérique contribueront à renforcer la coopération avec les parties prenantes et à tirer parti de leurs avantages, et à établir les meilleures pratiques et à trouver les solutions possibles pour gérer les risques de l'espace numérique et à promouvoir les bonnes pratiques de gestion des risques.
9. Les institutions et les petites et moyennes entreprises doivent sensibiliser les responsables de la gestion des technologies numériques aux risques liés à la vie privée.
10. Renforcer la sensibilisation au concept de citoyenneté numérique chez les jeunes âgés de 18 à 40 ans sur la manière d'interagir avec l'environnement numérique et les outils technologiques pour réaliser des bénéfices personnels et communautaires de manière positive.
11. Sensibiliser à l'utilisation sécurisée des cartes électroniques pour lutter contre les utilisations illégales dans les transactions électroniques.
12. Publier régulièrement des bulletins d'information sur les cybercrimes et les menaces cybernétiques et les moyens d'y faire face.
13. Qualifier les employés de différents secteurs, en particulier le secteur de la sécurité de l'information, sur les nouveautés et les développements dans le domaine des technologies de l'information et des communications afin de les limiter et de les combattre.
14. Il faut accélérer les efforts pour mettre en œuvre les législations sur l'intelligence artificielle conformément à la vision Égypte 2030 et à la stratégie nationale de cybersécurité.

References:

(1) OECD Digital Economy Papers Managing Digital security and Privacy Risk, 2016 Ministerial Meeting on the Digital Economy, Back Growth Report the Digital Economy innovation, Growth and social prosperity, 2016, p, 5.

(2) Oced digital Economy papers ,Op cit p.5

(3) Bernat :Enhancing the digital security of critical activities, Going Digital Toolkit Note, 2021 No. 17. P.4.

(4) Op. Cit, P. 4.

(٥) ذياب البدانية : الجرائم الإلكترونية، المفهوم والأسباب، ورقة مقدمة فى الملتقى العلمى- الجرائم المستحدثة فى ظل التغيرات والتحولات الإقليمية والدولية ٢-٤/٩/٢٠١٤م عمان - الأردن.

(٦) فوزى حسين الزبيدى : منهجية تقييم مخاطر الأمن القومى : دراسة تحليلية لمنهجية تقييم مخاطر الأمن القومى NSRA، رؤى استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، المجلد (٣) العدد (١١)، ٢٠١٥م، ص ١١ى.

(٧) أولريش بك، مجتمع المخاطر العالمى بحثًا عن الأمن المفقود، ترجمة علا عادل وآخرون، القاهرة، المركز القومى للترجمة، ٢٠١٣م، ص٢١٤.

(8) Jarvis, Darry I S "Theorizing Risk: Ulrich Beck, Globalization and Risk of the Risk society" Lee Kaun Yew School of public policy, National University of sing pore , p 3

(٩) نجـوان أحمد عاصم عبد الجـواد : الجريمة السيبرانية وتأثيرها على الأمن القومى المصرى، دراسة سوسيو تحليلية، جامعة الفيوم، مجلة كلية الآداب، الإنسانيات والعلوم الاجتماعية، المجلد (١٥)، العدد (١) يناير ٢٠٢٣م، ص ٢١٠٤.

(١٠) إسلام فوزى : الأمن السيبرانى، الأبعاد الاجتماعية والقانونية، تحليل سوسيولوجى، القاهرة، المجلة الاجتماعية القومية، المجلد السادس والخمسون، العدد الثانى، مايو ٢٠١٩م.

References:

(١١) مكتب الأمم المتحدة المعنى بالمخدرات والجريمة : دراسة شاملة عن الجريمة السيبرانية، فيينا، ٢٠١٣م، ص ٧.

(12) Suhasini Verma, (et. al): Mounting Cases of Cyber- Attacks and Digital payment. India, 2023.P.61

(13) Yuchong Li, &, Qinghui Liu: A Comprehensive Review Study of Cyber- attacks and Cyber Security; Emerging trends and recent developments Energy reports,2021, P.8179.

(١٤) سامى محمد بونيف : دور الاستراتيجيات الاستباقية فى مواجهة الهجمات السيبرانية، الردع السيبرانى إنموذجًا.المجلة الجزائرية للحقوق والعلوم السياسية، المجلد (٤) العدد (٧)، ٢٠١٩م، ص ١٢

(15) Yuchong Li, & Qinghui, Liu, 2021 op. cit., P.8180

(١٦) خورجى فلوريس كابيخاس، عائشة عفيفى، نيكولاى لوزنيسكى : الأمن السيبرانى فى مؤسسات منظومة الأمم المتحدة تقرير وحدة التفتيش المشتركة، الأمم المتحدة ، ٢٠٢١م، ص٧.

(١٧) أمنية عبيشات: الأمن الرقمى – قراءة فى مفهومه واستراتيجية حمايته، مجلة المسار للدراسات القانونية والسياسية، المجلد (١) العدد (١) ٢٠٢٣م، ص ١٠٠ .

(١٨) مركز هردو لدعم التعبير الرقمى: الأمن الرقمى وحماية المعلومات، الحق فى استخدام شبكات آمنة، القاهرة ،٢٠١٧ ، ص ٦

(١٩) أمينة عبيشات (٢٠٢٣م): مرجع سابق ، ص ٩٩.

(20) Sakshi Singh&Suresh Kumar: THE TIMES OF CYBER ATTACKS: ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering TOME XIII 2020 FASCICULE 3, July – September, P 134-135

(٢١) نشرة تكنولوجيا المعلومات والاتصالات للتنمية فى المنطقة العربية – اللجنة الاقتصادية والاجتماعية لغربى آسيا (الإسكوا): الأمم المتحدة نيويورك، العدد (١٨) ٢٠١٢م، ص ١٠ .

(22) Digital Notes on cyber security, Department of information technology, Malla Reddy College of Engineering & Technology India ,2021, pp7-9

(٢٣) الاستراتيجية الوطنية للأمن السيبرانى (٢٠٢٣م -٢٠٢٧م)، وزارة الاتصالات وتكنولوجيا المعلومات.

(٢٤) خورخى فلوريس كابيخاس، عائشة عفيفى، نيكولاى لوزنيسكى ٢٠٢١م. مرجع سابق ، ص ١٤

(25) Lynn Batten, & Gang Li, : Application and Techniques in information security international conference Atis 6 th . Osaka University, Osaka, Japan.2016 P, 60

(٢٦) تقرير (TTU) الوثيقة RPM-ARB 1044- A قطاع تنمية الاتصالات، الاجتماع الإقليمى التحضيرى للمؤتمر العالمى لتنمية الاتصالات ٢٠١٠م لمنظمة الدول العربية، دمشق، الجمهورية العربية السورية، ١٧-١٩ يناير ٢٠١٠م.

(27) Nadiya Kostyuk, & yuri M. Zhukov: Invisible Digital front can cyber Attacks Shape Battlefield Events. Journal of Conflict Resolution, Vol 63 (2), 2019, P. 318.

(28) Hemraj, Saini, & Yerra shanker Rao, & T.C Panda: cyber- crimes and their Impacts, A review. International Journal of Engineering research and Application (IJERA) no/2. 2012, P 209

(29) Mario Spremié, & Alen Simunic,: Cyber Security Challenges in Digital Economy,2018. P 979.

(30) Proceedings of the world congress on Engineering No/ 1 London

(31) Mario Spremié, &, Alen, Simunic ,Op. cit., p 979

(32) Ryan Shandler, &, Miguel Alberto Gomez: The hidden threat of cyber- attacks- undermining public confidence in government, Journal of information technology & politics .2022 p 363

(٣٣) إسلام فوزى : مرجع سابق ، ص ١١٢ – ١١٣.

(34) James A. Lewis: Op Cit.

(٣٥) الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧م - ٢٠٢١م).

(36) https://mcit.gov.eg/Ar/Media_Center/Press_Room/Press_Releases/67460

تاريخ الدخول ٢٤/٤/ ٢٠٢٤م الساعة ١١,٥٠ مساء

(٣٧) الدستور المصرى ٢٠١٤م.

(٣٨) القانون رقم ١٧٥ لسنة ٢٠١٨م قانون مكافحة جرائم تنقية المعلومات.

(٣٩) القانون رقم ٩٤ لسنة ٢٠١٥م لمكافحة الإرهاب.

(٤٠) الاستراتيجية الوطنية للذكاء الاصطناعى، يوليو ٢٠٢١م . وزارة الاتصالات وتكنولوجيا المعلومات .

(٤١) الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧م – ٢٠٢١م) .

(٤٢) استراتيجية الحوسبة السحابية الحكومية ، ٢٠١٤ م ، وزارة الاتصالات وتكنولوجيا المعلومات .

(٤٣) الاستراتيجية الوطنية للأمن السيبرانى (٢٠٢٣م – ٢٠٢٧م) .

(٤٤) مصر والأمن السيبرانى : الهيئة العامة للاستعلامات https://www.sis.gov.eg/Story/258293 تاريخ الدخول ٢٥/٤/٢٠٢٤م الساعة ١١:٤٧ مساء

(٤٥) المرجع السابق

(٤٦) المرجع السابق

Répercussions et Risques Sociaux des Crimes et des Attaques Cybernétiques Contre la Sécurité Numérique et les Mécanismes de Lutte à la lumière de la vision de l'Égypte 2030

■ *Dr. Asmaa Jaber Mehran*

Professeure Adjointe de Sociologie Criminelle - Faculté des Lettres - Université d'Assiout

Résumé:

La présente étude a visé à fournir une analyse sociologique des risques sociaux des crimes et des cyberattaques sur la sécurité numérique et à suivre les mécanismes et les efforts de l'État égyptien à la lumière de la Vision 2030. Les résultats ont montré que la sécurité numérique est une nécessité urgente imposée par le développement technologique et le système de transformation numérique pour garantir la sécurité et la protection de l'information et des technologies de l'information et de la communication.

Les résultats ont montré que la plupart des pays du monde ont été exposés à de nombreux crimes et cyberattaques qui ont ciblé des secteurs vitaux de la société, et ont ensuite adopté diverses lois afin de surmonter les menaces et les dangers qui en résultent. Les résultats ont montré que l'Égypte est l'un des premiers pays à avoir adopté des lois et des réglementations, à avoir créé des centres et des conseils spécialisés, à avoir élaboré de nombreuses stratégies qui comprennent divers programmes stratégiques différents, et à avoir organisé des conférences afin de protéger l'État des dangers des crimes et des cyberattaques, et pour créer un environnement numérique sûr et fiable pour la société égyptienne de tous les walks of life.

Mots-clés: Cybercrimes, Cyberattaques, Sécurité Numérique, Vision Égypte 2030

الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى وآليات المواجهة فى ضوء رؤية مصر ٢٠٣٠

■ أ.م.د/ أسماء جابر مهران

أستاذ علم اجتماع الجريمة المساعد – كلية الآداب – جامعة أسيوط

المستخلص :

هدفت الدراسة الراهنة إلى تقديم تحليل سوسيولوجى للمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى ورصد آليات وجهود الدولة المصرية فى ضوء رؤية مصر ٢٠٣٠ .

لقد أظهرت النتائج أن الأمن الرقمى يعد ضرورة ملحة فرضها التطور التكنولوجى ومنظومة التحول الرقمى لضمان سلامة وأمن المعلومات وتكنولوجيا الاتصالات .

بيَّنت النتائج أن معظم دول العالم تعرَّضت للعديد من الجرائم والهجمات السيبرانية التى استهدفت القطاعات الحيوية فى المجتمع، ومن ثم قامت بإصدار القوانين المختلفة من أجل التغلب على التهديدات والأخطار الناجمة عنها. أوضحت النتائج أن مصر من أوائل الدول التى قامت بسن التشريعات والقوانين وإنشاء المراكز والمجالس المتخصصة، ووضع الكثير من الاستراتيجيات التى تتضمن العديد من البرامج الاستراتيجية المختلفة، وعقد المؤتمرات من أجل حماية الدولة من مخاطر الجرائم والهجمات السيبرانية، ولتحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصرى بمختلف أطيافه.

الكلمات المفتاحية : الجرائم السيبرانية، الهجمات السيبرانية، الأمن الرقمى، رؤية مصر ٢٠٣٠