مجلة البحوث الإعلامية

مجلة علمية محكمة تصدر عن جامعة الأزهر/كلية الإعلام

المراسلات:

- القاهرة- مدينة نصر - جامعة الأزهر - كلية الإعلام - ت: ٠٢٢٥١٠٨٢٥٦
- الموقع الإلكتروني للمجلة: http://jsb.journals.ekb.eg
- البريد الإلكتروني: mediajournal2020@azhar.edu.eg

- العدد الثامن والخمسون - الجزء الرابع - ذو القعدة ١٤٤٢هـ - يوليو ٢٠٢١ م
- رقم الإيداع بدار الكتب المصرية ٦٥٥٥
- الترقيم الدولي للنسخة الإلكترونية: ٢٦٨٢-٢٩٢ x
- الترقيم الدولي للنسخة الورقية: ٩٢٩٧-١١١٠

الهيئة الاستشارية للمجلة

قواعد النشر

تقوم المجلة بنشر البحوث والدراسات ومراجعات الكتب والتقارير والترجمات وفقًا للقواعد الآتية:

- **يعتمد النشر على رأي اثنين من المحكمين المتخصصين في تحديد صلاحية المادة للنشر.**
- **ألا يكون البحث قد سبق نشره في أي مجلة علمية محكمة أو مؤتمرًا علميًا.**
- **لا يقل البحث عن خمسة آلاف كلمة ولا يزيد عن عشرة آلاف كلمة ... وفي حالة الزيادة يتحمل الباحث فروق تكلفة النشر.**
- **يجب ألا يزيد عنوان البحث –الرئيسي والفرعي- عن ٢٠ كلمة.**
- **يرسل مع كل بحث ملخص باللغة العربية وآخر باللغة الانجليزية لا يزيد عن ٢٥٠ كلمة.**
- **يزود الباحث المجلة بثلاث نسخ من البحث مطبوعة بالكمبيوتر .. ونسخة على CD، على أن يكتب اسم الباحث وعنوان بحثه على غلاف مستقل ويشار إلى المراجع والهوامش في المتن بأرقام وترد قائمتها في نهاية البحث لا في أسفل الصفحة.**
- **لا ترد الأبحاث المنشورة إلى أصحابها .... وتحتفظ المجلة بكافة حقوق النشر، ويلزم الحصول على موافقة كتابية قبل إعادة نشر مادة نشرت فيها.**
- **تنشر الأبحاث بأسبقية قبولها للنشر .**
- **ترد الأبحاث التي لا تقبل النشر لأصحابها.**

محتويات العدد

م	القطاع	اسم المجلة	اسم الجهه / الجامعة	نقاط المجلة (مارس 2020)	نقاط المجلة (يوليو 2020)	ISSN-P	ISSN-O
1	الدراسات الإعلامية	مجلة البحوث الإعلامية	جامعة الأزهر	6.5	7	1110-0297	2682-292X
2	الدراسات الإعلامية	مجلة بحوث العلاقات العامة الشرق الأوسط	الجمعية المصرية للعلاقات العامة	6	7	2314-8721	2314-873X
3	الدراسات الإعلامية	المجلة العربية لبحوث الإعلام و الإتصال	جامعة الأهرام الكندية	5	5	2536-9393	
4	الدراسات الإعلامية	مجلة إتحاد الجامعات العربية لبحوث الإعلام و تكنولوجيا الإتصال	Cairo University	4	4	2356-9891	
5	الدراسات الإعلامية	المجلة العلمية لبحوث الإعلام و تكنولوجيا الإتصال	جامعة جنوب الوادى	3.5	3.5	2536-9237	
6	الدراسات الإعلامية	مجلة البحوث و الدراسات الإعلامية	اكاديمية الشروق	3.5	5.5	2357-0407	
7	الدراسات الإعلامية	المجلة العلمية لبحوث العلاقات العامة والإعلان	جامعة القاهرة – مركز بحوث الرأى العام	3	5.5	2356-9131	
8	الدراسات الإعلامية	المجلة العلمية لبحوث الإذاعة والتلفزيون	جامعة القاهرة – مركز بحوث الرأى العام	3	5.5	2356-914X	
9	الدراسات الإعلامية	المجلة العلمية لبحوث الصحافة	جامعة القاهرة – مركز بحوث الرأى العام	3	5.5	2356-9158	
10	الدراسات الإعلامية	المجلة المصرية لبحوث الإعلام	جامعة القاهرة – مركز بحوث الرأى العام	3	5.5	1110-5836	
11	الدراسات الإعلامية	المجلة المصرية لبحوث الرأى العام	Cairo University, Center of Public Opinion Research	3	6.5	1110-5844	

- يطبق تقييم مارس 2020 للمجلات على كل الأبحاث التى نشرت فيها قبل 1 يوليو 2020
- يطبق تقييم يوليو 2020 للمجلات على كل الأبحاث التى ستنشر فيها بدء من 1 يوليو 2020 و حى صدور تقييم جديد في يوليو 2021
- المجلات التي لم تتقدم بطلب إعاده تقييم سيظل تقييم مارس ٢٠٢٠ مطبقا علي كل الأبحاث التي ستنشر بها وذلك لحين صدور تقييم جديد في يوليو 2021
- يتم إعاده تقييم المجلات المحلية المصرية دورياً في شهر يوليو من كل عام ويكون التقييم الجديد سارياً للسنة التالية للنشر في هذه المجلات

استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزاً لرؤية مصر 2030: دراسة استشرافية

Strategies for Combating cybercrimes in the Information Age in support of Egypt's 2030 vision: A prospective study

أ.م. د. أميرة محمد محمد سيد أحمد

أستاذ الصحافة المساعد- كلية الآداب - جامعة دمياط.

mera308ahmed@gmail.com

ملخص الدراسة

سعت الدراسة لوضع رؤية استراتيجية نموذجية متكاملة لمكافحة الجرائم الإلكترونية من زوايا مختلفة يمكن تطبيقها على كافة المستويات، والتي من شأنها حماية المجتمع من الشائعات والأخبار المضللة المثارة على مواقع التواصل الاجتماعي، وتأمين سلامة عمل قطاعات الدولة المختلفة من خلال تحقيق الأمن لها من أي اختراقات وتعزيز الحفاظ على الأمن القومي -من خلال استطلاع آراء الخبراء والمتخصصين- عبر ثلاث جولات مختلفة بتطبيق أسلوب دليفي، وأسلوب التخطيط الاستراتيجي، وتوصلت الدراسة إلى: تعدد أسباب وأساليب انتشار تلك الجرائم، وتنوع تهديداتها على الأصعدة الاجتماعية والسياسية والأمنية والاقتصادية، كما تعددت الآليات المقترحة ما بين الآليات القانونية والأمنية والتقنية والإعلامية والتربوية والتعليمية، والفنية والدولية للحد من مخاطر وانتشار تلك الجرائم والحفاظ على الأمن السيبراني، وسلامة المجتمع وشبكات البنية الحيوية التحتية وتدعيمها بكل وسائل الأمن والحماية.

الكلمات المفتاحية: الجرائم الإلكترونية- الأمن القومي- أسلوب دليفي– التخطيط الاستراتيجي- رؤية مصر 2030.

Abstract

In this study, a strategy has been developed for cybercrimes prevention. Many aspects have been considered in the strategy and they can be applied at different levels. In addition to protecting society from rumors, and misinformation on social media, the strategy aims to ensure the integrity of the work of different public sectors by ensuring their security from any intrusions which will enhance the maintenance of national security.

By exploring the views of experts and specialists through three different rounds using a Delphi method and a strategic planning method, the study concluded the following: First, there are many reasons and methods for the spread of cybercrimes. Second, because of the cybercrimes, there are a variety of threats on social, political, security, and economic levels. Third, many mechanisms are proposed to reduce the risks and spread of such crimes, maintain infrastructure security and social safety. These mechanisms range from legal, security, technology, media, education mechanisms to effective international collaboration.

Key words: Cybercrimes, - National Security - Delphi method- strategic planning- - Egypt Vision 2030

مقدمة:

في ظل الحراك المعلوماتي والتطور التكنولوجي الهائل في مجال تقنية المعلومات والاتصال واقتصاد المعرفة، وفي ظل الانفتاح المعلوماتي والعولمة الرقمية، وبروز تقنيات الثورة الصناعية الخامسة والذكاء الاصطناعي في مختلف القطاعات، وفي ظل التحول الرقمي للدول وتضاعف الاعتماد على المنصات الرقمية ووسائلها الاتصالية، سواء في التعليم، والعمل، والاستشارات الطبية، وعقد المؤتمرات، وغيرها من المجالات؛ نتيجة لما فرضته جائحة كورونا (كوفيد 19) من عزلة وتباعد اجتماعي، الأمر الذي أسهم بالفعل في زيادة تفشي معدل الهجمات السيبرانية أو الهجمات على خدمات البنية التحتية الحيوية للدول في الفترات الأخيرة، وزيادة معدل انتشار الشائعات والمعلومات المفبركة، حيث ظهرت أشكالًا عدة للجرائم الإلكترونية وتوسع إطارها في العصر الحديث، موظفة أسلحة رقمية على اختلاف أشكالها تلائم طبيعة سياق العصر الرقمي: كالبريد الإلكتروني، ومواقع التواصل الاجتماعي وتقنيات الذكاء الاصطناعي، كتوظيف البرامج التقنية المتطورة، وتقنيات الحوسبة السحابية (I Cloud)، وتكنولوجيا إنترنت الأشياء، والبيانات الضخمة، الخوارزميات، على اختلاف أشكالها في تصميم البرمجيات الخبيثة (Malicious Code)، لضرب الأمن المعلوماتي للبنية الحيوية للدول، حتى أصبح السيطرة عليها بشكل فردي أمرًا غاية في الصعوبة لكافة دول العالم، لعدم مواكبة التحولات الرقمية للديناميكية المستمرة لطبيعة مخاطر وتهديدات تلك النوعية من الجرائم.

وتعددت أشكال تلك الجرائم المستحدثة على النطاق الدولى بشكل متطور، ومن أبرز أشكالها: الإرهاب الرقمى، التزوير بمختلف أشكاله، انتهاك حقوق الملكية الفكرية وبراءات الاختراع، الاعتداء على خصوصية الأفراد، الملاحقة، التشهير، الهجمات الرقمية، الشائعات الموجهة، الحرب النفسية، الاحتيال المعلوماتى واختراق بيانات المواقع الرسمية للدول وتعطيل خدماتها، وقرصنة وتسريب المعلومات الحساسة السرية

والتلاعب الفعال بها،وغيرها من الجرائم التى تستهدف أمن الدولة الاستراتيجى وأمنها المعلوماتى، كاستخدام المنظمات الإرهابية لأساليب التضليل الفكرى للشباب، لضرب الأمن الفكرى للدول واستقطاب الشباب في القضايا الفكرية المتطرفة ودعم وتمويل الإرهاب وغيرها من الجرائم.

تلك الجرائم لها تحدياتها القانونية والأمنية والتقنية وخطورتها على البنية الحيوية للدول ولأنظمتها وهجماتها المستمرة، ولها تأثيرها السلبى على جميع النواحى وعلى الاقتصاد الدولى كافة، والتى تنعكس بدورها على الهوية الوطنية والأمن القومى للبلاد، الأمر الذى يتطلب ضرورة التصدى بحزم لهذا النوع من الجرائم، واختلفت الدول في طرق التصدى لتلك النوعية من الجرائم على المستوى الوطنى، فظهرت إشكاليات عدة في هذا الصدد سواء على المستويات كافة، ومع ذلك زاد انتشار تلك الجرائم بشكل غير مسبوق في العصر الحديث، نتيجة لتطور آليات وأساليب تنفيذها من قبل المجرم المعلوماتى، الأمر الذى يستدعى من كافة الجهات استحداث ترسانة وآليات وقائية فعالة للتصدى لهذا النوع من الجرائم، وكيفية مواجهتها من النواحى التشريعية والقضائية، والتقنية والأمنية، والإعلامية والتعليمية والدولية، فهناك حاجة ماسة لحماية الفضاء المعلوماتى وأمنه بكافة الأشكال والوسائل والأساليب والاستراتيجيات، وإلى زيادة درجة الوعى الأمنى من خلال توعية المجتمع بخطورتها بمختلف الوسائل والطرق عبر منصات وسائل الإعلام الجديد في كيفية محاربة الجرائم بشتى أنواعها ولمهاجمة تحديات بناء الثقة في مجتمع المعلومات، لتحقيق بيئة أمنة وبناء مجتمع معرفي أمن، ومن هنا جاءت فكرة الدراسة.

الدراسات السابقة:

يعد الرجوع للدراسات السابقة خطوة مهمة وأساسية في البحث العلمي، ويمكن تناول أبرز الدراسات في هذا المجال كما يأتي: -

1- **دراسة: Ahmed Alkaabi (2020)**

سعت الدراسة لوضع استراتيجيات للمساعدة في الحد من الجرائم الإلكترونية وتعزيز الأمن السيبراني، باستخدام الاستبيان كأداة لجمع البيانات وتحليل المستندات الحكومية للتعرف على تلك الجرائم، وتوصلت الدراسة أن معظم الهجمات الإلكترونية تنشأ بسبب خطأ بشري يرتبط بنقص المعرفة حول اختلاف ديناميات الجرائم الإلكترونية والأمن السيبراني، وأن زيادة المعرفة والوعي من قبل موظفي تكنولوجيا المعلومات وغيرهم من الموظفين المعنيين بديناميات الأمن السيبراني يعد ضروريًا للغاية في الحد من تلك

الجرائم، كما توصلت أن المراقبة والتنبيهات المناسبة هى الاستراتيجية الأكثر فاعلية لمنع الجرائم الإلكترونية وتعزيز الأمن السيبراني، يليها اكتساب المعرفة حول الأمن السيبراني، ثم تعزيز إدارة المخاطر واتخاذ القرار، ثم تطوير التقنيات والبرامج، وإنشاء فريق أمني قوي، وتطبيق قوانين الأمن السيبراني، يليها التخصيص الفعال للموارد [1].

2- **دراسة: Mohammed I. Alghamdi (2020)**

سعت الدراسة لتطوير رؤية استراتيجية لمكافحة الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، من خلال التعرف على طبيعة وأنواع الجرائم الإلكترونية وأبعاد الأمن السيبراني، ودور مكافحة الجرائم الإلكترونية في تعزيز الأمن السيبراني، باستخدام الاستبيان كأداة لجمع البيانات، وتوصلت الدراسة لعدة نتائج من أهمها: تمثلت أبعاد الرؤية الاستراتيجية التطويرية في: مراقبة الشبكة وإعدادات التنبيه للكشف عن الأنشطة المشبوهة يعد مهمًا للغاية، تقييم المخاطر، وتطوير سياسة الأمن السيبراني، توظيف أحدث لتقنيات الأمان والمعدات اللازمة للكشف عن التهديدات والمخاطر والتصدي لها، تعزيز وتنسيق سياسات التعاون التنظيمي بين القطاعين العام والخاص؛ التأكيد على الحاجة إلى القيم الأساسية مثل أمن البيانات الشخصية وحرية التعبير والتدفق الحر للمعلومات؛ والدعوة إلى تعاون دولي مشترك [2].

3- **دراسة محمد حميد، مصطفى جاد الحق (2019)**

سعت الدراسة لوضع رؤية استراتيجية لمكافحة الجرائم السيبرانية، باستخدام الاستبيان كأداة لجمع البيانات، وباستخدام المنهج الوصفي التحليلي، وتوصلت الدراسة لعدة نتائج من أبرزها: تتمثل استراتيجيات مكافحة تلك النوعية من الجرائم لتعزيز الأمن الإنساني في: تنمية الوعي المجتمعي بمخاطر ارتكاب تلك الجرائم، ورفع نسبة الكفاءة الوطنية والوسائل المستخدمة لحماية البنية التحتية الوطنية [3].

4- **دراسة: محمد مسعد (2019)**

سعت الدراسة لوضع رؤية استراتيجية لمكافحة الجرائم السيبرانية تعزيزًا للأمن الإنساني، باستخدام المنهج الوصفي التحليلي، وبالاعتماد على الاستبيان كأداة لجمع البيانات، وتوصلت لعدة نتائج، تمثلت الرؤية الاستراتيجية في: إنشاء نيابة متخصصة للتحقيق، ومواجهة وضبط كافة أنواع الجرائم السيبرانية، إنشاء وحدة أمنية نوعية بوزارة الداخلية متخصصة، سرعة إعداد قانون الأمن السيبراني ليحدد ضوابط عمل المشغلين مقدمي خدمة الاتصالات ويعزز مكافحة الجرائم في اليمن، وحماية المجتمع سيبرانيًا [4].

5- **دراسة: علي الشهري (2019)**

سعت الدراسة لوضع رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني، من خلال التعرف على طبيعة تلك الجرائم وأسبابها، والوقوف على التهديدات والمخاطر التي تعترض الأمن السيبراني في السعودية، باستخدام المنهج الوصفي، وبالاعتماد على أداتي الاستبيان و S.W.O.T كأدوات لجمع البيانات، وتوصلت الدراسة لعدة نتائج لعل من أبرزها: الجرائم الإلكترونية لا تعترف بأي حدود مكانية أو زمنية، وأن التقنيات الحديثة وفرت فرصًا غير مسبوقة لانتشارها، وأن انتهاك السياسات الأمنية الخاصة بالأمن السيبراني تمثل أهم التهديدات التي تواجه الفضاء السيبراني، وتمثلت ملامح الرؤية المقترحة في : تطبيق التشريعات والأنظمة في مواجهة تلك الجرائم من خلال إنشاء المزيد من المحاكم المختصة، تطوير التقنيات الحالية لرفع كفاءة رصد تلك الجرائم وملاحقتها، تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم الإلكترونية والأمن السيبراني. [5]

6- **دراسة: بدرة لعو (2018)**

سعت الدراسة إلى التعرف على مدى فاعلية الهيئة الوطنية للحد من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لتحقيق الأمن الإلكتروني، باستخدام المنهج التحليلي، للمرسوم الرئاسي رقم 261/15، والمنهج المقارن للتشريعين الفرنسي والإماراتي، وتوصلت الدراسة لعدة نتائج من أهمها: أغفل المشروع الجزائري دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها في الحالات الطارئة، كما أغفل ضبط القواعد القانونية الخاصة بالاحتفاظ بالمعلومات المستقاة من خلال أداء الهيئة لمهامها وإتلافها في المرسوم الرئاسي. [6]

7- **دراسة: عبدالاله عوض المطيري (2018)**

سعت الدراسة إلى التعرف على دور الإعلام الرقمي في التوعية بالجرائم الرقمية، باستخدام المنهج الوصفي التحليلي، وبالاعتماد على الاستبيان كأداة لجمع البيانات، وتوصلت الدراسة لعدة نتائج من أبرزها: ضرورة الحاجة لاستخدام منصات الإعلام الرقمي لزيادة درجة الوعي الأمني من خلال توعية الجماهير، بالأساليب المتبعة لاستقطاب الشباب في القضايا الفكرية، التركيز على موقع تويتر في نشر التوعية بتلك الجرائم، كما أشارت إلى ضرورة إنشاء وحدات متخصصة مثل الشرطة الإلكترونية للحد من مخاطر تلك الجرائم. [7]

8- **دراسة: ميادة بشير، يوسف عثمان (2018)**

استهدفت معرفة دور العلاقات العامة في التوعية بالجرائم الإلكترونية بالتطبيق على عدة هيئات تمثلت في: وزارة الداخلية، وزارة الاتصالات، المركز القومي للمعلومات، المركز السوداني لأمن المعلومات، وزارة العدل ، والهيئة القومية للاتصالات، باستخدام المنهج الوصفي ، وبالاعتماد على عدة أدوات منها : الاستبيان والمقابلة والملاحظة ، وتوصلت لعدة نتائج من أهمها: نجحت الإدارات في عقد شراكات واتفاقيات بخصوص التوعية بمخاطر الجرائم الإلكترونية، ومن أكثر الوسائل الإعلامية كانت الصحف والتليفزيون، لكنها لم تهتم باستخدام الإعلام الرقمي في التوعية، كما توصلت أن هناك اتفاقيات بين إدارة العلاقات العامة بالجهات التشريعية والتنفيذية، لتكوين هيئات للتوعية بقضايا التكنولوجيا. [8]

9- **دراسة: لورنس الحوامدة (2017)**

سعت الدراسة لبيان مكافحة الدول للجرائم المعلوماتية من خلال وضع التشريع المنظم لها، بالاعتماد على المنهجين المقارن والتحليلي للنصوص القانونية في كل من السعودية والإمارات والبحرين والأردن، وتوصلت لعدة نتائج مفادها: الجهود الوطنية لا تزال دون المستوى المطلوب لمواجهة مخاطر تلك الجرائم، وأيضًا صدور الاتفاقية العربية لمكافحة تلك الجرائم الموقعة في 2010/12/21م تعد نقطة تحول في التعاون العربي لمكافحتها، وأغلبية تلك الجرائم تحتاج لتوافر القصد العام، والبعض منها يتطلب توافر القصد الخاص كأحد الأركان المعنوية للجريمة. [9]

10- **دراسة: بدري فيصل (2017)**

سعت الدراسة إلى تسليط الضوء على الظواهر الإجرامية التي زاد انتشارها مع الاستعمال المتزايد لشبكة الإنترنت، باستخدام المنهج التحليلي، وتوصلت الدراسة إلى أن بعض الاتفاقيات الدولية لا تزال تتخذ كمرجع لصياغة النصوص المتعلقة بوضع الإطار القانوني لحماية النظام المعلوماتي، كاتفاقية تريبس وبرن، وأيضًا البعد الإجرائي لتلك الجرائم ينطوي على تحديات عديدة، ممثلة في: سرعة الكشف خشية ضياع الدليل، خصوصية قواعد التفتيش،والضبط الملائم لتلك الجرائم. [10]

11 - **دراسة: مريم مسعود (2013)**

سعت الدراسة التعرف على أبرز آليات مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في القانون 04/09، باستخدام منهجي التحليلي والمقارن، وتوصلت الدراسة إلى أن: - القانون تضمن عديد من الآليات المستحدثة لمكافحة تلك الجرائم، ومن أهمها:

- إنشاء هيئة وطنية للوقاية من تلك الجرائم ومكافحتها، وأن مراقبة الاتصالات الرقمية وتفتيش النظم المعلوماتية يعد من أهم الإجراءات، وأيضًا تضمن آليات تنسيق القوانين الجزائية العالمية لإحكام قبضة العدالة على المجرمين في أي دولة.[11]

التعليق على الدراسات السابقة

من واقع العرض السابق للدراسات السابقة، يمكن الخروج بمجموعة من المؤشرات، وتتمثل في:

- تنوع الآليات المستخدمة في مكافحة الجرائم الإلكترونية على اختلاف أنواعها من دولة لأخرى.
- وضع آليات وقائية للجرائم الإلكترونية تعد سمة معيارية أساسية لا يمكن الاستغناء عنها في ظل التنافس الرقمي وتحديات العولمة.
- لا يوجد نظام متفق عليه دوليًا لمكافحة تلك الجرائم.
- التعاون الدولي ضروري لمكافحة تلك الجرائم والحد من خطورتها.
- كما اختلفت الدراسة الحالية مع الدراسات السابقة في عدة نقاط أهمها: المنهج المستخدم،الأساليب المستخدمة في الدراسة، نوعية وعينة الدراسة، مجتمع الدراسة، والاستراتيجية المقترحة.

أوجه الإفادة من الدراسات السابقة:

تم الإفادة من تلك الدراسات في التعرف على الآليات الوقائية المقترحة للحد من الجرائم الإلكترونية؛ وبالتالي الإفادة منها في وضع الاستراتيجية المقترحة.

مشكلة الدراسة:

مع بروز الحوسبة السحابية وتأثر الفضاء السيبراني بشكل واضح بجائحة كوفيد 19، وزيادة معدل التهديدات والهجمات السيبرانية، وفي ظل زيادة توجه الدول لمواكبة التطورالتقني والمعلوماتي وتغلغل وسائل تقنية المعلومات والاتصالات في مناحي الحياة بعالمنا المعاصر وتعزيز النفاذ إليها ، وفى ظل التحول الرقمي للمؤسسات وقطاعات الدول زاد من حجم انتشار البيانات والمعلومات وتبادلها، الأمر الذي ساعد في زيادة حجم الاختراقات حتى أصبح الفضاء السيبراني بيئة خصبة للحروب والجرائم، من قبل المتسللين السيبرانين سواء كانوا أفرادًا أم مجموعات منظمة إلى جانب النشاطات الإرهابية الممولة من قبل بعض الدول، نتيجة للطابع المفتوح لتلك الساحة الافتراضية وعدم وجود رقابة قانونية محكمة عليها، ومن هنا جاءت مشكلة الدراسة، حيث تتمثل في استحداث رؤية استراتيجية نموذجية لمكافحة تلك الجرائم، من زوايا مختلفة يمكن

تطبيقها على كافة المستويات، والتي من شأنها تعزيز الحفاظ على الأمن السيبراني - باستطلاع آراء الخبراء بتطبيق أسلوبي دليفي والتخطيط الاستراتيجي، للوصول إلى فضاء سبراني آمن لحماية المصالح الوطنية والحفاظ على أمن وسلامة المجتمع وقيمه.

أهمية الدراسة

تكتسب الدراسة أهميتها من عدة اعتبارات أساسية، تتمثل في: -

1- الحاجة الملحة لتلك النوعية من الدراسات، لزيادة حجم التهديدات والمخاطر الأمنية في الفضاء السيبراني أكثر من أي وقت مضى.

2- للحد من التأثيرات السلبية لتكنولوجيا الاتصال والإعلام.

3- حاجة المكتبة الإعلامية لهذا النوع من الدراسات والإسهام في إثرائها.

4- قد تكون مجالًا لفتح توجهات جديدة لصانعي القرار لاتخاذ سياسات وقائية فعالة لحماية البنية التحتية الحساسة من الهجمات الرقمية.

5- من كونها إحدى المواضيع المهمة التي تفرض نفسها على الساحة الدولية، وباعتبارها جريمة لا تعرف الحدود والمسافات، فكافة دول العالم تعاني منها، حتى المتقدم منها.

6- لتزايد الهجمات السيبرانية في معظم دول العالم مع استمرار جائحة كوفيد-19.

7- من الدراسات البينية التي تجمع عدة تخصصات متباينة، كالجمع بين مجال الإعلام الرقمي والمجال السياسي، والتقني، والقانوني، والأمني.

أهداف الدراسة:

سعت الدراسة لوضع تصور مقترح لاستراتيجيات وآليات مكافحة الجرائم الإلكترونية للحفاظ على الأمن القومي المصري، وفى إطار هذا الهدف هناك عدة أهداف فرعية تسعى الدراسة لتحقيقها، وتتمثل في: -

- الوقوف على الأساليب المستحدثة للجرائم الإلكترونية.
- رصد أسباب انتشار الجرائم الإلكترونية.
- رصد أبرز التهديدات التي تثيرها الجرائم الإلكترونية.
- تشخيص الوضع الحالي لمنظومة الأمن السيبراني.
- الكشف عن الآليات الأمنية للحد من تلك الجرائم.
- الكشف عن الآليات التقنية للحد من تلك الجرائم.
- رصد الآليات الإعلامية للحد من تلك الجرائم.
- رصد الآليات القانونية للحد من الجرائم الإلكترونية.

- رصد الآليات التربوية للحد من الجرائم الإلكترونية.

تساؤلات الدراسة:

سعت الدراسة إلى الإجابة عن تساؤل رئيس ممثل في كيفية الحد من الجرائم الإلكترونية للحفاظ على الأمن القومي، ولتحقيق أهداف رؤية مصر 2030، ويتفرع من هذا التساؤل عدة تساؤلات فرعية، وتتمثل في: -

1. ما الأساليب المستحدثة للجرائم الإلكترونية؟
2. أي من المشاكل والتهديدات التي تثيرها تلك الجرائم؟
3. كيف يتم الارتقاء بالآليات التقنية للحد من تلك الجرائم؟
4. أي من الآليات الأمنية التي يمكن تطبيقها للحد من تلك الجرائم؟
5- أي من الآليات والاستراتيجيات الإعلامية التي يمكن اتباعها للحد من تلك الجرائم؟
6- أي من الآليات القانونية التي يمكن تفعيلها للحد من تلك الجرائم؟
7- أي من الآليات والاستراتيجيات التربوية والتعليمية التي يمكن اتباعها للحد من تلك الجرائم؟

نوع الدراسة:

تنتمي الدراسة إلى حقل الدراسات الوصفية الاستشرافية لوضع رؤية استراتيجية متعددة الأبعاد لمكافحة الجرائم الإلكترونية للحفاظ على الأمن القومي، من خلال رصد أساليب وأسباب وتهديدات تلك الجرائم ودراسة منظومة الأمن السيبراني، تمهيدًا لاستشراف استراتيجية للحد منها.

مناهج الدراسة:

في ضوء طبيعة الدراسة والأهداف التي سعت لتحقيقها، اعتمدت الدراسة على عدة مناهج متكاملة، وتتمثل في: -

المنهج الوصفي التحليلي: وذلك لوصف وتحليل الظاهرة موضع الدراسة بمختلف أبعادها -الجرائم الإلكترونية- للوصول إلى نتائج تفيد في إعداد الاستراتيجية المقترحة.

المنهج الاستقرائي: الذي يقوم على تبني رؤية مستقبلية للواقع المأمول فيه -وضع رؤية استراتيجية فعالة للحد من تلك الجرائم، تنطلق من تقييم الوضع الحالي للمعالم الأساسية لتلك الظاهرة.

أدوات جمع البيانات:

طبقًا لنوعية الدراسة وأسلوبها وأهدافها، تمثلت أدوات الدراسة في: -

1- الاستبيان باعتباره من أنسب الأدوات للدراسة، وتم تطبيقه عبر ثلاث جولات مختلفة، الجولة الأولى اشتملت على أسئلة مفتوحة استقرائية طبقًا لتخصص عينة الدراسة ، في حين اشتملت الجولة الثانية والثالثة على الأسئلة المغلقة تم بناؤها بناء على الآراء التي حصلت على نسبة توافق عالية في الجولة الأولى ، وتم إعداده بما يتلائم مع منهجية أسلوب دليفي في التطبيق وبما يحقق أهداف الدراسة.

2-فحص الوثائق للأبحاث والدراسات والكتب العلمية العربية والإنجليزية وتقارير المخاطر العالمية لعام 2020 م الصادر عن المنتدى الاقتصادي العالمي، والتي تم الإفادة منها في وضع معالم الاستراتيجية المقترحة.

3-أداة التحليل الاستراتيجي (SWOT analysis): لرصد نقاط القوة والضعف لمنظومة الأمن السيبراني، وللوقوف على الفرص والتهديدات المحيطة بها من قبل البيئة الخارجية.

أساليب الدراسة:

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها تم استخدام: -

1) **أسلوب دليفي** (Delphi Technique) والذى يعد واحدًا من أبرز الأساليب المستخدمة في الدراسات المستقبلية، وذلك بهدف الوصول لرؤية نموذجية لاستراتيجيات وآليات مكافحة جرائم الفضاء السيبراني –الجرائم الإلكترونية- من خلال استطلاع آراء عينة من الخبراء والمتخصصين عبر ثلاث جولات مختلفة لتحليل الظاهرة موضع الدراسة، وتم تطبيق هذا الأسلوب من خلال دراسة العوامل المرتبطة بالظاهرة موضع البحث (الأساليب المستحدثة لتلك الجرائم- أسباب انتشار تلك الجرائم– التهديدات - آليات مكافحة تلك الجرائم من النواحي التقنية- الأمنية– الإعلامية- التعليمية - القانونية)، وتحليل الوضع الراهن لمنظومة الأمن السيبراني، كنقطة رئيسة لصياغة مجموعة من الاستراتيجيات لمكافحة تلك الجرائم.

الخطوات المنهجية لتطبيق أسلوب دليفي:

1- تحديد موضوع الدراسة وأهدافها وتم إعداد استمارة استبيان مفتوحة الأسئلة، بما يحقق أهداف الدراسة والإجابة على تساؤلاتها.

2- تحديد الخبراء والمتخصصين من ذوي الصلة بالأمن السيبراني وتكنولوجيا الاتصال - عينة الدراسة، والتواصل معهم لشرح طريقة تطبيق أسلوب دليفي.

3- تم إرسال الاستبيان الأولي لعينة الدراسة، وطُلِبَ من كل منهم وضع إجاباته الاستقرائية لتلك الأسئلة، وفقًا لتخصصه.

4- تم تحليل النتائج ، وتحديد الاتفاق والاختلاف بين الإجابات ، وقد أسفرت نتائج تلك الجولة عن متوسط اتفاق في الإجابات المقترحة ، لتحقيق الأهداف المرجوة.

5- تم تصميم استبيان مغلق بناءً على الإجابات الأولية للخبراء وللمتخصصين، وفقًا لمقياس ليكرت الخماسي .

6- تم إرسال الاستبيان المغلق مرة أخرى لعينة الدراسة، مع تقرير نتائج استبيان المرحلة الأولى، بدون تحديد لهوية المبحوثين.

7- تم تحليل نتائج الاستبيان المغلق، وتم إعداد استبيان مغلق أخر بناءً على درجة التوافق في الإجابات، واستبعاد المؤشرات التي حصلت على نسبة محايد ومعارض بشدة ومعارض إلى حد ما.

8- تم إرسال الاستبيان المغلق، مع تقرير نتائج تحليل الجولة الثانية، لعينة من المبحوثين الذين وافقوا على الإرسال.

9- تم تحليل نتائج استبيان الجولة الثالثة، وحصلت جميع المؤشرات على نسبة توافق عالية، لذا تم اعتماد تلك الخطوة في التحليل وكتابة نتائج الدراسة.

2) **أسلوب التخطيط الاستراتيجي**: وتم تطبيقه من خلال ثلاث مراحل، وتمثلت في:

المرحلة الأولى : وتتعلق بالإجابة على سؤال أين نقف؟ وهو متعلق بتحليل الوضع الراهن لمنظومة الأمن السيبراني المصري، بالاعتماد على أداة التحليل الاستراتيجي (SWOT).

المرحلة الثانية : ومرتبطة بالإجابة على سؤال : إلى أين نريد أن نصل؟ وتمثلت تلك المرحلة في تحديد ركائز الرؤية الاستراتيجية وأهدافها.

في حين تمثلت **الخطوة الثالثة** : في الإجابة على سؤال كيف نصل؟ وللإجابة على ذلك تم تحديد المؤشرات والآليات التي تساعدنا على الانتقال من الواقع الحالي (أين نقف؟) وصولًا للأهداف المرجوة (إلى أين نريد أن نصل؟) أملًا في الحد من تلك الجرائم، والممثلة في الاستراتيجية المقترحة.

مجتمع الدراسة وعينته

انسجامًا مع أهداف ومتطلبات الدارسة بأن جرائم الفضاء السيبراني ليست مقتصرة فقط على الأكاديميين وحدهم باعتبارها ظاهرة متشعبة ومتعددة الأبعاد، في البداية تم

وضع مقترح ب (60) مفردة، ولكن لصعوبة الوصول والتجاوب من قبل البعض، تم التطبيق الفعلي على عينة عمدية بلغ قوامها (45 مفردة) منوعه ما بين: أساتذة تكنولوجيا الاتصال والإعلام، أساتذة وخبراء الأمن السيبراني، أساتذة القانون، الخبراء السياسيين والاستراتيجيين، نخبة من جهاز الشرطة والقضاة، الإعلاميين، وقد روعي في اختيار العينة تعدد تخصصاتهم، ارتباطهم بموضوع الدراسة، عملهم في مؤسسات مرموقة، سنوات الخبرة التي لا تقل عن خمسة أعوام في مجال التخصص، لتحقيق الهدف الرئيس للدراسة، وإعطاء نظرة أكثر شمولية حول موضوع الدراسة، مرت عملية الوصول النهائي لعينة الدراسة بعدة مراحل، تم التواصل مع 35 شخصًا من الخبراء من ذوي التخصصات السابق الإشارة إليها، وتم توضيح لهم هدف الدراسة وطريقة تطبيق أسلوب دليفي، وطلب من بعضهم ترشيح (25 شخصًا) لهم صلة بالمجال، حتى يكتمل العدد النهائي للعينة، ولديهم الاستعداد للمشاركة في الاستبيان، تم الترشيح للعدد المطلوب، وتم التواصل معهم، ولكن هناك خمسة عشرة شخصًا رفضوا لانشغالهم، في حين أبدى عشرة موافقتهم على المشاركة في الدراسة، وبالتالي يكون إجمالي العينة (45) خبيرًا وأكاديميًا، وبالتالي تم الاعتماد على هذا العدد لصعوبة الوصول للعدد المقترح، ويمكن توضيح تخصصات العينة كما يأتي:-

جدول (1) يوضح لجنة الخبراء والأكاديميين المقترحة

م	التوزيع المهني	العدد	النسبة
النخبة الأكاديمية	أساتذة تكنولوجيا الاتصال والإعلام	9	٪20
	أساتذة القانون	8	٪17.7
	أساتذة الأمن السيبراني	8	٪17.7
الخبراء والنخبة	خبراء ومستشارون في الأمن السيبراني	5	٪11.1
	خبراء سياسيون واستراتيجيون	4	٪8.8
	نخبة من جهاز الشرطة والقضاة	6	٪13.3
	نخبة من الإعلاميين	5	٪11.1
المجموع		45	٪100

أساليب المعالجة الإحصائية

تم استخراج المتوسط الحسابي والوزن النسبي والانحراف المعياري لكل فقرة من فقرات الاستبيان وفقًا لاستجابات عينة الدراسة، تم الاعتماد على النسخة الأخيرة –المرحلة الثالثة– من تطبيق الاستبيان، وذلك للإجابة على تساؤلات الدراسة وتحقيقًا لأهدافها.

مدخل لجرائم الفضاء السيبراني:

زادت الجرائم الإلكترونية بشكل كبير، نتيجة لتطور تكنولوجيا الاتصال وبروز العولمة الرقمية، فعلى الرغم من حقيقة أن الإنترنت يساعد في إجراء الأنشطة الاقتصادية والاجتماعية المختلفة، إلا أن هناك مجموعة من المخاطر التي يتم ارتكابها عبر تلك الشبكة من سرقة البيانات والوصول غير القانوني إلى المعلومات الشخصية، وغيرها من التهديدات[12]، فالجرائم السيبرانية كمجال معرفي مجال متعدد التخصصات يجمع بين عدة علوم، ومنها: علم الجريمة، وعلم النفس وعلم الاجتماع، وعلوم الكمبيوتر، والأمن السيبراني، لتقديم فهم متعمق لطبيعة الجريمة السيبرانية، من حيث استكشاف أسبابها وتهديداتها، بالإضافة إلى المسائل القانونية والأخلاقيات واستراتيجيات الوقاية والمكافحة، حيث تترابط الجريمة السيبرانية والأمن السيبراني عبر العديد من الأماكن والمنصات والجهات الفاعلة، وتتغير قضايا تلك الجرائم بشكل مستمر وسريع، خاصة مع تطور المهارات والتقنيات[13].

وتعد تلك الجرائم والأمن السيبراني من مجالات البحث الناشئة التي تشكلت من خلال التطورات التكنولوجية، لقد درس العلماء أنواعًا مختلفة من تلك الجرائم، حيث ركز بعضهم على الطرق التي يمكن من خلالها الحد منها وتقليلها وحتى منعها، ومع ذلك، كان من الصعب تحقيق تلك الاستراتيجيات في الواقع بسبب العوامل البشرية والتقنية المحيطة بتلك الجرائم [14]، فقد أصبح التوسع والتنويع المتزايد في استراتيجيات وممارسات الجريمة الإلكترونية عقبة صعبة من أجل فهم مدى المخاطر الكامنة وتحديد سياسات وقائية فعالة للشركات والمؤسسات والوكالات[15]، حيث تعددت أشكال تلك الجرائم في عصرنا الحديث، نظرًا لتعدد الوسائل والأساليب الرقمية التي يلجأ إليها المجرم المعلوماتي في ظل انفتاح الفضاء الافتراضي، حيث اختلف الباحثون فيما بينهم في تحديد معنى الجريمة الإلكترونية، وكل منهم اعتمد على زاوية معينة في تعريفها، منهم من تبني التعريف من الناحية التقنية المرتبطة بالوسيلة الاتصالية المستخدمة، ومنهم من تبناه من ناحيته التشريعية، ويمكن تعريفها على أنها: أي مخالفة ترتكب ضد الأفراد والمؤسسات والدول لدوافع إجرامية سواءً كان ذلك بطريقة مباشرة أم غير مباشرة،

باستخدام عديد من وسائل الاتصال الحديثة مثل غرف الدردشة أو البريد الإلكتروني أو الموبايل وغيرها. [16]

حيث تؤثر تلك الجرائم بشكل كبير على خصوصية الأفراد لأنها تنطوي على وصول غير قانوني واستخدام ضار للبيانات من قبل المهاجمين، فتلك الجرائم مرتبطة باختراق كلمات المرور أو المواقع الإلكترونية أو شبكات الدول أو المنظمات، وارتكاب مختلف الجرائم الجنائية باستخدام تقنية المعلومات ، وقد ترجع معظم هجمات الأمن السيبراني إلى أخطاء بشرية مختلفة يرتكبها موظفو تكنولوجيا المعلومات الأقل كفاءة أو الأقل تأهيلًا [17]، مما يوفر مجالًا للمتسللين للتلاعب بأنظمة الشبكة، حيث يركز المهاجمون بشكل أكبر على استغلال نقاط الضعف البشري[18]، وهذا يفسر الانتشار الكبير لتلك الجرائم في المنظمات ذات الموظفين الأقل تأهيلًا، لذا من الضروري فهم الوظائف البشرية في تعزيز الأمن السيبراني [19]، حيث تخسر الحكومات كثير من الإيرادات للتصدي لتلك الهجمات، والتي تؤثر بشكل كبير على الخدمات الأساسية والنمو الاقتصادي للدول، وهذا ما يجعل ملف الأمن السيبراني أولوية حكومية أساسية يجب أن توليها الحكومة المسؤولة اهتمامًا كبيرًا. [20]

كما تعددت دوافع ارتكاب تلك الجرائم، ما بين الدوافع السياسية والاقتصادية، فأصبح اختراق الأنظمة للحصول على معلومات سياسية وعسكرية واقتصادية مسألة مهمة، إلى جانب الدوافع الاقتصادية، فالشركات التجارية تعيش أيضًا حربًا فيما بينها من خلال محاولات الاختراق المستمر لحساباتها[21]، فضلًا عن الدوافع الفكرية حيث تؤثر تلك الجرائم على الدولة وعلى اقتصادها إذا لم يتم تدارك تلك النوعية من الجرائم، حيث تمثل تهديدًا خطيرًا على الأمن القومي لانتشارها المتزايد، ولصعوبة التصدي لها بالأساليب والتكنيكات التقليدية ، الأمر الذي يتطلب إقرار سياسات دولية مشتركة، لمواجهة تهديد الهجمات السيبرانية المحتملة، حيث يفكر صانعو القرار بشكل متزايد بشأن استخدام استراتيجيات الردع لتكملة الدفاع السيبراني، لكن من الصعب إلى حد ما التعامل مع التهديد من خلال سياسات واستراتيجيات الدفاع الوطني فقط، وذلك لأن الفضاء السيبراني فضاء مفتوح صعب السيطرة عليه من جانب وطني أو إقليمي، لذا لا بد من التعاون على الصعيد العالمي من أجل مكافحة الإرهاب السيبراني وغيرها من الجرائم [22]، وهذا التعاون لا يكون فقط على المستوى التشريعي ، ولكن أيضًا على المستوى العسكري بما في ذلك استراتيجيات الردع ، فالأمر يتطلب إنشاء فرق خبراء الدفاع السيبراني دوليًا لديها القدرة على الاستجابة للحوادث والهجمات السيبرانية التي

تواجه دولة ما، لتعزيز سياسات الدفاع السيبراني المشترك، ووضع برنامج تدريبي دولي لمواجهة تلك الهجمات ، وإنشاء تجمع استخباراتي دولي، لجمع المعلومات الاستخبارية بحيث لا تشمل فقط مراقبة المواقع الإرهابية، ولكن أيضًا جمع المعلومات الإلكترونية كدليل على الهجمات المحتملة، فالإرهاب السيبراني مصدر قلق متزايد للعالم كله، فالنظام الحالي للقوانين والمعايير والتعريفات الدولية غير كافٍ لمعالجته؛ إنه في الواقع يزيد من مخاطر التهديد من خلال إنشاء منطقة رمادية أو فجوة يمكن أن يستغلها الإرهابيون السيبرانيون [23]، لذا يجب أن تكون مكافحة تلك الجرائم والتهديدات هدفًا مشتركًا لجميع البلدان في جميع أنحاء العالم، ولا تستخدم كورقة مساومة للعلاقات الدولية، فيجب على البلدان التعاون فيما بينهم لمكافحة تلك الجرائم على أساس التفاهم والاحترام لقانون وثقافة البلدان الأخرى، بهذه الطريقة، يمكننا تحقيق تعاون حقيقي بدلًا من شكلي [24]، فالجرائم الإلكترونية تتطلب نظامًا منهجيًا وشاملًا وتشريع مستقر وتعزيز التنسيق الدولي [25]، وهذا يتطلب التركيز على التقنيات التي تساعد في الوقاية من تلك الجرائم، وتحديد الأهداف، وبالتالي وضع خطط العمل والتدابير ومسؤوليات المؤسسات للمساعدة في تحقيق الأهداف المحددة، للحفاظ على الأمن السيبراني. [26]

التعريفات الإجرائية

تعد تلك الخطوة مهمة في البحث العلمي؛ للتعرف على ما يتم تبنيه من مصطلحات داخل نطاق الدراسة ، والمتمثلة في: -

الرؤية الاستراتيجية: تصور مقترح مبنى على أسس علمية، لتحقيق الهدف المنشود، وتعزيز رؤية مصر 2030 في الحد من مخاطر وتهديدات جرائم الفضاء السيبراني في ظل التحول الرقمي العالمي.

الجرائم الإلكترونية: جرائم الفضاء السيبراني العابرة للحدود وللمسافات، يتم ارتكابها بوسائل تكنولوجيا الاتصال المختلفة، لها صور متعددة ومتنوعة، لها تأثيرها على الأمن القومي للبلاد بمختلف محاوره.

أسلوب دليفي : أسلوب للتعرف على آراء الخبراء والمتخصصين بحيث تكون بمثابة بدائل مختلفة لآليات واستراتيجيات مقترحة لمواجهة مخاطر جرائم الفضاء السيبراني من خلال توجيه استبيان لهم عبر ثلاث جولات.

نتائج الدراسة:

تم تطبيق أسلوب دليفي عبر ثلاث جولات مختلفة، ويمكن عرض نتائجها كما يأتي: -

أولًا: نتائج جولة دليفي الأولى:

تمثلت الجولة الأولى من دليفي بعرض الأسئلة على عينة بلغ قوامها 30 مفردة بما يمثل 66.6٪ من إجمالي العينة المقترحة، وتم توضيح كافة النقاط المتعلقة بالبحث وتوضيح الطريقة المتبعة في الدراسة، وتم إرسال الأسئلة الخاصة بالاستبيان المفتوح، من خلال أربعة أبعاد رئيسة ، وتتمثل في: (أساليب الجرائم المستحدثة– أسباب انتشار تلك الجرائم على نطاق واسع– تهديدات ومخاطر تلك الجرائم– آليات مكافحة تلك الجرائم (التقنية– الإعلامية– الأمنية– التعليمية) كلٌ حسب تخصصه، واستغرقت الجولة الأولى حوالي أسبوعين بدأت من تاريخ 2020/11/1 حتى تاريخ 2020/11/15، وتم استرجاع الاستبيان بمتوسط 100٪. وبعد تجميع استجابات استبيان الجولة الأولى، تم تحليل النتائج، وقد أسفرت نتائج تلك الجولة عن متوسط اتفاق في بعض الإجابات المقترحة، لتحقيق الأهداف المرجوة بناء على درجة التوافق، حيث تم تحليل إجابات عينة الدراسة حول الاستبانة المفتوحة الاستقرائية، وتم إرسال التقرير الذي يتضمن نتائج استجابات الجولة الأولى، بناءً على تلك الجولة تم بناء استبيان مغلق، تم تطبيقه في الجولة الثانية.

ثانيًا: نتائج جولة دليفي الثانية:

تمثلت الجولة الثانية من دليفي بعرض الأسئلة المغلقة على (42) مفردة، بهدف الوصول إلى نتائج أعمق وأشمل من واقع خبرتهم العلمية والعملية، وتم التواصل معهم، لإبلاغهم عن بدء الجولة الثانية من خلال إرسال استبانة مغلقة اشتملت على عدة أسئلة ذات مقياس ليكرت الخماسي (موافق بشدة – موافق إلى حد ما – محايد – معارض بشدة– معارض إلى حد ما)، واستغرقت تلك الجولة حوالي عشرة أيام، من 2020/11/20 إلى 1 /2020/12، وتم استرجاع (40) استبانة بمتوسط 95.2٪، تم تحليل نتائج الاستبانة المغلقة، ثم استخلاص نتائجها الإحصائية، وإرفاقها مع نسخة معدلة منها – بعد تجميع الاستجابات التي حصلت على نسبة موافقة عالية واستبعاد الإجابات التي حصلت على درجة محايد ومعارض- إلى الخبراء مرة أخرى، لاستقصاء التغير في آرائهم بناءً على التحليل الأخير، للخروج بمجموعة من الآليات والاستراتيجيات.

ثالثًا: نتائج جولة دليفي الثالثة:

بناءً على نتائج الجولة الثانية تم استبعاد مؤشرين للأساليب المستحدثة للجرائم المعلوماتية؛ لأنها حصلت على درجة توافق أقل من 80٪ لأنها كانت تقع في فئتي معارض ومحايد، وأيضًا تم استبعاد ثلاث مؤشرات من أسباب انتشار تلك الجرائم، وبالنسبة للتهديدات تم استبعاد مؤشر واحد من التهديدات الاجتماعية، وأيضًا للتهديدات الاقتصادية والسياسية ليبلغ إجمالي المؤشرات المستبعدة ثلاث مؤشرات، وبالنسبة للآليات التقنية والأمنية اللازمة لمكافحة تلك الجرائم تم استبعاد ثلاث منها، وخمسة من الآليات الإعلامية، وأربعة من الآليات القانونية ، وخمسة من الآليات التعليمية، بناءً على تلك العناصرالمستبعدة تم تصميم استبيان مغلق للمؤشرات التي حصلت على نسبة توافق أعلى، وتم التواصل مع عينة الدراسة من الجولة الثالثة لملء الاستمارة، لإبلاغهم عن بدء الجولة الثالثة، وتم التطبيق على (30) مبحوثًا منهم عينة من الجولة الأولى والثانية ممن وافقوا على الإجابة، إلى جانب ثلاث أشخاص للمرة الأولى، وقد طلب منهم تأمل النتائج الإحصائية التي أسفرت عنها نتائج تحليل أسئلة الجولة الثانية وإبداء آرائهم حولها طبقًا لمقياس ليكرت الخماسي، واستغرقت الجولة الثالثة الفترة الزمنية ثلاث أسابيع، وتم استرجاع 30 استبانة بمتوسط 100٪، وتم الحصول على توافق نسبي بالرأي - في بعض المؤشرات - بين الخبراء والمختصين للخروج بقائمة من المؤشرات الخاصة بمحاور الاستمارة، والتي سعت الدراسة لتحقيقها، والوصول إلى درجة الثبات، لتحديد الوزن النسبي لقيمة كل مؤشر، ويمكن عرض النتائج النهائية للجولة الأخيرة كما يأتي في تلك الجداول:-

جدول (2) يوضح المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لاستجابات أفراد عينة البحث وفقًا لفقرات الأساليب المستحدثة للجرائم الإلكترونية.

م	المؤشرات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الأهمية
1	اختراق الشبكات وجمع البيانات الحساسة وتشفيرها من خلال تقنيات الهندسة الاجتماعية	4.5333	0.86037	٪90.666	2
2.	استخدام برامج للتجسس من خلال الأساليب الخفية التي تهدف إلى الدخول غير المشروع على الأنظمة والشبكات التقنية والأمنية	4.0667	1.38796	٪81.334	3
3.	نشر الفيروسات والبرامج الخبيثة لحجب الخدمات الضرورية عن المواطنين.	3.9333	1.28475	٪78.666	6
4.	استخدام برامج ورسائل التصيد والتجسس لسرقة البيانات وابتزاز الآخرين.	3.9667	1.44993	٪79.334	5
5.	قرصنة التطبيقات السحابية	4.6	0.62146	٪92	1
6.	رسائل البريد الإلكتروني المخادعة لضرر الآخرين ونشر المعلومات المفبركة.	4.3667	0.96431	٪87.334	4
7.	استخدام أدوات متطورة لتشفير البيانات الحساسة وخرق الأنظمة الأمنية.	3.3667	1.3257	٪67.334	7
	المتوسط العام	4.11904			

يتضح من بيانات الجدول السابق تعدد أساليب وتكنيكيات ارتكاب الجرائم الإلكترونية، حيث جاء أعلى متوسط حسابي لعبارة "قرصنة التطبيقات السحابية"، وبوزن نسبي 92٪ وهي تقع في فئة الموافقة العالية، كما تراوحت المتوسطات الحسابية لفقرات هذا المحور ما بين (4.6- 3.3)، وقد بلغ المتوسط الحسابي الإجمالي لهذا المحور 4.1، ويعزو ذلك لأن المجرم السيبراني يتسم بالابتكار في إيجاد طرق جديدة لتضليل مستخدمي المنصات الرقمية وتعطيل الخدمات الحيوية، فتلك الأساليب تسهم في تعطيل البنية التحتية للمعلومات وتدمير البيانات والأنظمة، وخلق ثغرات أمنية محتملة في التطبيقات الأقل أمنًا التي تم إنشاؤها لتسهيل إنجاز المهام عن بُعْد في ظل تفشي جائحة كوفيد 19،

فكلما تقدمت وسائل تكنولوجيا المعلومات والاتصالات تقدمت معها أساليب المخترقين وتكتيكاتها، فنتيجة لعدم انتشار الثقافة الرقمية المجتمعية للاستخدام الأمن والأمثل لتلك الأدوات والوسائل، الأمر الذي أدى لسرعة تطور أساليب وتقنيات ارتكاب تلك الجرائم، فالاحتيال الرقمي والاختراقات الأمنية من أبرز الأدوات والأساليب المستخدمة في ارتكاب الجرائم الاقتصادية والأمنية والاجتماعية والعسكرية والفكرية والتقنية على الصعيد الدولي.

جدول (3) يوضح المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لاستجابات أفراد عينة البحث وفقًا لفقرات أسباب انتشار الجرائم الإلكترونية

م	المؤشرات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الأهمية
.1	غياب الوعي المجتمعي بطرق ارتكاب تلك الجرائم ومكافحتها	4.4333	0.72793	٪88.666	5
.2	عولمة السياق الدولي للفضاء السيبراني	4.2333	0.85836	٪84.666	7
.3	قلة الوعي الثقافي بخطورة تلك الجرائم وقوانينها لدى عديد من مرتكبيها	4.6	0.67466	٪92	2
.4	غياب الدور الإعلامي التوعوي للحد من مخاطر تلك الجرائم	4.6667	0.60648	٪93.334	1
.5	غياب سياسة التعاون الدولي فيما يضمن ملاحقة فاعلة لمرتكبي تلك الجرائم.	4.3333	0.71116	٪86.666	6
.6	زيادة مستخدمي وسائل تكنولوجيا الاتصال وتضخم البيانات المتداولة.	4.5667	0.62606	٪91.334	3
.7	غياب التطبيق الفعلي للتشريعات والقوانين الرادعة لمرتكبي تلك الجرائم على الصعيد المحلي والدولي.	4.4667	0.68145	٪89.334	4
	المتوسط العام	4.47143			

يتضح من مؤشرات الجدول السابق ارتفاع درجة موافقة المبحوثين على تعدد أسباب انتشار الجرائم الإلكترونية، والتي تراوحت ما بين الأسباب الإعلامية والاجتماعية والثقافية وعولمة السياق الدولي وغياب التطبيق الفعلي للتشريعات المتعلقة بتلك الجرائم

لضعف التشريعات القانونية المتعلقة بها، وقد تراوحت المتوسطات الحسابية لعبارات المحور ما بين (4.6 -4.2)، وقد بلغ المتوسط الحسابي الإجمالي لهذا المحور 4.4، وجاء أعلى متوسط لعبارة غياب الدور الإعلامي التوعوي للحد من مخاطر تلك الجرائم بمتوسط 4.6، وبوزن نسبي 93.3٪ في حين حصلت عبارة عولمة السياق الدولي للفضاء السيبراني على أقل متوسط حسابي بنسبة 4.23، وهى تقع في فئة الموافقة العالية، وهذا مؤشر على تعدد الأسباب التي أدت لانتشار تلك الجرائم، الأمر الذي يتطلب ضرورة الوقوف على تلك الأسباب ودراستها لوضع استراتيجية علاجية ووقائية فعالة للحد من انتشار تلك النوعية من الجرائم، في ظل التحول الرقمي ، وتطور التقنية ووسائل تخزين المعلومات بشكل متسارع من خلال توعية المجتمع من خلال حملات إعلامية ممنهجة بخطورة تلك الجرائم بكافة وسائل الإعلام المختلفة، لأن الأمن القومي للدول مرتبط بقدرتها على حماية بياناتها وأسرارها والتصدي للهجمات المحتملة على البنية التحتية والشائعات والأخبار المزيفة.

جدول (4) يوضح المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لاستجابات أفراد عينة البحث وفقًا لفقرات أنواع تهديدات الجرائم الإلكترونية

م	المؤشرات	المتوسط الحسابى	الانحراف المعياري	الوزن النسبى	درجة الأهمية
من الناحية الاجتماعية	تؤثر سلبًا على أخلاقيات المجتمع وقيمه، وعلى ارتفاع نسب الممارسات الإجرامية.	4.6333	0.66868	٪92.666	2
	خلل عام يهدد الأمن الاجتماعى.	4.5	0.73108	٪90	4
	زيادة التطرف الفكري.	4.65	0.62972	٪93	1
	زيادة الإدمان الرقمى.	4.5	0.695	٪90	4
من الناحية السياسية	ممارسة أساليب الضغط السياسي والترويج للأفكار والمعلومات المضللة، والتي تضر بالأمن السياسى.	4.58	0.77682	٪91.6	3
	نشر الشائعات والأكاذيب الملتوية والمناهضة للدول بهدف إضعافها.	3.3333	1.29544	٪66.666	9
	تسريب المعلومات الحساسة والتخابر مع الجهات المعادية.	4.3333	0.99424	٪86.666	7

التهديدات الاقتصادية	التكلفة المالية للهجمات الإلكترونية عالية.	3.3333	1.29544	٪66.666	9
	ضرب القدرة على التنافس والابتكار الاقتصادي	4.2333	0.72793	٪84.666	8
	تدمير البنية الحيوية التحية للاقتصاد الوطني.	4.3333	0.71116	٪86.666	7
التهديدات الأمنية والتقنية	تدمير النظم المعلوماتية، والشبكات والبنية التحتية الحيوية.	4.5	0.57235	٪90	4
	الابتزاز وإرباك مؤسسات المجتمع.	4.4333	0.8172	٪88.666	5
	شل الأهداف الحيوية للدولة.	4.36	0.6862	٪87.2	6
المتوسط العام		4.28639			

توضح النتائج تعدد أنواع التهديدات التي تثيرها جرائم الفضاء السيبراني على جميع الأصعدة الاجتماعية، السياسية، الأمنية، الاقتصادية، والتقنية سواء على مستوى الدولة أم على مستوى المؤسسات، أم على مستوى الأفراد، وقد تراوحت المتوسطات الحسابية لعبارات هذا المحور ما بين (4.6- 3.3)، وقد بلغ المتوسط الحسابي الإجمالي لهذا المحور 4.2، فجاءت التهديدات الاجتماعية في الدرجة الأولى، يليها التهديدات السياسية، ثم الأمنية، ثم التهديدات الاقتصادية ، ويعتمد مستوى تلك التهديدات على سياق الضحية، ونوعية الهجوم، والأنظمة المعلوماتية، حيث يجد الإرهابيون المنصات الرقمية بيئة ثرية لنشر أفكارهم، فمن الناحية السياسية والأمنية تسعى لنشر الشائعات المحرضة للشعب والمناهضة للدولة، والترويج للأفكار المضللة التي تتناسب مع مصالحهم بهدف إضعافها وزعزعة استقرارها، والتي تضر بالأمن السياسي والأمني للدول، ومن الناحية الاجتماعية تؤدي إلى زيادة التطرف الفكري، وحدوث خلل عام يهدد أمن المجتمع وتفككه الأسري، وبالتالي الإضرار بالأمن الاجتماعي، وغيرها من التهديدات الاقتصادية الناجمة عن التكلفة المالية للهجمات الإلكترونية، وبالتالي التأثير على الأمن القومي للدولة، فالتهديدات السيبرانية في تزايد وتطور مستمر مع انفتاح وعولمة الفضاء الافتراضي، فنوعية تلك الجرائم من شأنها أن تهدم المجتمعات إن لم يكن المجتمع لديه وعي كاف بتلك الجرائم وأساليبها وتكتيكاتها وما تهدف إليه.

جدول (5) يوضح المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لاستجابات أفراد عينة البحث وفقًا لفقرات السياسات الأمنية للحد من الجرائم الإلكترونية

م	المؤشرات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الأهمية
.1	تأمين الشبكات الداخلية والخارجية ذات العلاقة بالقطاعات الحيوية بأحدث البرامج والتطبيقات.	4.6	0.56324	٪92	1
.2	مراقبة وتحديث البنى التحتية الحيوية والمعلومات الوطنية بشكل دورى.	4.3333	0.60648	٪86.666	4
.3	إعادة هيكلة منظومة الجهاز الأمني المعلوماتي وتطويره بما يتناسب مع مستجدات العصر.	4.2	0.88668	٪84	5
.4	تشكيل لجنة أمنية لمراقبة المنصات الرقمية وتحليل المنشورات التي يتم تداولها عبر تلك المنصات دون الإخلال بخصوصية مستخدميها وحرياتهم.	4.4667	0.7303	٪89.334	3
.5	وضع خطط أمنية شاملة ضمن منظومة تعاون دولى، لحماية موضوع الرقمنة من التهديدات والاختراقات.	4.5333	0.57135	٪90.666	2
.6	تشكيل فرق طارئة أمنية وعاجلة للحماية والكشف عن العمليات الاحتيالية السيبرانية والأمنية.	4	0.94686	٪80	6
	المتوسط العام	4.3556			

يتضح من مؤشرات الجدول أهمية الآليات والسياسات الأمنية المقترحة للحد من الجرائم الإلكترونية، حيث حازت على درجة الموافقة العالية من قبل المبحوثين، وتراوحت المتوسطات الحسابية ما بين (4.6- 4)، وقد بلغ المتوسط الحسابي الإجمالي لهذا المحور 4.3، فجاء أعلى متوسط حسابي لعبارة تأمين الشبكات الداخلية والخارجية ذات العلاقة بالقطاعات الحيوية بأحدث البرامج والتطبيقات، وبوزن نسبي 92٪، وهذا مؤشر على ضرورة مواجهة الاختراقات الأمنية على جميع المستويات، فالسياسات الأمنية تعد واحدة من أهم أساسيات هرم الأمن السيبراني، لسلامة المحتوى الرقمي وتأمين البنية التحتية الحيوية، فمن الضروري توافر الحماية الأمنية الفعالة لأنظمة المعلومات

والخصوصية وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية المستخدمين من مخاطر الفضاء السيبراني، خاصة في ظل تضخم البيانات المتداولة، لأنه إذا لم تكن الأنظمة التقنية محمية وأمنة بشكل فعال، فالضرر سيكون كبير على مستويات عدة ، وخصوصًا في ظل انتشار الأزمات العالمية، كما حدث مع جائحة كوفيد19.

جدول (6) يوضح المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لاستجابات أفراد عينة البحث وفقًا لفقرات السياسات التقنية للحد من انتشار الجرائم والتهديدات الإلكترونية

م	المؤشرات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الأهمية
.1	استخدام أنظمة الأمن السيبراني المعتمدة على تقنيات الذكاء الاصطناعي لتحليل البيانات وتحديد الأنماط ذات الصلة بالهجمات المحتملة بسرعة أكبر.	4.1	1.29588	٪82	2
.2	تطوير وتحديث البرامج والتطبيقات المعلوماتية والتقنية باستمرار، بشكل يتيح التعرف على الفنيات الدقيقة التي تساعد على كشف الجريمة ومرتكبيها.	3.9333	1.43679	٪78.666	4
.3	توظيف آليات التعامل الأولى، لاكتشاف مقاطع الفيديو التي يتم تزيفها وفبركتها (deep fake) بشكل أوتوماتيكى.	3.2667	1.38796	٪65.334	5
.4	استخدام تقنيات وآليات الحماية الحديثة والمتقدمة في كافة القطاعات الحيوية المستهدفة .	4.0667	1.20153	٪81.334	3
.5	التتبع الدقيق لأصول التطبيقات السحابية.	4.2	1.21485	٪84	1
	المتوسط العام	3.91334			

من الرصد السابق لبيانات الجدول تراوحت المتوسطات الحسابية لعبارات هذا المحور ما بين (4.2- 3.2)، وقد بلغ المتوسط الحسابي لتلك الآليات (3.9)، وجاء أعلى متوسط لصالح عبارة التتبع الدقيق لأصول التطبيقات السحابية، بوزن نسبي 84٪، من أهم

الآليات التقنية للحد من انتشار الجرائم والتهديدات الإلكترونية، ويعزو ذلك إلى أهمية تلك السياسات التقنية للتطوير المستمر لأنظمة الاتصالات والبنى التحتية المرتبطة بها وأدوات وبرامج الاختراق ، لتحقيق عملية التكيف الدائم مع التطورات التقنية المستمرة باستمرار وإدارة الأمن السيبراني بكفاءة، لأن التطور التقني وانتشار استخدام التطبيقات والخدمات الإلكترونية يقابله تطور في الاستهداف والاختراقات الأمنية، لذا من الضروري إلقاء الضوء على الثغرات الأمنية المحتملة للشبكات والأدوات وتقنيات الهندسة الاجتماعية، للحد من المخاطر السيبرانية مع استمرار تطور تلك المخاطر والتهديدات خلال فترة انتشار جائحة كوفيد 19.

جدول (7) يوضح المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لاستجابات أفراد عينة البحث وفقًا لفقرات الآليات والاستراتيجيات الإعلامية للحد من انتشار الجرائم الإلكترونية

م	المؤشرات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الأهمية
.1	توعية المواطنين بالاستخدام الأمثل للمنصات الرقمية وفي الكشف عن الأساليب والحيل التي يستخدمها المجرم السيبرانى.	4.8	0.48423	٪96	1
.2	تثقيف الجمهور بشأن الجرائم والتهديدات السيبرانية وتعريفه بالقوانين والعقوبات الرادعة لمرتكبيها من خلال البرامج التليفزيونية.	4.7667	0.56832	٪95.334	2
.3	إنشاء مواقع إلكترونية لتبادل المعلومات من نشرات إخبارية وتقارير وإعداد المطبوعات التي تتضمن الأفكار والمعلومات المفيدة عن الأمن السيبرانى.	4.5333	0.7303	٪90.666	6
.4	توظيف المنصات الرقمية في اتجاه الجانب الوقائي المتمثل في بث روح الولاء والانتماء الوطني، وتوعية الناس بمخاطر تلك الجرائم السيبرانية،	4.6667	0.60648	٪93.334	3

	والتي تمثل تهديداً للمجتمعات من أعمال العنف والإرهاب الرقمي.				
.5	التدريب الإعلامى المجتمعى للإبلاغ عن المواقع التى تجسد الأخبار الزائفة ، وكشف بؤر ومخطط المنظمات الإرهابية.	4.5667	0.89763	٪91.334	5
.6	القيام بالحملات الإعلامية التوعوية للحد من الشائعات والمعلومات المفبركة التى تهدد حياة الأشخاص والدولة، موظفة مختلف الوسائل الإعلامية.	4.6	0.62146	٪92	4
	المتوسط العام	4.65555			

يتضح من مؤشرات الجدول السابق، ارتفاع درجة موافقة المبحوثين على العبارات السابقة، وقد تراوحت المتوسطات الحسابية ما بين (4.5-4.8)، وقد بلغ المتوسط الحسابي الكلي لهذا المجال 4.6، وهو يمثل الدرجة العالية، ويمكن تفسير تلك النتيجة بأن الإعلام بمختلف أشكاله له دور وقائى ومهم في الحد من انتشار تلك الجرائم وفي التوعية بالقضايا الأمنية وفى زيادة مستوى الوعي واليقظة وتنمية الحس الاجتماعى الوطنى في التصدى للجرائم والهجمات السيبرانية ، وبالتالي تنمية مهارات البحث ومعرفة القوانين والجرائم السيبرانية، حيث تصدرت عبارة توعية المواطنين بالاستخدام الأمثل للمنصات الرقمية وفي الكشف عن الأساليب والحيل التي يستخدمها المجرم السيبراني أهم الآليات والسياسات الإعلامية المقترحة للحد من انتشار تلك الجرائم، حيث حازت على أعلى وزن نسبي بنسبة 96٪، والتي تبرز الدور الإعلامي التوعوي.

جدول (8) يوضح المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لاستجابات أفراد عينة البحث وفقًا لفقرات الآليات القانونية للحد من انتشار الجرائم الإلكترونية

م	المؤشرات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الأهمية
.1	إعادة النظر في معظم التشريعات بإصدار السلطة المختصة بعض المراسم التنظيمية لمقاهي الإنترنت.	4.7	0.53498	٪94	1
.2	تعزيز سياسية التعاون الدولي في مجال مواجهة القرصنة والإجرام الإلكتروني، من خلال رسم سياسات وقوانين تهدف إلى تشديد العقوبات على مرتكبي هذا النوع من الجرائم.	4.5	0.77682	٪90	4
.3	تطوير طرق ووسائل لتتبع مرتكبي الجرائم الإلكترونية بشكل دقيق والإمساك بهم.	4.5333	0.68145	٪90.666	3
.4	توحيد الجهود بين الجهات المختلفة، التشريعية، والقضائية، والفنية، والعسكرية.	4.6	0.62146	٪92	2
.5	التعاون القضائي وسن قوانين مشتركة للتعامل مع اكتشاف ورقابة المحتوى الإلكتروني وما ينتج عنه من جرائم.	4.4667	0.89955	٪89.334	5
.6	تفعيل تطبيق المعاهدات الدولية الخاصة بمكافحة جرائم الإنترنت على نطاق واسع.	4	1.33907	٪80	6
	المتوسط العام	4.466667			

تشير بيانات الجدول السابق حصول جميع فقرات هذا المحور على درجة الموافقة العالية، وهذا مؤشر على أن القواعد العلمية وإصدار التشريعات واللوائح التنفيذية وتحديد متطلباتها وإعادة النظر في التشريعات الحالية، أمر ضروري وركيزة أساسية لحماية المنظومة الأمنية الرقمية، باعتبار أن التشريعات والقوانين تمثل إحدى أضلاع هرم الأمن

السيبرانى أملًا في الحد من انتشار تلك الجرائم، لذا من الضرورى إقرار اللائحة التنفيذية لتلك الجرائم وتطبيق القوانين والمعاهدات الدولية بصرامة وحزم، فقد تراوحت المتوسطات الحسابية ما بين(4.7-4)، وقد بلغ المتوسط الحسابي الكلي (4.6) وهو يمثل درجة الموافقة بشدة، واحتلت عبارة إعادة النظر في معظم التشريعات بإصدار السلطة المختصة بعض المراسم التنظيمية لمقاهي الإنترنت أعلى متوسط حسابي، ووزن نسبي بنسبة 94٪.

جدول (9) يوضح المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لاستجابات أفراد عينة البحث وفقًا لفقرات السياسات التربوية للحد من انتشار الجرائم الإلكترونية

م	المؤشرات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الأهمية
1.	تطوير البرامج الأكاديمية والمناهج الدراسية المتعلقة بالأمن السيبراني، لتعزيز ثقافة الاستخدام الآمن والأمثل لإدارة البيانات بشكل فعال وإدارة مخاطره.	4.4667	0.68145	٪89.334	5
2.	إنشاء مراكز بحثية لإجراء البحوث والدراسات العلمية الرصينة فيما يخص تلك الجرائم وكيفية حماية البنى التحتية والأشخاص من المخاطر والتهديدات السيبرانية.	4.5667	0.67891	٪91.334	3
3.	تعزيز ثقافة التعاون الأكاديمي الدولي والتبادل المشترك للمعلومات والخبرات في هذا المجال.	4.6667	0.60648	٪93.334	1
4.	وضع تنظيم قانوني وأكاديمي فعال يضع الإطار الصحيح لاستخدام تلك التقنيات الحديثة ويواجه حالات الخروج عليها.	4.5	0.62972	٪90	4
5.	وضع الآليات التربوية للتعامل مع الجرائم المعلوماتية بحرفية وبتوعية تتناسب خطورتها.	4.6	0.67466	٪92	2

6.	عقد المؤتمرات والندوات العلمية باستمرار للتوعية الفكرية وإكساب المعارف والمهارات اللازمة لحماية البيانات.	4.6667	0.54667	٪93.334	1
7.	الاستمرار في إجراء البحوث والدراسات العلمية والعمل المستمر على الارتقاء بالآليات الأمنية والتقنية المستحدثة في هذا المجال.	4.6	0.56324	٪92	2
8.	وضع مناهج دراسية للثقافة المعلوماتية والمواطنة الرقمية في كل المراحل الدراسية.	4.1	1.21343	٪82	6
	المتوسط العام	4.52084			

يتضح من مؤشرات الجدول السابق الأهمية النسبية لفقرات السياسات التعليمية والأكاديمية للحد من انتشار الجرائم الإلكترونية، حيث حازت على درجة موافقة عالية، وقد تراوحت المتوسطات الحسابية لتلك الفقرات ما بين (4.64 – 4.1)، وبلغ المتوسط الحسابي الكلي لهذا المجال 4.5، وهو يمثل الدرجة العالية، فقد حازت عبارة "عقد المؤتمرات والندوات العلمية باستمرار للتوعية الفكرية وإكساب المعارف والمهارات اللازمة لحماية البيانات" أعلى متوسط حسابي وأعلى وزن نسبي بنسبة 93.3٪، وهذا مؤشر على أن المؤسسات التعليمية والتربوية لها دور مهم في إكساب المعارف والمهارات اللازمة لحماية البيانات والتوعية بمخاطر الاستخدام السلبي لتكنولوجيا الاتصال وتعزيز ثقافة المواطنة الرقمية والأمن السيبراني.

الرؤية الاستراتيجية المقترحة للحد من الجرائم الإلكترونية

انطلقت الرؤية الاستراتيجية من واقع خلاصة تحليل نتائج آراء الخبراء والمتخصصين – عينة الدراسة- في الجولة الثالثة والتي حصلت على نسبة توافق عالية، ومن واقع توصيات الدراسات السابقة، وتحليل الوثائق المتعلقة بالأبحاث والكتب العلمية والتقارير الدولية، كالتقرير السنوي للمنتدى الاقتصادي العالمي الخاص بالمخاطر والتهديدات العالمية التي تناولت الأمن السيبراني، واستراتيجية (2030) التي أعلنتها وزارة الاتصالات وفق منهجية التخطيط الاستراتيجي التي تتناول ثلاث خطوات رئيسة، وتتمثل في الشكل الآتي: –

أولًا: أين نقف: أي تحليل الواقع الراهن - منظومة الأمن السيبراني المصري - تم الاعتماد في ذلك على أداة التحليل الاستراتيجي (SWOT Analysis)، لدراسة نقاط القوة والضعف في البيئة الداخلية، وكذلك نقاط الفرص والتهديدات في البيئة الخارجية – لغرض معالجتها أو التقليل منها، لرفع كفاءة أداء المنظومة الأمنية السيبرانية ، وإمكانية التنبؤ بكافة الفرص المتاحة لها.

نقاط القوة: وتتمثل في جهود الدولة المصرية لمكافحة تلك الجرائم للحفاظ على الأمن السيبراني، وتتمثل في: - وجود استراتيجية فعالة لإدارة مخاطر أمن المعلومات- وجود استراتيجية وطنية للأمن السيبراني- إرساء أسس "حوكمة الأمن السيبراني في معظم القطاعات- الاستقرار السياسي والاجتماعي والاقتصادي– وجود برامج وأقسام أكاديمية مخصصة للأمن السيبراني في الجامعات- الاهتمام بدراسات وأبحاث الفضاء السيبراني- تطوير الإجراءات المضادة لتلك الجرائم- إنشاء هيئة وطنية للدفاع المعلوماتي- وجود فريق فني وتقني متخصص في التقنية المعلوماتية– إصدار قانون حماية البيانات الشخصية، وبالتالي رفع مستويات أمن البيانات - إنشاء مركز للاستجابة للطوارئ المعلوماتية «CERT» لتعزيز أمن البنية المعلوماتية- تشكيل المجلس الأعلى للأمن السيبراني- احتلال مصر مرتبة متقدمة في مؤشر الأمن السيبراني Global

Cybersecascii117rity Index GCI - إصدار قانون مكافحة جرائم تقنية المعلومات.

- **نقاط الضعف، وتتمثل في:** غياب الوعي المجتمعي بالتهديدات والهجمات السيبرانية- ضعف التمويل اللازم لحماية البنية التحتية الرقمية- صعوبة التنبؤ بالمخاطر وتوقعها وتجنبها- نقص عدد المختصين والتقنين الذين يمتلكون المهارات اللازمة في مجال الأمن السيبراني- ضعف الدور الإعلامي في التوعية بالجرائم التي تهدد الأمن السيبراني ومحاربة الشائعات والأخبار المضللة- غياب الثقافة الرقمية للاستخدام الآمن والأمثل لإدارة البيانات بشكل فعال من قبل معظم أفراد المجتمع.

الفرص: التحول الرقمي العالمي- التطور التكنولوجي الكبير- التعاون الدولي لمكافحة تلك الجرائم- الاتفاقيات والشراكات الدولية للحفاظ على الأمن السيبراني- الوعي العالمي بخطوة الهجمات والتهديدات السيبرانية- وجود ميزانية سنوية دولية مخصصة للدفاع عن الأمن السيبراني ومكافحة مخاطره- التنسيق الدولي بين الدول في سبيل تأمين الفضاء السيبراني.

التهديدات: الفضاء الافتراضي المفتوح الذي أسهم في التطور السريع للجرائم السيبرانية- التكلفة التكنولوجية المرتفعة لحماية الأمن السيبراني- تطور أسلحة المجرم المعلوماتي واعتماده على تقنية عالية في التعامل مع التقنية المعلوماتية- العولمة الرقمية- الغزو الفكري- صعوبة التعرف على منفذي تلك الهجمات بسهولة - الاستغلال السيء لثورة تكنولوجيا المعلومات - السرعة في إتلاف الأدلة ومحو آثارها - وجود بعض الجهات الخارجية التي تتربص بالأمن القومي.

ثانيًا: إلى أين نريد أن نصل؟ ويتمثل ذلك في تحديد ركائز الرؤية الاستراتيجية وأهدافها، ويمكن توضيحها كما يأتي:

أ. ركائز الرؤية الاستراتيجية

انطلقت الرؤية الاستراتيجية من عدة ركائز، وتمثلت في: -

- الرؤية المستقبلية رؤية مصر 2030، لتحقيق الاستقرار والتنمية المستدامة والحفاظ على الأمن السيبراني والاستراتيجي.

- المادة (31) من الدستور المصري، والتي نصت على أن حماية أمن الفضاء الإلكتروني أمن قومي.
- استراتيجية 2020 "التي أعلنتها وزارة الاتصالات وتكنولوجيا المعلومات، المتمركزة حول ثلاثة أهداف أساسية، ممثلة في: التحول نحو مجتمع رقمي، تطوير صناعة تكنولوجيا المعلومات والاتصالات، وتحويل مصر إلى مركز رقمي عالمي.

ب. أهداف الرؤية الاستراتيجية

هناك مجموعة من الأهداف التي سعت الرؤية الاستراتيجية لتحقيقها، وتتمثل في: -

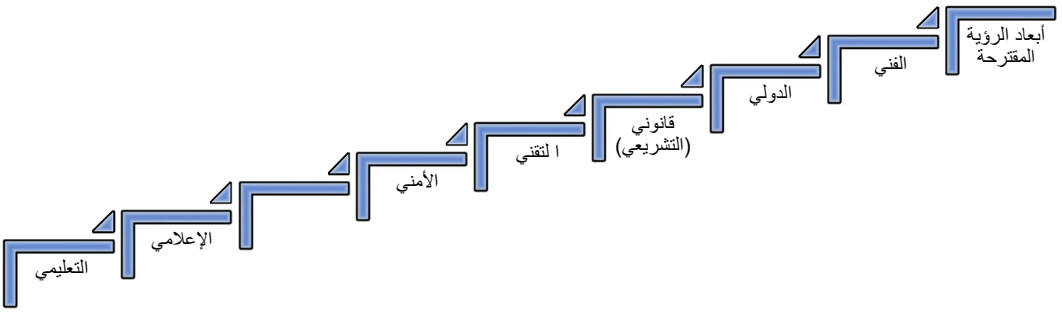
- تعزيز سياسات الأمن السيبراني، من خلال توفير الحماية الفعالة للبنية الحيوية التحتية.
- تفعيل دور الإعلام بمختلف وسائله في مجال التوعية بمخاطر وتهديدات الفضاء السيبراني.
- تعزيز التكامل والتعاون بين كافة قطاعات وأجهزة الدولة ذات الصلة والقطاع الخاص لمواجهة المخاطر والاستجابة السريعة للهجمات الرقمية.
- تعزيز الوعي العام بمجال الأمن السيبراني، بما يتماشى مع التطور التكنولوجي في مجال الحوسبة السحابية وإدارة البيانات وحوكمة المعلومات وتقنيات الذكاء الاصطناعى (AI) .

كيف نصل؟

وتم تحديد ذلك من خلال تحديد المؤشرات والآليات التي تساعدنا على الانتقال من الواقع الحالي (أين نقف؟) للوصول إلى الأهداف المرجوة (إلى أين نريد أن نصل؟)، وبالاعتماد على خلاصة تحليل نتائج آراء الخبراء والمتخصصين -عينة الدراسة- في الجولة الثالثة، وعلى توصيات الدراسات السابقة، ويمكن عرضها كما يأتي: -

منطلقات الاستراتيجية المقترحة:

- تتمثل في عدة آليات وأبعاد تشمل مختلف القطاعات الحيوية المهمة والتي من شأنها التقليل من مخاطر وتهديدات الجرائم الإلكترونية، وتتمثل في الشكل التالي : -



شكل (1) يوضح أبعاد الرؤية المقترحة

البعد التعليمي:

هناك مجموعة من المتطلبات التي يجب على المؤسسات التعليمية والتربوية تفعيلها داخل المؤسسات التعليمية بكافة مراحلها للحفاظ على الأمن السيبراني: -

- إدراج أنظمة مكافحة جرائم الفضاء السيبراني ضمن المناهج التعليمية لكافة المراحل الدراسية، لتعزيز ثقافة الأمن الرقمي، والتي من شأنها دعم الاستخدام الآمن لتكنولوجيا الاتصال.
- إعداد دراسات عن التجارب العالمية لحماية البنية الحيوية التحتية.
- إقامة المؤتمرات والندوات العلمية بشكل دوري للتوعية الفكرية للشباب ولمواجهة خطر الإلحاد والتطرف الفكري.
- تطوير مهارات الطلاب البحثية لتكوين كوادر مهنية متخصصة في مجال إدارة الأمن السيبراني، وتعزيز الوعي الأمني لديهم، بما يتماشى مع التطور التكنولوجي في مجال الحوسبة السحابية وإدارة البيانات.
- تطبيق التربية الإعلامية كمقرر أساسي للطلاب في مراحل التعليم ما قبل الجامعي، للتعرف على الأخبار الزائفة والشائعات المثارة عبر المنصات الرقمية.
- الحراك العلمي الدولي من خلال عقد شراكات واتفاقيات دولية بين الجامعات، بهدف زيادة تأهيل المختصين للتعامل مع تلك الجرائم والمجالات ذات العلاقة.

- القيام بعمل دراسات متطورة لتحليل المخاطر والتهديدات في البنية التحتية الحيوية، والاستجابة إلى خروقات الأمن، لضمان بيئة حوسبة أمنة لحماية المعلومات.
- تعزيز المسؤوليات والالتزامات الأخلاقية لدى الطلاب عند استخدام المنصات الرقمية وتوظيفها لخدمة المجتمع والوطن.

البعد الأمني:

يتعلق هذا الجانب بكل ما هو أمني لحماية البنية التحتية الرقمية، من خلال:

- إعادة هيكلة منظومة الجهاز الأمني المعلوماتي وتطويره بما يتناسب مع المستجدات العصرية، من خلال تقوية وتحديث أنظمة التشغيل، ورفع كفاءة المبرمجين، لتصميم برامج وأنظمة من الصعب اختراقها أو تهكيرها.
- إخضاع المواقع الإلكترونية المشتبه فيها للرقابة المشددة، لإعداد خطط المواجهة، واتخاذ التدابير الاحترازية بشكل دوري.
- الفحص الأمني للأنظمة التقنية للمنشآت الحيوية باستمرار،ولتأمين الخدمات الحكومية وقطاعات البني التحتية الحساسة.
- اعتماد معايير حماية مناسبة لإدارة نظام العمل عن بُعْد، وخصوصًا في ظل انتشار جائحة كوفيد 19.
- زيادة نظم تأسيس البيانات الشخصية للمسؤولين بالدولة وإنشاء نسخ احتياطية مؤمنة.
- وضع سيناريوهات لمنع محاولات اختراق المواقع الإلكترونية الرسمية، للوقوف على الثغرات التي تحتمل من خلالها اختراق تلك المواقع، واستخدام الأساليب الحديثة لمتابعة مستخدمي تلك المواقع.
- إنشاء مراكز متخصصة لتلقي الشكاوى ضد تلك الجرائم، لديها قدرات ومهارات فنية وإدارية وتقنية للتعامل معها على غرار المركز الأمريكي IC3.

البعد التقني:

يتعلق هذا الجانب بكل ما هو تقني لحماية المنظومة التقنية الاتصالية من الاختراقات والتهديدات، ويتم الارتقاء بتلك الآليات بعدة طرق، وتتمثل في: -

- استخدام تقنيات وبرامج حماية متقدمة للبريد الإلكتروني وللحسابات الرسمية، مضادة للفيروسات قادرة على التصدي لأي هجمات مشبوهة، ولرفع كفاءة معايير الأمن والأنظمة، قادرة على معالجة المخاطر الرقمية المتعلقة بالحوسبة السحابية للبنيات التحتية الحيوية.
- تطوير البرمجيات المقاومة للهجمات السيبرانية من خلال تزويد أنظمة أمن المعلومات بأحدث الأساليب والتقنيات وخصوصًا تقنيات الذكاء الاصطناعي، للتصدي للتهديدات والهجمات السيبرانية المحتملة.
- التحديث المستمر لبرامج مكافحة التجسس وإيجاد أقصى درجات الحماية للبيانات.
- عمل شفرات لاكتشاف الهجمات المحتملة وتتبعها ، ورصد آلية كيفية تطويرها وإنشاء نظام الإنذار المبكر لرصد الهجمات والتهديدات السيبرانية المتوقعة، وذلك من خلال عمل محاكاة لتقنيات الهجوم الرقمية الفعلية لكشف نقاط الضعف الأمنية.
- اتباع سياسة فعالة وقوية لتشفير البيانات والمعلومات الحساسة والتركيز على أمن التقنية السحابية.

البعد الإعلامي :

للإعلام دور مهم في التوعية والتصدي لتلك الجرائم، فهناك مجموعة من الآليات والاستراتيجيات الإعلامية، وتتمثل في: -

- معالجة القضايا الأمنية الاستراتيجية الرقمية من خلال استضافة المتخصصين والخبراء في هذا المجال في مختلف وسائل الإعلام.
- التوعية الدائمة لمستخدمي المنصات الرقمية بالطرق التي يمكن للقراصنة اختراق الأنظمة والبيانات الحساسة والكشف عن الأساليب والحيل والتكنيكات المستخدمة.
- العمل على الإفادة من إيجابيات الإعلام الرقمي بما يخدم المصلحة العليا للبلاد من خلال توظيفها في نشر الوعي والثقافة الرقمية، ودعم أمن وسلامة البلاد.

- تثقيف الجمهور بالمخاطر المرتبطة بالبنية التحية الحيوية للمعلومات، للإبلاغ عن الحوادث السيبرانية ، وتعريفه بالقوانين والعقوبات الرادعة لمرتكبيها، وكذلك بكيفية تجنب الوقوع ضحية للمجرمين في مختلف وسائل الإعلام .
- إطلاق حملات أمنية تليفزيونية ورقمية متكاملة لتعزيز الوعي الثقافي بالقوانين والسياسات المتعلقة بالأمن السيبراني والجرائم السيبرانية وأساليب اختراق المواقع والحسابات الشخصية والرسمية،وتعزيز الاستغلال الأمثل للمنصات الرقمية.
- عمل منصات ومبادرات رقمية لمكافحة الشائعات والأخبار المضللة، خصوصًا في ظل انتشار جائحة كوفيد 19، ولرفع درجة الوعي الاجتماعي بمخاطر التوظيف السيء لوسائل التكنولوجيا لدى الأفراد والمؤسسات.
- تعزيز الأمن السيبراني داخل المجتمع من خلال بث البرامج التليفزيونية والرقمية التي تبين مخاطر الجرائم والتهديدات السيبرانية وأسباب انتشارها وانعكاساتها على الأمن القومي للدولة.

البعد التشريعي:

أي الاهتمام القانوني لحماية الأمن السيبراني من التهديدات والمخاطر، وتتمثل في: -

- إقرار اللائحة التنفيذية لقانون مكافحة تلك الجرائم، وآليات تطبيق قانون تلك الجرائم، وخصوصًا المتعلقة بالتحريض والشائعات واختراق الحسابات الرسمية.
- تخصيص دوائر قضائية لمرتكبي تلك الجرائم لسرعة البت في تلك القضايا، وعدم استخدام مادة الرأفة من قانون العقوبات في مثل تلك النوعية من الجرائم.
- ضرورة وضع قوانين وتشريعات على كل ما يتم بثه وتداوله من معلومات وأخبار على شبكة الإنترنت، بشكل يتيح تتبع مرتكبى الجرائم الرقمية بشكل دقيق.
- تتبع المعلومات الرقمية ورصدها، لغرض تحديد الاتجاهات واستراتيجيات العلاج طويلة الأجل، للقضاء على تلك النوعية من الجرائم.
- سن التشريعات الدقيقة الشاملة التى تناسب مقاومة تلك الجرائم، من خلال صياغة قوانين تنظم وتواكب التطورات التكنولوجية المتسارعة للحد من التهديدات والمخاطر المحتملة.

البعد الفني:

ويتمثل في تطوير قدرات ومهارات العاملين في قطاع أمن المعلومات من خلال عدة آليات، وتتمثل في: -

- تزويد العاملين بأحدث الأجهزة والبرامج التقنية، لمساعدتهم في الحصول على المعلومات الدقيقة، وتعزيز السلامة المعلوماتية، والتعرف على مواطن الضعف في المنتجات البرمجية.
- تطوير الإمكانات والمهارات الأمنية من متخصصين وخبراء في هذا المجال، لتعزيز المعرفة والخبرة لرفع مكانة الأمن السيبراني، ولاستيعاب التطورات المعرفية المتسارعة لعصر المعرفة والمعني بالشبكات الذكية.
- التدريب المستمر للكوادر الفنية وتأهيلهم بمهارات احترافية عالية وفق المعايير المهنية المعترف بها على كيفية التعامل مع تلك الهجمات، ورفع درجة الوعي لديهم بالمخاطر والتهديدات المصاحبة للتطور السريع لاستخدام التكنولوجيا.
- عقد ورش تدريبية باستمرار عن الذكاء السيبراني الاستراتيجي، وكيفية توظيفه في جميع قطاعات الدولة الحيوية، لتقليل مخاطر التهديدات السبيرانية المحتملة.

البعد الدولي:

- هناك مجموعة من الآليات التي يجب مراعاتها على الصعيد الدولي، والتي من شأنها الحد والتقليل من انتشار تلك الجرائم:
- عقد شراكات واتفاقيات دولية في حماية البنى المعلوماتية العالمية وإنشاء مركز دفاع دولي.
- التعاون القضائي المشترك بين الدول ووضع تدابير قانونية دولية من سن قوانين مشتركة للتعامل مع تلك الجرائم، للحفاظ على الاستقرار والأمن الدولي.
- التعاون الدولي في مجال حماية وتأمين الفضاء السيبراني والدفاع والردع ضد الإرهاب ومواجهة التحديات الأمنية السيبرانية.
- عقد مؤتمرات وندوات دولية لمناقشة الأمن السيبراني والهجمات الإلكترونية للإرهابيين وتقييم التجارب السابقة في مكافحة الإرهاب السيبراني.
- إنشاء هيئة استخبارات دولية لجمع وتبادل المعلومات الاستخبارية عن المواقع الإرهابية والهجمات الرقمية المحتملة.

- التعزيز الدولي لمعايير البنية التحتية، وتبادل المعلومات عن التهديدات السيبرانية، ووضع عقوبات دولية لمعاقبة وردع منفذي تلك الجهات ومموليها.
- التدريب الدولي المشترك لمواجهة الهجمات السيبرانية، والوقوف على أحدث التكنيكات وامتلاك المعارف حول التدابير الوقائية المختلفة للحد من تلك الجرائم، وحماية المعلومات الحساسة.

الأطراف المستهدفة للاستراتيجية (الشركاء الأساسيون للاستراتيجية المستهدفة)

التعاون المتبادل بين الوزارات والقطاعات الحكومية والخاصة الحيوية في المجتمع للحد من مخاطر وتهديدات الجرائم الإلكترونية وتوفير الحماية الشاملة للبيانات والمعلومات ، والتصدي لأي هجمات إلكترونية تضر بنظام الأمن السيبراني ، ممثلًا في: -

شكل (2) يوضح الأطراف المستهدفة

أي إشراك كل من القطاعات الحكومية ذات العلاقة المباشرة بالأمن السيبراني والبنية التحتية الحيوية، إضافة إلى إشراك مؤسسات القطاع الخاص تأكيدًا على مبدأ الشراكة من النواحي التشريعية، التقنية، الإعلامية، الأمنية، التربوية، والتعاون على المستوى الإقليمي والدولي للحد من تلك الجرائم.

ختامًا يمكن القول بإن: - الجرائم الإلكترونية إذا لم يتم السيطرة عليها سوف تصبح غاية في الخطورة ، فالقضاء عليها تمامًا غير ممكن شأنها شأن بقية الجرائم الأخرى، ولكن يمكن تنفيذ السياسات والآليات اللازمة لتقليل مخاطرها ، لأنه بقدر تطور أساليب

وتكنيكات الجريمة تتطور أساليب مكافحتها، فالحد منها يتطلب تعاون مشترك من كافة الجهات المعنية ، للحفاظ على الأمن القومي وتعزيز الرؤية المستقبلية "رؤية 2030" .

توصيات الدراسة:

في ضوء النتائج التي توصلت لها الدراسة، فإنها توصي بعدة نقاط أساسية، على الحكومات مراعاة النقاط التالية للحفاظ على أمنها السيبراني: -

- تطوير البنية التحتية الرقمية؛ لمواكبة تقنيات الذكاء الاصطناعي وتحولات الثورة الصناعية الخامسة والتقدم العالمي المتسارع في الخدمات الرقمية، بما يضمن سبل وقائية فعالة لحماية تلك الساحة الافتراضية، خصوصًا في ظل انتشار الأزمات العالمية.
- تخصيص ميزانية لمنظومة الأمن السيبراني؛ لزيادة تطوير إمكانياتها وقدراتها، لمواجهة تلك الجرائم والتهديدات.
- تعزيز التعاون الإقليمي والدولي بين كافة الأجهزة المختلفة: القضائية– التشريعية- الإعلامية– الأكاديمية– الأمنية؛ لوضع خطط وسياسات مشتركة وقائية فاعلة للتصدي لتلك الجرائم.
- إجراء المزيد من الدراسات البينية المشتركة ما بين مجال الإعلام والأمن السيبراني.

قائمة الهوامش والمراجع

1. - Ahmed Alkaabi , A strategic Vision to Reduce Cyber-Crime and Enhance Cyber security, **International Journal of Advanced Science and Technology**, Vol. 29, No. 7 , 2020, pp 14268-14274.
2. - Mohammed I. Alghamdi , A Strategic Vision to Reduce Cybercrime to Enhance Cyber Security **, Webology**, Vol 17, No 2, December, 2020 ,pp289-295.
3. - محمد حميد، مصطفى جاد الحق، رؤية استراتيجية لمكافحة الجرائم السيبرانية، **المجلة العربية الدولية للمعلوماتية**، المجلد 7، العدد 12، ٢٠١٩.
4. محمد مسعد، رؤية استراتيجية لمكافحة الجرائم السيبرانية تعزيزًا للأمن الإنساني، **رسالة ماجستير** (جامعة نايف العربية للعلوم الأمنية: كلية العلوم الاستراتيجية ، 2019).
5. - على الشهري، رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، **رسالة دكتوراه** (جامعة نايف العربية للعلوم الأمنية: كلية العلوم الاستراتيجية، 2019).
6. - بدرة لعو، الأمن الإلكتروني وفقًا للتشريع الجزائري: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال نموذجًا، **المجلة العربية للدراسات الأمنية**، المجلد 33، العدد 72، 2018.
7. - عبدالاله المطيري، دور الإعلام الجديد في التوعية من الجرائم الإلكترونية، **رسالة ماجستير** (جامعة نايف العربية للعلوم الأمنية: كلية العلوم الاجتماعية ، 2018).
8. ميادة بشير، يوسف عثمان، توظيف برامج العلاقات العامة في التوعية بمخاطر الجرائم الإلكترونية : دراسة تحليلية وصفية على الإدارات المسؤولة عن الجرائم الإلكترونية (وزارة العدل، وزارة الداخلية، ووزارة الاتصالات وتكنولوجيا المعلومات في الفترة بين 2016- 2017م) **مجلة العلوم الإنسانية**، المجلد 19، العدد 2، 2018، ص156-175.
9. لورنس الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها : دراسة تحليلية مقارنة، **مجلة الميزان للدراسات الإسلامية والقانونية** ، المجلد 4 العدد 1، 2017، ص183-220.
10. بدري فيصل ، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي ، **رسالة دكتوراه** (جامعة الجزائر: كلية الحقوق، 2017).
11. - مريم مسعود، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09، **رسالة ماجستير** (جامعة قاصدي مرباح: كلية الحقوق والعلوم الإنسانية، 2013).

12. - Bob Butler , Irving Lachow ,multilateral approaches for improving global security in cyberspace, **Georgetown Journal of International Affairs**, 2012,pp 5-14.
13. - Kyung Shick , Claire Lee ,The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity, **International Journal of Cybersecurity Intelligence & Cybercrime**, Vol. 1, No .1 ,2018, pp 1-4.
14. - Claire Seungeun , Toward Mitigating, Minimizing, and Preventing Cybercrimes and Cybersecurity Risks**, International Journal of Cybersecurity Intelligence & Cybercrime,** Vol. 3 , Issue 2, 2020, p1.

15. - Roderic Broadhurst, et.ail , Organizations and Cyber crime : An Analysis of the Nature of Groups engaged in Cyber Crime, **International Journal of Cyber Criminology** ,Vol 8 , Issue 1 , 2014 ,pp 1- 20.
16. - Debarati Halder , K. Jaishankar , **Cyber Crime and the Victimization of Women: Laws, Rights and Regulations** (USA : Hersher , 2011) P 55.
17. - Ahmed Alkaabi , op.cit , pp14272-14274.
18. - Mark Evans, et.ail, Heart-is: A novel technique for evaluating human error-related information security incidents, **Computers & Security**, Vol . 80, 2019, pp 74-89.
19. - Hans de Bruijn, Marijn Janssen , Building cybersecurity awareness: The need for evidence based framing strategies, **Government Information Quarterly**, Vol . 34 , No .1 , 2017 , pp 1-7.
20. -Word Economic Forum (2020), **Cybercrime Prevention Principles for Internet Service Providers**, Retvied from: https://es.weforum.org/reports
21. - دولي خضر، ناصر نفيسة، دور الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، **مجلة المؤشر للدراسات الاقتصادية**، المجلد 2، العدد 2، 2018، ص54.
22. - Murat Dogrul,et.ail , Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, **2011 3rd International Conference on Cyber Conflict**, Tallinn, 2011, p 29 .
23. - Ibid, pp 41-42.
24. - Yue Ba , understanding cybercrime and developing a monitoring device , **Bachelor`s thesis Information Technology** (turku university of applied science , 2017) p25.
25. - Qianyun Wang, A Comparative Study of Cybercrime in criminal Law: China, US, England, Singapore and the Council of Europe**, PhD** (Erasmus Universiteit Rotterdam, 2016) pp351-352.
26. - John S. Davis , et.ail , **A framework for programming and budgeting for cybersecurity** (Santa Monica: RAND Corporation, 2016)p 53.

References

- Alkaabi , A (2020): A strategic Vision to Reduce Cyber-crime and Enhance Cyber security, International Journal of Advanced Science and Technology, 29, (7).
- Al-Hawamdeh, L (2017): Information Crimes: Its Pillars and the Mechanism of Combating It: A Comparative Analytical Study, Al-Mizan Journal of Islamic and Legal Studies, 4(1).
- Al-Mutairi, A. (2018): The Role of New Media in Awareness of Cybercrime, Master Thesis ,Naif Arab University for Security Sciences: College of Social Sciences.
- Alshahri, A. (2019): A strategic vision to reduce cybercrime to enhance cybersecurity in the Kingdom of Saudi Arabia, PhD ,Naif Arab University for Security Sciences: College of Strategic Sciences.
- B ,Hans & J , Marijn (2017) : Building cybersecurity awareness: The need for evidence based framing strategies, Government Information Quarterly, 34 (1) .
- Ba ,Y (2017) : understanding cybercrime and developing a monitoring device , Bachelor`s thesis Information Technology , turku university of applied science,
- Bashir, M.& Othman, Y. (2018): Employing Public Relations Programs in Awareness of the Risks of Cybercrime: A Descriptive Analytical Study on the Departments Responsible for Cybercrime (Ministry of Justice, Ministry of Interior, and Ministry of Communications and Information Technology in the period between 2016-2017 AD) Journal of Human Sciences, 19(2).
- Broadhurst , R & et.ail (2014) : Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology , 8(1)
- Butler , B & Lachow , I (2012): multilateral approaches for improving global security in cyberspace, Georgetown Journal of International Affairs .
- Davis ,J & et.ail (2016) : A framework for programming and budgeting for cybersecurity , Santa Monica: RAND Corporation
- Dogrul ,M & et.ail (2011) : Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, 2011 3rd International

Conference on Cyber Conflict, Tallinn .

- Evans , M & et.ail (2019) : Heart-is: A novel technique for evaluating human error-related information security incidents. Computers & Security 80.
- Faisal , B (2017) : Combating Information Crime in International and Internal Law, PhD ,University of Algiers: Faculty of Law .
- Halder ,D & Jaishankar ,K (2011): Cyber Crime and the Victimization of Women: Laws, Rights and Regulations ,USA, Hersher .
- Hamid, M , Gad Al-Haq, M (2019): A Strategic Vision to Combat Cybercrime, The Arab International Journal of Informatics, 12(7).
- I. Alghamdi , M (2020) : A Strategic Vision to Reduce Cybercrime to Enhance Cyber Security , Webology, 17 (2).
- khadr, D., Nasser, N. (2018): The Role of Artificial Intelligence in Confronting Cybercrime, Al Moasher Journal for Economic Studies, 2(2).
- Laou, B. (2018): Cyber Security According to Algerian Legislation: The National Authority for the Prevention of Crimes Related to Information and Communication Technologies as a Model, The Arab Journal for Security Studies, 33(72).
- Masoud ,M (2013) : Mechanisms for Combating Information and Communication Technologies Crimes in the Light of Law No. 04/09, Master Thesis ,Kasdi Merbah University: Faculty of Law and Human Sciences.
- Musaad, M. (2019): A Strategic Vision for combating cybercrime in order to enhance human security, master's thesis ,Naif Arab University for Security Sciences: College of Strategic Sciences.
- Seungeun ,C (2020) : Toward Mitigating, Minimizing, and Preventing Cybercrimes and Cybersecurity Risks, International Journal of Cybersecurity Intelligence & Cybercrime , 3 (2) .
- Shick ,K (2018): Claire Lee ,The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity," International Journal of Cybersecurity Intelligence & Cybercrime, 1 (1).
- Wang ,Q (2016): A Comparative Study of Cybercrime in criminal Law: China, US, England, Singapore and the Council of Europe, PhD ,Erasmus Universiteit Rotterdam .

- World Economic Forum (2020): Cybercrime Prevention Principles for Internet Service Providers, Retrieved from: https://es.weforum.org/reports

Journal of Mass Communication Research «J M C R»

A scientific journal issued by Al-Azhar University, Faculty of Mass Communication

Correspondences

- Al-Azhar University- Faculty of Mass Communication.
- Telephone Number: 0225108256
- Our website: http://jsb.journals.ekb.eg
- E-mail: mediajournal2020@azhar.edu.eg

- **Issue 58 July 2021 - part 4**
- **Deposit - registration number at Darelkotob almasrya /6555**
- **International Standard Book Number "Electronic Edition" 2682- 292X**
- **International Standard Book Number «Paper Edition»9297- 1110**

Rules of Publishing

Our Journal Publishes Researches, Studies, Book Reviews, Reports, and Translations according to these rules:

- Publication is subject to approval by two specialized referees.
- The Journal accepts only original work; it shouldn't be previously published before in a refereed scientific journal or a scientific conference.
- The length of submitted papers shouldn't be less than 5000 words and shouldn't exceed 10000 words. In the case of excess the researcher should pay the cost of publishing.
- Research Title whether main or major, shouldn't exceed 20 words.
- Submitted papers should be accompanied by two abstracts in Arabic and English. Abstract shouldn't exceed 250 words.
- Authors should provide our journal with 3 copies of their papers together with the computer diskette. The Name of the author and the title of his paper should be written on a separate page. Footnotes and references should be numbered and included in the end of the text.
- Manuscripts which are accepted for publication are not returned to authors. It is a condition of publication in the journal the authors assign copyrights to the journal. It is prohibited to republish any material included in the journal without prior written permission from the editor.
- Papers are published according to the priority of their acceptance.
- Manuscripts which are not accepted for publication are returned to authors.