مجلة دراسات في الخدمة الاجتماعية العدد 63 الجزء الثالث يوليو 2023
الموقع الاليكتروني: https://jsswh.journals.ekb.eg بريد إليكتروني: jsswh.eg@gmail.com

جهـود منظمات مكافحة الجريمة المعلوماتية في تحقيق الأمن السيبراني

Efforts of organizations to combat cybercrime in achieving cyber security

الدكتورة سلمي محسن حسن صالح

دكتوراه الفلسفة في الخدمة الاجتماعية تخصص " تنظيم المجتمع"

ملخص:

الجريمة المعلوماتية أحد متغيرات العصر الحديث والتي تعتبر من أصعب أشكال الجرائم لأنها أكثر صعوبة في اكتشاف مرتكبها، كما أن التطور السريع في التقنيات الحديثة، جعل من اليسير ارتكاب الجريمة المعلوماتية بكافة أشكالها، وسلطت تلك الدراسة الضوء على أساليب مواجهة الجريمة المعلوماتية من خلال جهود المؤسسات الحكومية والخاصة والتي تختص في مواجهة الجريمة المعلوماتية، وأشكال الجريمة المعلوماتية، آليات منظمات مكافحة الجريمة الالكترونية في مصر، دور وزارة الداخلية المصرية، وتوصلت الدراسة إلى أن مستوى وقوع الجرائم المعلوماتية في المجتمع المصري مرتفع، كما تم استخدام منهج المسح الاجتماعي، كما أنها تعتبر دراسة وصفية تستهدف تحديد الدور الذي تقوم به منظمات مكافحة الجريمة المعلوماتية في تحقيق الامن السيبرانى، وتكونت عينة الدراسة من (٢٠) مفردة، كما استخدمت الباحثة برنامج spss في التحليل الإحصائي، وأثبتت النتائج أن مستوى أداء منظمات مكافحة الجريمة المعلوماتية مرتفع، كما اكدت النتائج ان هناك العديد من الصعوبات التي تواجه المنظمات في مواجهة الجرائم المعلوماتية، كما أنه توجد العديد من المتطلبات التي تحتاجها المؤسسات لتحقيق الأمن السيبرانى.

الكلمات المفتاحية:(منظمات، الجريمة، المعلوماتية، الأمن السيبرانى).

Abstract:

Information crime is one of the variables of the modern era, which is considered one of the most difficult forms of crimes because it is more difficult to discover the perpetrator, and the rapid development of modern technologies has made it easy to commit information crime in all its forms. This study sheds light on the methods of confronting information crime through the efforts of institutions Governmental and private, which specializes in confronting information crime, forms of information crime, mechanisms of anti-cybercrime organizations in Egypt, the role of the Egyptian Ministry of Interior, and the study found that the level of information crimes in Egyptian society is high, and the social survey method was used, and it is considered a descriptive study It aims to determine the role played by organizations combating information security, sample (20) single, the researcher crime in achieving cyber also used the spss program in statistical analysis, and the results

proved that the level of performance of organizations combating information crime is high, and the results also confirmed that there are many difficulties that Organizations face cybercrime, and there are security. many requirements that organizations need to achieve cyber
Keyswords: (Organizations, Information, crime, Cyber security).

اولاً: مدخل لمشكلة الدراسة:

تطورت الجريمة بتطور نمط حياة الانسان، ولقد بلغ هذا التطور اوجهه بظهور المجتمعات بمفهومها المعاصر، حيث أن هذه المجتمعات أصبحت تعيش الكثير من التراكمات ما نتج عنها وقوع الكثير من الجرائم، وذلك جراء الضغوط النفسية وتميز حيا ة الأفراد بطبيعة برجماتية مادية حيث أصبح الفرد داخل هذه المجتمعات يسعي بشتى الطرق للوصول إلى إشباع رغباته الشخصية، حتى ولو وصل به الامر إلى ارتكاب العديد من الجرائم تكون نتائجها وخيمة على الأفراد بصفة خاصة وعلى المجتمع بصفة عامة (يوسف، صغير،٢٠١٣، ص١).

كما تطورت الجريمة المرتكبة عبر الانترنت بشكل رهيب في الآونة الأخيرة، وذلك بالنظر إلى التطور المستمر والمتسارع لشبكة الانترنت، مما جعل هذه الشبكة وسيلة مثالية لتنفيذ العديد من الجرائم بعيدًا عن أعين الجهات الأمنية، حيث مكنت شبكة الانترنت العديد من المجرمين والجماعات الإجرامية من القيام بعدة أفعال غير مشروعة مستغلين مختلف التسهيلات التي تقدمها هذه الشبكة وذلك بدون أدني مجهود وبدون الخوف من العقاب، وهوما دفع العديد من الدول والهيئات والمنظمات إلى التحذير من خطورة هذه الظاهرة التي تهدد كل مستخدمي الانترنت، حيث أصبحت من أسهل الوسائل التي يعتمد عليها مرتكبي الجريمة (يوسف، صغير، ٢٠١٣ ص٣-٤).

كما أوضح مؤشر «الأمن السيبراني « GCI الصادر عن الاتحاد الدولي للاتصالات أعلن عن حصول مصر خلال 2020 على المركز 23الـــــــــ عالميا بين 182 دولة بـــ 95.45 درجة، بينما تصدرت أمريكا المؤشر بـــ 100 درجة، تلتها بريطانيا في المركز الثاني بـــ 99.54 درجة، ثم السعودية في المركز الثاني مكرر بـــ 99.54 درجة، كاشفا عن أن مصر اتخذت خطوات هامة لدعم الأمن السيبراني من أهمها: تأسيس مجلس أعلى للأمن السيبرانى في عام 2015 ووضع استراتيجية وطنية للأمن السيبراني 2017-2021، إلى جانب تأسيس المركز الوطني للاستعداد لطوارئ الحاسبات

والشركات EG-CERT ، كما جاءت مصر في المرتبة الأولى عالميًا في تنافسية قطاعي الإنترنت والهاتف خلال 2021 وفقًا لمؤشر المعرفة العالمي.(تقرير الاتحاد الدولى للاتصالات، 2022، https://www.itu.int/itu-d/sites/statistics/ar/

وفي ظل الحراك المعلوماتي والتطور التكنولوجي الهائل في مجال تقنية المعلومات والاتصال واقتصاد المعرفة وفي مجال 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(كوفيد19) من عزلة وتباعد اجتماع، الامر الذي أسهم بالفعل في زيادة تفشي معدل الهجمات السيبرانية (سيد، ٢٠٢١، ص١١٦).

ومع شيوع استخدام الكمبيوتر اواخر سبعينات القرن الماضي برزت ظاهرة القرصنة الالكترونية، وسرعان ما تحول السلوك الذى بدأ في بدايته انحرافا لمراهقين شغوفين بالتكنولوجيا، حربًا تشن بين الدول وهى تهدد منشآت حيوية كالمفعلات النووية ومحطات الكهرباء كما تدمر المخزونات النقدية لبنود ودول وتهتك أسرارًا لا يرد لها الخروج الى العلن وكشفت ارقام وبيانات عالمية تزايد الجرائم الالكترونية في مختلف انحاء العالم مع التوسع المتزايد لاستخدام الانترنت والاجهزة الذكية واظهرت دراسة لموقع ارقام ديجيتال ان عدد ضحايا الهجمات والجرائم الالكترونية يبلغ 555 مليون مستخدم سنويًا واكثر من 1.5 مليون ضحية يوميًا فى حين تقع ضحية كل ثانية لهذه الهجمات واكثر انواع الجرائم سرقة هويات وعدد 224 مليون سرقة وأظهرت الدراسة ان مواقع التواصل الاجتماعي هي الاكثر اختراقًا اذ بينت ان اكثر من 600 الف حساب فيسبوك يتم اختراقها يوميا وبينت الدراسة ان الكلفة السنوية المخصصة للأمن المعلوماتي قدرت 100 مليار دولار بعدها كاث في حدود 63.1 مليار دولار سنة 2011 ومن المتوقع ان تتجاوز 120 مليار دولار بحلول سنة 2017 وحسب تقرير نشرته شركة مشاريع الامن الليبرالي (CYBERSECURUTY VENTURES) بعنون Cyber Security Economy Predictions 2017-2021 فان العالم سينفق ما قيمته 1 تريليون دولار خلال الفترة التي تمتد من 2017 الى عام 2021 على منتجات وخدمات الامن السيبراني لمكافحة الجريمة الالكترونية (سيد، 2021، ص117).

وتميزت الهجمات السيبرانية التقنية بتنوعها وظهورها بأشكال مُختلفة ومُعقدة، منها ما يمس حقوق ومصالح عامة للمجتمع، وما يمثل انتهاك لحقوق وحريات الأفراد، واصبحت هذه الجرائم تشكل خطرًا على الاصعدة الاجتماعي والاقتصادي والقانوني نهيك عما تخلفه من تراجع وانهيار فى مجال الاستثمار (بطيخ، 2020، ص18).

وباعتبار المعلوماتية ظاهرة علمية اقتصادية اجتماعية، لا يمكن تتطور دون ان تتوافر لها القواعد القانونية التي تنظم استغلالها ونظرًا لأنها لازالت في مرحلة التطور والتفاعل فإنها مثل كل تطور جديد تحمل في طياتها جانبًا مظلمًا يتجسد في مجال القانون الجنائي في ظاهرة الإجرام المعلوماتي. (القهوجي، 2019، ص7).

وتعتبر الجريمة المعلوماتية من بين الجرائم التى تباينت تسمياتها عبر المراحل الزمانية لتطورها التى ارتبط بتقنية المعلومات فقد اصطلح على تسميتها بداية بإساءة استخدام الكمبيوتر ثم احتيال الكمبيوتر فالجريمة المعلوماتية بعدها جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر ثم الجرائم التقنية العالمية الى جرائم الهاكرز فجرائم الانترنت وأخيرًا (cyber crime) وقد حاولت العديد من الأعمال الاكاديمية تعريف الجريمة الالكترونية وتعرفة بأنها الارتكاب المتعمد لفعل ضار من الناحية الاجتماعي او فعل خطير محظور يعاقب علية القانون وتمثل الجرائم الالكترونية مجموعه الافعال غير القانونية التى تتم عبر معدات او اجهزة الكترونية او شبكة الانترنت او تبث عبرها محتوياتها وهى ذلك النوع من الجرائم التي تتطلب الالمام الخاص بتقنيات الحاسب الألى ونظم المعلومات لارتكابها او التحقيق فيها ومقاضاة فاعليها (الكعبي، ٢٠٠٩ ص٣٣).

والجريمة المعلوماتية ليست مقصورة على منطقة او دولة معينة، هي مشكلة عالمية إلا فى المجتمع العربي قد شهد مؤخرًا تزايدًا ملحوظًا في استخدام التقنية العالمية، مما يؤدي بالتبعية إلى زيادة انتشار الجريمة المعلوماتية والتي تتطلب تكثيف الجهود وأخذ السُبل والآليات الفنية التقنية قبل التشريعية لدعم سياسة الأمن المعلوماتي وتأمين البنية التحتية لتكنولوجيا المعلومات، وإلى نشر الوعي بمخاطر هذه التقنية، وكذلك إلى تشريع قوانين وطنية واقليمية ودولية فى إطار ما يسمي بالاتفاقات لتعزيز الدعم الدولي، والاقليمي لمواجهتها باعتبارها جريمة عابرة للحدود وأفه خطيرة تهدد أمن المجتمعات العربية (الدريبي، ٢٠١٣، ص ٢٥٩).

جهود منظمات مكافحة الجريمة المعلوماتية في مصر:

فيما يتعلق بآليات مواجهة الجرائم المعلوماتية، الجهود الحكومية والأهلية أيضًا في مجال مكافحة الجريمة، فقد أنشأت وزارة الداخلية المصرية عام ٢٠٠٢ آليه في هذا الإطار تحت مسمي " إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للإدارة العامة للمعلومات والتوثيق بالقرار الوزاري رقم ١٣٥٠٧ لسنة ٢٠٠٢ ، وقد تحددت مهام الإدارة في رصد ومتابعة جرائم التطور التكنولوجي وتتبع مرتكبيها من خلال أحدث النُظم الفنية والتقنية الحديثة ويتم تقنين الإجراءات بعد عملية التتبع الفني وضبط القائم بارتكاب الجريمة التي يكون تكييفها القانوني من خلال قانون العقوبات والجريمة التي تتعامل معها الإدارة تتمثل في الأنشطة غير القانونية التي يكون فيها الكومبيوتر وسيلة أو غاية او كليهما وتتخذ أشكالاً متعددة بما فيها الاحتيال باستخدام البطاقات الائتمانية وبيع المواد الالكترونية وانتهاك حقوق الملكية الفكرية في مصر وسرقة البريد الالكتروني والتزوير باستخدام الماسحات الضوئية والطابعات وجرائم الشبكات واختراقها والدخول على أجهزة الحاسب الآلي للغير وسرقة المعلومات التي تمثل سرية خاصة لبعض الأشخاص أو المؤسسات أو الشركات، وقيام البعض بنشر مواقع تُسيء لأشخاص آخرين أو تسئ للدولة، كما ظهرت جرائم عالمية أخري يقوم بها بعض الهاكرز ومنها إطلاق الفيروسات واختراق المواقع الرسمية او الشخصية أو اختراق الأجهزة الشخصية وأنظمة شفرات الكومبيوتر للمؤسسات والأفراد، وجرائم التجسس الصناعي، وجرائم الأموال مثل السطو والاحتيال والنصب والجريمة، وجرائم المخدرات، وغسيل الأموال، جرائم الآداب، تجارة السلاح، جرائم الابتزاز الالكتروني، جرائم الغش الالكتروني، بالإضافة إلى جرائم القرصنة وجرائم محتوي الانترنت من المواقع الإباحية أو المعادية سواء دينيًا وسياسيًا (إسماعيل، ٢٠٢٢، ص١٠٧).

القانون المصري بشأن الجرائم المعلوماتية:

ووفقاً لــ الدستور المصري لسنة 2014 المادة 57، فأن للحياة الخاصة حرمة، وهى مصونة لا تمس، والمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون (العبيدي، ٢٠٢٢، ص٢٤٥).

كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك.

أما المادة 99، تنص على أن كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم وللمضرور إقامة الدعوى الجنائية بالطريق المباشر(العبيدي، ٢٠٢٢، ص٢٤٦).

ووفقاً للبيان الصادر عن المنظمات الحقوقية، يعاقب القانون المصري بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع الكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارا أو صورا وما في حكمها، تنتهك خصوصية أي شخص (العبيدي، ٢٠٢٢، ص٢٤٧).

آلية عمل الإدارة ومراحل التحري والضبط:

تمر القضايا التي ترد إلى إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات، بالعديد من الإجراءات، منها: فحص البلاغ في القسم الفني، وتأكيد المعلومات الواردة به، ثم تثبيت الاتهامات عبر القسم الجنائي، ومهمته تحرير المحضر، ثم يعود الملف على القسم الفني مرة أخري لمتابعة الإيميلات ونصب الكمائن الإلكترونية، وتحديد شخصية المتهم، وعنوانه، واعداد تقرير فني برقم التليفون المستخدم في الدخول علي الإنترنت، أو مكان مقهي الانترنت المستخدم في ارتكاب الواقعة، ومن ثم يقوم القسم بضبط جهاز الحاسب الآلي المستخدم في ارتكاب الجريمة، وفحصه، وبعد ذلك يتم تسليم الجهاز إلي القسم الفني ليتولى مثل هذه العمليات، واستخراج الأدلة والصور التي تدين المتهم، ثم يتم إعداد تقرير فني استكمالي لإرفاقه مع المتهم الذي يتم إحالته للنيابة للتحقيق، فضلاً عما تقدم، يتم ضبط الجريمة من خلال بلاغ أو معلومة تصل إلي جهاز الأمن، وتقوم الإدارة بتتبعها وإثباتها بالأدلة وبالأسلوب التقني والفني ومدي الجرم والمخالفة التي تمت وتقديم مرتكبها إلى المحاكمة، ومما يساعد على السرعة في الإنجاز والأداء كما أن الإدارة تضم

نخبة متميزة من الضباط والفنيين المدربين على مكافحة جرائم الانترنت، وكيفية التعامل مع أحدث اجهزة الفحص الفني الموجودة بالوزارة للتعامل مع مثل هذه الجرائم والتحفظ عليها بشكل آمن، وسحب كل البيانات، والمعلومات، والصور، بطريقة سليمة لضمها إلي ملف القضية (إسماعيل، ٢٠٢٢، ص١٠٩).

كافحة الجرائم المعلوماتية في مصر

تعمل الدولة على تخصيص رقم مكافحة الجرائم الإلكترونية، من أجل الإبلاغ عن الجرائم المعلوماتية في مصر والذي يكون خلال مدة لا تزيد عن ثلاثة شهور من التعرض للجريمة المعلوماتية، كما أنه لابد من الاحتفاظ بجميع الرسائل والتهديدات الخاصة بالجريمة وتقديمها للجهات المختصة عند الإبلاغ، حيث تحرص الدولة على التحقيق في الجريمة فور الاتصال على الرقم وتقديم البيانات (حسن، ٢٠١٩ ص٣٦).

كما تحرص الدولة على تشديد العقوبات الخاصة بالجرائم الإلكترونية، حيث تسعى بذلك للحد من الجرائم التي يتعرض لها الشخص عبر الإنترنت، بالإضافة إلى الحد من عمليات اختراق الحسابات التي انتشرت في الآونة الأخيرة، تسعى الدولة بذلك على المحافظة على الحرية الشخصية التي من حق أي مستخدم للإنترنت أن يتمتع بها (حسن، ٢٠١٩، ص٣٦).

ومن مظاهر الجهود المبذولة من الإدارة الجديدة تشكيل مجموعات عمل المتابعة شبكة الإنترنت يوميًا على مدى اليوم لمراقبتها وفحص التعاملات والمعاملات التي تتم عليها من وإلى الخارج، وإذا ما ظهر أية مخالفات أو أعمال تمثل خروجا على القانون والشرعية أو تهديد أمن واستقرار الوطن يتم التدخل فورًا بالتنسيق مع الأجهزة النوعية الأخرى ويأتي في إطار الآليات الخاصة بمواجهة الجرائم الالكترونية في مصر، آلية الابلاغ عن الجرائم، حيث بإمكان المواطنين الإبلاغ عن الجرائم الإلكترونية عبر الوسائل الاتية: (صابر، ٢٠٢٣).

1- الموقع الإلكتروني لوزارة الداخلية علي شبكة الانترنت.

2- اخطار إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بمقر وزارة الداخلية بشارع الشيخ ريحان سواء بالحضور الشخصي أو الاتصال بأرقام تليفونات: 27928484/ 27926071 / 27924091 /27924090

3- كما يمكن تلقي البلاغات من خلال الخط الساخن (١٠٨) والذي تم إنشاؤه مؤخرا لهذا الغرض.

دور وزارة الداخلية فى مواجهة الجرائم المعلوماتية: (صابر، ٢٠٢٣)

- التوعية المستمرة للضباط والعاملين في جميع جهات الوزارة.
- تم انشاء الكترونية متخصصة في مجال الحاسبات وبثها لجميع جهات الوزارة عن طريق شبكة الانترنت.
- تم انشاء موقع على شبكة الانترنت وتخصيص صفحة لتلقى بلاغات وشكاوى المواطنين.
- عقد الندوات المتخصصة في بعض مجالات اساءة استخدام التكنولوجيا الحديثة.
- المشاركة فى المؤتمرات والندوات المنعقدة محليًا وعالميًا فى مجال الجريمة المعلوماتية.
- صقل الخبرات العالمية والعلمية لضباط والعاملين عن طريق الدورات التدريبية محليًا ودوليًا.
- المشاركة فى وضع مقترحات التشريعات الجديدة لحماية استخدام الحاسبات والانترنت.
- التنسيق مع الاجهزة النوعية المختصة بأعمال المكافحة وتبادل المعلومات.
- تم انشاء قواعد بيانات تخدم اعمال المكافحة والملفات والسجلات الخاصة بذلك.
- التنسيق مع الجهات المعنية بإصدار التراخيص لمزاولة انشطة تكنولوجيا المعلومات.

دور الجمعيات الأهلية في مكافحة الجرائم المعلوماتية:

ولا يمكن إنكار الدور الذي تمارسه الجمعية المصرية لمكافحة جرائم الإنترنت في مجال التصدي لهذا النوع من الجرائم باعتبارها إحدى الآليات الأهلية التي بذلت من جهود فنية وبحثية من أجل الحد من جرائم المعلوماتية والانترنت، ويمكن رصد بعضًا من هذه الجهود في النقاط التالية: (قرار وزير الداخلية، ٢٠٠٢)

1- وقَعت الجمعية بروتوكول تعاون مع كلية الحقوق جامعة عين شمس بهدف تثقيف وتدريب طلبة وخريجي كليات الحقوق والآداب والإعلام والسياحة والآثار والتجارة والحاسبات والمتخصصين، والسادة القضاة واعضاء النيابة العامة والسادة المحاميين والعاملين في القطاعات القانونية في المؤسسات وتأهيل وإكساب المتدربين المهارات القانونية والعلمية والعملية والفنية الخاصة بارتباط المعلوماتية والاتصالات بتخصصاتهم ومدى تأثير استخدام تكنولوجيا المعلومات في انجاز مهام اعمالهم

والتعريف بماهية التعامل مع الاشكاليات القانونية في حقل المعاملات الالكترونية حول موضوعات تشمل كيفية اثبات الشخصية، كيفية التوقيع الالكتروني، أنظمة الدفع النقدي الرقمي (المال الرقمي أو الالكتروني)، سرية وأمن المعلومات من مخاطر إجرام التقنية العالية، خصوصية العميل، المسئولية عن الأخطاء والمخاطر، حجية المراسلات الالكترونية، التعاقدات المصرفية الإلكترونية، مسائل الملكية الفكرية البرمجيات وقواعد معلومات البنك أو المستخدمة من موقع البنك أو المرتبطة بها، علاقات وتعاقدات البنك مع الجهات المزودة للتقنية أو الموردة لخدماتها أو مع المواقع الحليفة، مشاريع الاندماج والمشاركة والتعاون المعلوماتية.

2- مبادرة انطلقت من القاهرة كمبادرة دولية تبنتها الجمعية الدولية لمكافحة الإجرام السيبيري بفرنسا، بالتعاون مع الجمعية المصرية لمكافحة جرائم الإنترنت، تحمل بارقة أمل لسن قوانين رادعة تحمي رواد شبكة الإنترنت من التجاوزات غير اللائقة التي تحدث على الشبكة، بداية من الإرهاب الإلكتروني ومرورًا بالسطو على الحقوق الفكرية، وانتهاء بتجريم تجارة الرقيق الأبيض على الشبكة العنكبوتية وماهية التنظيم القانوني للعالم الافتراضي بأقسامه من المعاملات القانونية الرقمية وعقود التجارة الإلكترونية وحماية الملكية الفكرية عبر الإنترنت والتعريف بأنماط وأشكال الجرائم عبر الإنترنت وماهية الدليل الرقمي وحجيته في الإثبات وعرض احدث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم.

أشكال الجرائم المعلوماتية: (جابر، ضرغام،٢٠١٧، ص١٧).

1- تخريب المعلومات وإساءة استخدامها: ويشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب، تحريف المعلومات، تحريف السجلات الرسمية.

2- سرقة المعلومات ويشمل بيع المعلومات كالبحوث والدراسات الهامة أو ذات العلاقة بالتطوير التقني أو الصناعي، او العسكري أو تخريبها أو تدميرها.

3- تزوير المعلومات ويشمل الدخول لقواعد فى النظام التعليمي وتغيير المعلومات وتحريفها مثل تغيير تقديرات الطلاب.

4- تزييف المعلومات: وتشمل تغيير فى المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.

5- انتهاك الخصوصية: ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها.
6- التصنت: وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.
7- التجسس: ويشمل اعتراض المعلومات ومحاولة معرفة ما يكون به الأفراد.
8- التشهير: ويشمل باستخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.
9- السرقة العلمية: الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.
10- سرقة الاختراعات وخاصة فى المجالات العلمية لاستخدامها أو بيعها.
11- الدخول الغير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.
12- قرصنة البرمجيات: ويشمل النسخ الغير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.
13- قرصنة البيانات والمعلومات: ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.
14- خلاعة الأطفال: وتشمل صور خاصة للأطفال " الجنس السياحي للأطفال خاصة، وللإناث بشكل عام ونشر الجنس التخيلي (Cyber sex).
15- القنابل البريدية: وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملقومة إلكترونية.
16- إفشاء الأسرار وتشمل الحصول على معلومات خاصة جداً ونشرها على الشبكة.
17- الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسويق أو المالية أو الهاتف.
18- سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.
19- التحرش الجنسي ويقصد بها المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة أو المحادثة أو الملامسة.

20- المطاردة والملاحقة والابتزاز: وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما، وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.

21- الإرهاب الإلكتروني: ويشمل جميع المكونات السالفة الذكر في بيئة تقنية متعثرة والتي تؤثر على فرص الإرهاب ومصادره هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.

الجهود الدفاعية لمنظمات مكافحة الجريمة المعلوماتية:

تقوم منظمات مكافحة الجرائم المعلوماتية بعمل الآتي وفقاً لهذا الدور:

- تقديم المعلومات لأولئك الذين وقعوا ضحايا للجرائم المعلوماتية للحد من الضرر الذي لحق بهم حال حدوث الجريمة لهم، ومساعدة من يلجئون للمساعدة في حالة وقوعهم ضحايا للجرائم المعلوماتية (Kunz,2004,26-29).
- بعض تلك المنظمات يعمل كوسيط بين ضحايا الجريمة الالكترونية ومؤسسات انفاذ القانون لمساعدتهم على الإبلاغ عن تلك الجرائم حيث أن هؤلاء الضحايا قد لا يعرفون مدي أهمية الإبلاغ عما حدث لهم.
- توفر تلك المنظمات للضحايا الآليات المناسبة التي يمكن أن يستخدموها للإبلاغ عن تلك الجرائم، كما توفر تلك المنظمات الحماية القانونية لهم والدفاع عنهم.
- المطالبة بتعديل بعض التشريعات الحالية بما يتلاءم مع طبيعة جرائم الأنترنت، والتقنية وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات، وشرحها لهم بشكل واضح (الشهري، ٢٠١٩ ص٢٤).

كما اهتمت الكثير من المنظمات العربية المختصة بالمدافعة الاجتماعية ضد الجريمة بالدراسات الأمنية وإعداد أبحاث واقتراحات موضوعية تعالج ظاهرة الجريمة في المجتمع العربي، أخذت في الاعتبار ما يحيط بهذا المجتمع من تطورات اجتماعية واقتصادية وسياسية، تلك الأبحاث الدراسات والتقارير إنما هي أسس لمعالجة تلك الظاهرة لمنع الجريمة وتحقيق الأمن الاجتماعي (النبهان، ١٩٨٩، ص٢٤٣).

الجهود الوقائية لمنظمات مكافحة الجرائم الالكترونية:

وتعتبر الوقاية هي أفضل السُبل في مكافحة الجريمة المعلوماتية وذلك من خلال التدابير التي يجب أن تتخذها الدول لمنع الجريمة المعلوماتية والحد منها(Smith,2003,p3)

- وتكمُن الصعوبة الأساسية التي تعترض سلطات البحث والتحري في ميدان الجرائم المعلوماتية أن مرتكبي هذه الجرائم لا يتركون في غالب الأحيان آثارًا تدل على ارتكابهم بهذه الجرائم، إذ تكون المعلومات محفوظة تحت رقم او رمز سريًا او مشفرة كليًا إذ يصعب الدخول لها أو معرفتها، وبالتالي إقامة الدليل ضد هؤلاء لجناه، لذا وجب السهر على تكوين المحققين من ضباط الشرطة ورجال النيابة العامة وقضاة التحقيق، بل لابد من خلق وحدات خاصة تكون مهمتها الأساسية هي مراقبة وتتبع الشبكة عن طريق الإبحار فيها، ومثل هذه المراقبة القبلية قد تعطي نتائج هامة على مستوي الحد من الجريمة قبل ارتكابها عن طريق الوقاية (جابر، ٢٠١٧، ص٢٣).
- ويبرز الدور الوقائي في تنمية الوعي الأمني للمواطنين والوعي الأمني هو (وعي المواطنين بحقوقه وواجباته القانونية) مما يساعد علي دعم برامج الأجهزة والمؤسسات الأمنية للتصدي للجريمة بأنواعها المختلفة من خلال عمليات الوقاية، ومنها ارتكاب الجريمة، والوعي الأمني عملية مُركبة تتضمن معرفة الحقائق وإدراك المصالح المادية والثقافية وغيرها، وعلاقة هذه المصالح بالواقع الاجتماعي والسياسي والثقافي السائد مع تجنب المصالح الذاتية والانحياز إلى مصلحة المجتمع، ويجب على تلك الأجهزة تبني استراتيجية للتوعية الأمنية للمواطنين (جابر، ٢٠١٧، ص٢٤).

ثانيًا: النظريات المفسرة:

نظرية المنظمات:

وهناك متطلبات تحتاجها المنظمات للقيام بوظائفها هي: (صادق، ١٩٩٨، ص٢١٩)

1. تنمية التفاعل والاتصال الإنساني بين الأعضاء وبين مختلف مكونات المنظمة.
2. إسناد الأدوار الملائمة لأعضاء المنظمة بحيث يقوم كل منهم بالواجبات والأنشطة والمسئوليات التي تتفق مع الدور القائم.
3. تنظيم العلاقات بين مكونات المنظمة بإيجاد التكامل فيما بينهما.

4. العمل على ان تبنى الأعضاء قيمة اجتماعية مشتركة، ومن ضمن هذه القيم الموافقة على أهداف المنظمة والعمل من اجلها.
5. العمل على حصول المنظمة على الموارد التي تحتاجها من البيئة الاجتماعية والطبيعة المحيطة بها، اللازمة في تحقيق أهدافها.
6. إيجاد الوسائل اللازمة لتنظيم عملية اتخاذ القرارات في المنظمة، بحيث يتيح ذلك لغالبية الأعضاء فرص المساهمة في عملية اتخاذ القرار.
7. التنسيق بين الأنشطة التنظيمية بحيث يساعد هذا التنسيق على تحقيق أهداف المنظمة.
8. تنظيم حصول الأعضاء على احتياجات مادية او معنوية كافية نتيجة مساهمتهم في تحقيق أهداف المنظمة.
9. العمل على تنمية وحدة المنظمة وتكاملها.
10. إيجاد الوسائل التي تستطيع بها المنظمة تغيير بناءاتها وأهدافها وتنمية مواردها لكى تتلاءم باستمرار مع الظروف المتغيرة.

وتستفيد الباحثة من الدراسة الحالية في:

1. تحديد الوسائل والأليات التي تستخدمها منظمات مكافحة الجريمة المعلوماتية.
2. تحديد احتياجات منظمات مكافحة الجريمة المعلوماتية لتحقيق دورها.
3. تحديد المتطلبات التي من خلالها يمكن تطوير أداء المنظمة فى مكافحة الجريمة المعلوماتية.
4. تحديد التحديات التي تواجه المنظمات فى تحقيق الأمن السيبرانى.

ثالثًا: مفاهيم الدراسة :

1- مفهوم منظمات مكافحة الجريمة:

مفهوم المنظمة Organizations هي مجموعة من الخبراء يشتركون في اتخاذ قرارات وتحديد أهداف المنظمة بحيث تتفق أراءهم على تعزيز المجتمع ويسعون للعمل وراء المستقبل (Rein, 2015, p33).

2- مفهوم الجريمة المعلوماتية:

- مفهوم الجريمة (لغويًا): الذنب، جُرم وأجرم واجترم.
- المفهوم الثانى: الجناية، جرم عليهم وعليهم جريمة أجرم جنى جناية وجرم إذا عظم جرمه أى أذنب (حسن، ٢٠١٩، ص١٣).

- مفهوم الجريمة: يُعرف "سذرلاند" الجريمة بأنها السلوك الذي تُجرمه الدولة لما يترتب عليه من ضرر على المجتمع، والذي تتدخل لمنعه بعقاب مرتكبيه (شتا، ٢٠٠٤، ص٢٣).
- المفهوم اللغوي: مفهوم الجريمة المعلوماتية (Cyber Crime): تتكون الجريمة الإلكترونية او الافتراضية من مقطعين هما الجريمة (Crime والإلكترونية (Cyber) ويستخدم مصطلح الإلكترونية لوصف فكرة الحاسب الآلي أو عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجة عن القانون.
- مفهوم المعلوماتية (لغويًا): من اشتقاقات الفعل عَلَمَ وعَلِم بالشيء علمًا اى عرفه واعلم الشيء أي جعل له علامة وتعالم الجميع الشيء أي عرفوه، والمعلم يراد به ما يستدل به على الطريق من أثره.
- وجاءت كلمة معلومات للدلالة على التوقيت في قوله تعالى " الحج أشهر معلومات" وكذلك قوله تعالى (ويذكرون أسم الله في أيام معلومات) وكلمه علم تعنى أدرك الشيء بحقيقته، ومصطلح المعلوماتية ى الانجليزية فيقابلها تعبير "information" (جابر، ٢٠١٧، ص٢٣).
- بالنسبة للفقه فقد تعددت التعريفات للجريمة المعلوماتية بإبراز الوسيلة المرتكبة بها الجريمة، او التركيز على موضوع الجريمة، او التقنية المستخدمة او التركيز على جانبي الربح والخسارة لطرفي الجريمة المعلوماتية.
- وعرفت بأنها: كل أشكال السلوك غير المشروع او الضار بالمجتمع الذي يرتكب باستخدام الحاسب.
- كما عرفت بأنها "الأفعال العمدية التي سببت خسارة للحكومة أو ربح للأفراد المرتبطة بتصميم او استخدام او تشغيل النظام الذى تقع هذه الأفعال في نطاقه). وهى نشاط غير مشروع موجه لنسخ أو تغيير أو حذف او الوصول إلى المعلومات المخزونة داخل الكومبيوتر او تلك التي يتم تحويلها عن طريقه (جابر، ٢٠١٧، ص٢٥).
- ومن الجهات التي حاولت وضع تعريف لجرائم الحاسب الالي مكتب تقييم التقنية في الولايات المتحدة الامريكية إذ عرفها بأنها الجرائم التي تلعب فيها البيانات والبرامج المعلوماتية دورًا أساسيًا.

- كما عرفها Metwe بأنها "الفعل غير المشروع الذي يُستخدم فيه الحاسب الآلي كاداه رئيسية "(رستم، ١٩٩٩، ص١١٠).
- ويعرف الأستاذ Mass جرائم الحاسب الآلي بأنها: الاعتداء القانوني الذي يرتكب بواسطة المعلومات الحاسوبية بغرض تحقيق الربح ويعرفها الفقيه الأمريكي (Parker) بشكل أكثر توسعًا، بأنها كل فعل إجرامي متعمد أيًا كانت صلته بالمعلومات، ينشأ عنه خسارة تلحق بالمجني عليه او كسب يحققه الفاعل (عبد الله، ٢٠١١، ص٦٣).

التعريف الدولي للجريمة المعلوماتية: (البداينة، ٢٠١٤، ص٤)

- تعتمد لتعريفات الجريمة الالكترونية في الغالب على الهدف من استخدامها.
- هناك عدد محدود من الأفعال ضد السرية والنزاهة وتوافر بيانات الكومبيوتر أو أنظمة تمثل جوهر الجريمة الالكترونية.
- أعمال متعلقة بالكومبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر، بما فى ذلك أشكال الأفعال المتصلة بجريمة الهوية، وجرائم محتويات الكومبيوتر لا تصلح بسهولة إلى الجهود للوصول إلى تعاريف قانونية للمصطلح الكلى.
- وتعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلى الخلاف الذى أثير بشأن تعريف هذه الجريمة، ومن قبلها تعريف المعلومة ذاتها، فالجرائم المعلوماتية هى صنف جديد من الجرائم ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية، قد يصعب التعامل معها فيمكن تعريف الجريمة المعلوماتية هى كل فعل غير المشروع الذى يتورط فى ارتكابه الحاسب الآلي، أو هو الفعل الإجرامي الذى يستخدم فى اقترافه الحاسب الآلي كأداة رئيسية من خلال الاتصال بالأنترنت وهدفها اختراق الشبكات أو تخريبها والتحريف والتزوير أو السرقة أو الاختلاس أو قرصنة وسرقة حقوق الملكية الفكرية أو التشهير، والجريمة المعلوماتية ذات طبيعة خاصة لتعلقها بأساليب المعالجة الإلكترونية للبيانات من تجميع وتجهيز البيانات بغية الحصول على معلومات(محمد، ٢٠١٥، ص٤٠).

٣- مفهوم الأمن السيبراني:

- مفهوم الأمن لغويًا: الأمن من آمن يأمن آمنًا، أطمأن ولم يخف والأمن يقصد به الاستقرار والاطمئنان ونقول أمن منه أي سلم منه، نجا منه، امن من شره، فإن الأمن يعني صيانة أراضي البلاد وحريتها من العدوان الخارجي، أما الأمن الداخلي فهو حفظ النظام داخل البلاد (حمدوش، ٢٠٠٨، ص١٢).
- **مصطلح السيبرانية**: هو أحد أكثر المصطلحات ترددًا في معجم الأمن الدولي، وتشير المقاربة الاستمولوجية لكلمة (Cyber) إلى أنها لفظة يونانية الأصل مشتقة من كلمة (kybernetes) بمعني الشخص الذي يدير دفة السفينة، حيث تستخدم مجازًا للتعبير للمتحكم، وتجدر الاشارة ان العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكيWieners Norbert وذلك للتعبير عن التحكم الآلي، ويري البعض ان السيبرانية كلمة انجليزية مشتقة من كلمة (Cyber) وتعني(مرتبط بالحاسب الالي أو شبكات الحاسب) (ابن داوود، ٢٠٢٠، ص١٤٨)، وقيل انها تعني فضاء الانترنت أو العالم الافتراضي (الربيعة، ٢٠١٨، ص٨).
- مصطلح السيبرانية تعنى الالكترونية، وقد اتفق علماء المعلوماتية على إطلاق لفظ (سيبرانى) على كل ما يتعلق بالشبكات الالكترونية المرتبطة بالأنترنت والتطبيقات المتنوعة مثل (تويتر، الفيس بوك، الواتس آب وغيرها) (Fouad ,Noran, ,2021)
- **وتعرف الجرائم السيبرانية**: على أنها الجرائم التي تُرتكب ضد أفراد أو مجموعات من الأفراد الذين لديهم دوافع إجرامية لإيذاء سمعة الضحية عمدًا او الحاق الأذى البدني او العقلي بالضحية بصورة مباشرة او غير مباشرة، باستخدام شبكات الاتصالات الحديثة مثل الأنترنت (غرف الدردشة، رسائل البريد الإلكتروني– لوحات الاعلانات والمجموعات والهواتف المحمولة) (Elnaim,2013,p14)
- **المفهوم الاصطلاحي(سيبرانى)**: مجموعة من الإجراءات المُتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة.
- ويُقصد بها: مجموع الإجراءات الواجب اتخاذها من قبل الأجهزة الأمنية أو الأخرى غيرها ذات العلاقة، للمحافظة على سرية المعلومات الالكترونية، ومنع الاختراقات الفيروسية من أجل ضمان وصول المعلومات الحاسوبية إلى الجهات المختصة في الوقت المناسب، وضمان عدم وقوعها في أيدي الأعداء أو الأصدقاء على حد سواء

خصوصًا بعد الثورة الهائلة في عالم الاتصالات والتداولات الالكترونية، حيث شكل هذا النوع من الأمن هاجسًا استراتيجيا للقوي العالمية والمتمثلة في الولايات المتحدة الأمريكية والصين وروسيا، إذ تدور في وقتنا الحالي حرب الكترونية بين هذه القوي من أجل اختراق المعلومات والتأثير على أسعار البورصة والعملات وغيرها من المنشآت (علي، ٢٠٢٠، ص٥٦).

- **الأمن القومي**: هي الإجراءات او الأفعال التي يقوم بها المسئولين إلى جانب مساعدة المواطنون لتحقيق الاستقرار والتنمية من خلال القوة الاقتصادية والعسكرية (دورة الاستراتيجية والأمن القومي، ٢٠٢١).

مفاهيم ذات صلة بموضوع البحث:

- مفهوم الحاسوب (الحاسب الآلي) (Computer): هو عبارة عن جهاز إلكتروني تمّت برمجته حتى يقوم بحل الملايين من العمليات الحسابية والمنطقية بشكل آلي، وفي ثوانٍ معدودة، وتمر عملية حل هذه العمليات بعدة مراحل، حيث يتم إدخال البيانات إلى الحاسوب، ومن ثم يتم معالجتها حتى تتحول إلى معلومات بقيمة معينة، والتي يتم تخزينها واسترجاعها عند الحاجة. ويتم تشغيل الحاسوب بواسطة مجموعة من البرمجيات، والتي تسمى نظام التشغيل، التي تقوم بترتيب الأوامر وتنفيذها حسب الأولوية، بالإضافة إلى تنظيم عمل أجهزة الإدخال والإخراج، وغيرها من الوظائف الأخرى، ومن الأمثلة على أنظمة التشغيل المستخدمة لتشغل الحواسيب: الويندوز والماكنتوش واللينوكس (ابن داوود، ٢٠٢٠، ص١٥٠).
- مفهوم الأنترنت (شبكة المعلومات الدولية): إن اصطلاح الأنترنت هو اختصار لكلمتين إنجليزيتين الأولى International والثانية Network وبالتالي فإن اصطلاح Internet يقصد به شبكة الاتصالات الدولية، ومن أهم التعريفات التي قيلت عن شبكة الأنترنت، أنها شبكة هائلة من أجهزة الكومبيوتر الهائلة المتصلة فيما بينها بواسطة خطوط الاتصال عبر العالم.

يعرفه سلامة بأنه جهاز إلكتروني سريع ودقيق له القدرة على استقبال البيانات وتخزينها ومعالجتها.

وعرفه المناعي بأنه: آلة مساعدة للعقل البشرى ولديه القدرة على استقبال البيانات ومعالجتها وتخزينها بواسطة استرجاعها بسرعة فائقة (القميزي، ٢٠١٧، ص٣١٥).

- **فالأنترنت**: هو مجموعة شبكات وأجهزة الحاسب الإلكتروني التي تتواجد في مختلف دول العالم والتى تتصل ببعضها ويجمع بينها أنظمة الاتصالات الالكترونية التى تستخدم لنقل البيانات Internet Protocol transmission control protocol أى نظام نقل المعلومات، ويمكن لأى شخص لديه جهاز كومبيوتر شخصي pc لديه اشتراك لدى أحد مقدمي خدمة الإنترنت وجهاز كومبيوتر مزود بجهاز المودم Modem وخط تليفوني للدخول على الأنترنت (ابراهيم، ٢٠٠٨، ص١٥).
- **الإنترنت**: هو شبكة عالمية مكونة من مليارات أجهزة الكمبيوتر وغيرها من الأجهزة الإلكترونية تمكّن مستخدميها من الوصول إلى أي معلومات والوصول إلى أي شخص آخر في العالم كما يعدّ الإنترنت وسيلة توصيل جهاز كمبيوتر إلى جهاز كمبيوتر آخر، بحيث يمكن للجهازين إرسال واستقبال جميع أنواع المعلومات مثل النصوص، والصوت، والرسومات، والفيديوهات وهو ليس ملكاً لأحد حيث تتعاون العديد من المنظمات حول العالم في عمله وتطويره، ومن الجدير بالذكر أنّ كابلات الألياف البصرية تعدّ.

رابعًا: الدراسات السابقة المتصلة بموضوع الدراسة:

1. الدراسات المتصلة بالأمن السيبراني:

وسعت دراسة (حميد، ٢٠١٩): لوضع رؤية استراتيجية لمكافحة الجرائم السيبرية، باستخدام الاستبيان كاداه لجمع البيانات، باستخدام المنهج الوصفي والتحليلي، 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.

وسعت دراسة (الشهري، ٢٠١٩): لوضع رؤية استراتيجية للحد من الجرائم الالكترونية لتعزيز الأمن السيبراني، ومن خلال التعرف على طبيعة تلك الجرائم وأسبابها والوقوف على التهديدات والمخاطر التي تعترض الأمن السيبراني، باستخدام المنهج الوصفي، وبالاعتماد على أداتي الاستبيان و S.W.O.T كأدوات لجمع البيانات، وتوصلت الدراسة إلى عدة نتائج لعل من أبرزها : الجرائم الالكترونية التي لا تعترف بأي حدود مكانية أو زمانية، وأن التقنيات الحديثة وفرت فرصًا غير مسبوقة لانتشارها، وأن انتهاك السياسيات الأمنية الخاصة بالأمن السيبراني تمثل أهم التهديدات التي تواجه

الفضاء السيبراني، وتمثلت ملامح الرؤي المقترحة في تطبيقات التشريعات والأنظمة في مواجهة تلك الجرائم من خلال انشاء المزيد من المحاكم المختصة، تطوير التقنيات الحالية لرفع كفاءة رصد تلك الجرائم وملاحقتها، تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم الالكترونية والأمن السيبراني.

كما توصلت دراسة محمد (٢٠٢١) إلى ان الجريمة السيبرانية تتمثل في الأفعال الغير قانونية باستخدام الحاسب الآلي كوسيلة أو هدف، كما توصلت إلى ان الجريمة السيبرية خطر يتعين التصدي له بتوعية وتثقيف الأفراد عن الفضاء السيبراني وبالتدابير الوقائية الكفيلة بتقليل خطر الوقوع في مسار الجريمة الالكترونية.

واستهدفت دراسة اسكندر (٢٠٢٠) إلى تحليل التهديدات التي يتعرض لها الامن القومي والنابعة من الاستخدامات الغير سليمة للفضاء السيبراني مع التركيز بشكل خاص على انماط التوظيف السياسي للأدوات والهجمات السيبرانية وما يشكله ذلك من تهديدات امنية، مع تحديد أبرز الاتجاهات في تصنيف الهجمات السيبرانية وحدود تأثيرها وتهديداتها للأمن القومي، مناقشة الأثار والنواتج من حيث ردود أفعال المنظمات الدولية وما اتخذته من سياسات وما اصدرته من استراتيجيات لمجابهة هذه التهديدات.

2. الدراسات السابقة المتصلة بالجريمة المعلوماتية:

وسعت دراسة الحوامدة (٢٠١٦) لبيان مكافحة الدول للجرائم المعلوماتية من خلال وضع التشريع المنظم لها، بالاعتماد على المنهجين المقارن والتحليلي للنصوص القانونية وتوصلت إلى نتائج مفادها الجهود الوطنية لا تزال دون المستوي المطلوب لمواجهة مخاطر تلك الجرائم، وأيضًا صدور الاتفاقية العربية لمكافحة تلك الجرائم الموقعة ف21-12-يتعد نقطة تحول في التعاون العربي لمكافحتها وأغلبية تلك الجرائم تحتاج لتوافر القصد العام، والبعض منها يتطلب توافر القصد الخاص كأحد الأركان المعنوية للجريمة.

كما استهدفت دراسة عبد الحافظ (٢٠١٦) إلى الوقوف على حقيقة الجهود التي تقوم بها منظمات مكافحة الجرائم الالكترونية، والتعرف على العلاقة بين جهود منظمات مكافحة الجرائم الالكترونية، وتوصلت الدراسة إلى ان انعكاس جهود الوقاية التي تبذلها المنظمة لتنمية الوعي بمخاطر الجرائم الالكترونية.

دراسة ناصيف (٢٠١٧): هدفت الدراسة إلى التعرف على ممارسة برنامج مقترح من منظور خدمة الجماعة لتنمية وعى الشباب بمخاطر الجريمة الالكترونية مطبقة على عينة

من الشباب بجمعية الأهرام للعلوم والتكنولوجيا بالمنصورة – محافظة الدقهلية واعتمدت الدراسة على المنهج شبه التجريبي، وتمثلت أدوات الدراسة في مقياس وعى الشباب بمخاطر الجريمة الالكترونية والمقابلات الفردية والجماعية والتقارير الدورية، تم تطبيقها على عينة مكونة من (٥١) شاب من الشباب أعضاء جمعية الأهرام للعلوم والتكنولوجيا بالمنصورة، ممن يستخدموا تكنولوجيا المعلومات بانتظام، وجاءت نتائج الدراسة مؤكدة على وجود دالة احصائيًا بين الجماعة التجريبية والضابطة في القياس البعدي والقبلي.

كما استهدفت دراسة محمد (٢٠١٩): تحديد مستوى الوعى المجتمعي بالجرائم المعلوماتية لدى الطالبة الجامعية دراسة من منظور تنظيم المجتمع في الخدمة الاجتماعية واعتمدت الدراسة على منهج المسح الاجتماعي وتمثلت أداة الدراسة في استبانة تم تطبيقها على عينة مكونة من 214 طالبة من طالبات المستوى السابع والثامن بقسم الاجتماع والخدمة الاجتماعية في كلية العلوم الاجتماعية، وجاءت نتائج الدراسة مؤكدة على أن أهم الجرائم المعلوماتية من وجهة نظر عينة الدراسة جاءت كالاتي: بث الأفكار المتطرفة والعنف عبر الأنترنت حيث حصلت على متوسط2.75، ثم يليها في الترتيب جرائم السب والقذف والتشهير عن طريق الأنترنت حيث حصلت على متوسط 2.65، ثم يليها جرائم الابتزاز الجنسي عن طريق الإنترنت، حيث حصلت على متوسط 2.57 ثم يليها نشر الفيروسات على الأجهزة الإلكترونية، وتوصلت الدراسة إلى تصور مقترح من منظور طريقة تنظيم المجتمع للحد من مخاطر الجرائم المعلوماتية وتتضمن التصور والمسلمات التي ينطلق منها التصور المقترح، أهداف التصور المقترح.

واستهدفت دراسة سلطان(٢٠٢١) إلى معرفة أشكال الجرائم المعلوماتية وسمات دوافع مرتكبيها، بالإضافة إلى الكشف عن معدل ودوافع مشاهدة الشباب الجامعي المصري للآمال الدرامية العربية التي تحتوي على جرائم الكترونية، وعما اذا كانت هناك علاقة ارتباط بين معدل مشاهدة تلك الأعمال الدرامية واتجاهات الشباب نحو الجريمة الالكترونية، وقد توصلت الدراسة إلى مجموعة من النتائج أهمها تفوق الذكور مرتكبي الجرائم الالكترونية، كما أظهرت الدراسة ان النسبة الأكبر من الشباب في عينة الدراسة لديهم مواقف محايدة تجاه الجرائم المعلوماتية.

واستهدفت دراسة كساب (٢٠٢٠) إلى رصد التغطية الصحافية الإلكترونية للجرائم المعلوماتية وعلاقتها باستخدام الشباب المصري لشبكة الانترنت، كما توصلت الدراسة أن

جريمة النصب والاحتيال على المواطنين في صدارة الجرائم المعلوماتية، كما جاءت جريمة الانتهاك الشخصي لحرمة الحاسب الالي، وجريمة النصب والاحتيال على المواطنين، جريمة الاعتداء على الأموال، جريمة التحريض على ارتكاب أعمال تخريبية بمؤسسات الدولة والارهاب الالكتروني في صدارة جرائم الاعتداءات ضد مؤسسات الدولة.

كما استهدفت دراسة شوارب (٢٠١٨) التعرف على مدي إدراك الجمهور المصري من مستخدمي الانترنت لجرائم الانترنت التي يتعرضون لها أثناء استخدامهم للأنترنت ووضع استراتيجية تساعدهم على تجنب تلك الجرائم ولتحقيق التفاعل الواعي مع استخدام الانترنت وذلك من خلال تسليط الضوء على أهمية مساعدة المستخدمين على انتقاء الرسائل الايجابية وتجنب الرسائل السلبية من خلال تحقيق الادراك والوعي.

واستهدفت دراسة عفيفي (٢٠٢٢) تحديد ماهية القرصنة الالكترونية وأشكالها ووسائلها بالإضافة إلى توضيح تنامي الدور الذي تلعبه الانترنت في نشر أفكار ومبادئ وتنظيمات إجرامية وارهابية، كما تهدف إلى القاء الضوء على هذه الجريمة وأساليب التعامل معها شكلاً وموضوعًا من قبل أجهزة الشرطة والقضاء بما يتناسب مع المخاطر والأثار الاجتماعية والسياسية المترتبة عليها.

كما استهدفت دراسة منجود (٢٠٢٢):تحديد مستوى وعى الشباب الجامعي بمخاطر الجرائم المعلوماتية، وتحديد المعوقات التي تحد من التخطيط لتنمية وعى الشباب الجامعي بمخاطر الجرائم الإلكترونية، وتحديد المقترحات التي تساعد على التخطيط لتنمية التخطيط لتنمية وعى الشباب الجامعي بمخاطر الجرائم الإلكترونية، وصولاً إلى التوصل لرؤية مستقبلية لدور التخطيط الاجتماعي في تنمية وعى الشباب الجامعي بمخاطر الجرائم الإلكترونية، وتعد هذه الدراسة من الدراسات الوصفية ، واعتمدت الباحثة على المنهج العلمي باستخدام منهج المسح الاجتماعي بالعينة لطلاب الخدمة الاجتماعية جامعة حلوان وعددهم(376 (، وتمثلت أداة الدراسة فى استمارة استبيان إلكتروني لطلاب الخدمة الاجتماعية جامعة حلوان، وتوصلت نتائج الدراسة إلى أن مستوى وعى الشباب الجامعي بمخاطر الجرائم الإلكترونية متوسط، كما توصلت نتائج الدراسة إلى أن لا توجد فروق جوهرية دلالة إحصائيًا بين استجابات الطـــلاب وفقًا لمتغير النوع) ذكور وإناث) فى تحديدهم لمستوى تنمية وعى الشباب الجامعي بمخاطر الجرائم الإلكترونية، وأن توجد

فروق معنوية دالة إحصائياً بين استجابات الطـــلاب وفقــاً للمرحلة الجامعية في تحديدهم لمستوى تنمية وعى الشباب الجامعي بمخاطر الجرائم الإلكترونية.

خامسًا: صياغة مشكلة الدراسة:

وبناء على ما تم عرضه من التراث النظري وأطروحات علمية ساهمت في تحديد متغيرات الدراسة الحالية، فإن قضية الدراسة الحالية يمكن صياغتها في الأسئلة التالية:

- ما هي الجرائم التي ترتكب في المجتمع المصري بشكل كثيف؟
- ما هي الجهود التي تستخدمها منظمات ردع الجريمة المعلوماتية؟
- ما هي متطلبات تحقيق الأمن السيبرانى"؟

سادسًا: أهمية الدراسة:

توجد مجموعة من العوامل التي تحدد أهمية الدراسة والتي من خلالها تتضح أهمية الدراسة فيما يلي:

- الجرائم المعلوماتية جرائم حديثة، مما أدى ذلك إلى خلق تحديات متعددة على مستوى الأنظمة القانونية فى مختلف الدول.
- أثارت الجرائم المعلوماتية العديد من المشكلات نظرًا لطبيعتها الخاصة وما تمتاز به من تعقيد وسرعة في ارتكابها إلى جانب قدرة الجناة على الهرب والتخفي.
- الجرائم المعلوماتية جرائم عابرة للحدود والقارات، فقد تُرتكب هذه الجرائم داخل النطاق الاقليمي لأحدي الدول وتتحقق نتائجها خارج النطاق أي داخل دولة اخري.
- يتعين على المجتمع المحلي والدولي أن يتصدى للغزو الإجرامي التقني، من خلال سن المزيد التشريعات والقوانين والعقابية والإجرائية وتنمية الوعي لدي الشباب والمراهقين بخطورة تلك الجرائم المستحدثة.
- الاستخدام الكبير للأنظمة التكنولوجية قاد إلى الكثير من المشاكل والمخاطر، وقدم أصنافًا من الجرائم لم تكن متداولة.

سابعًا: أهداف الدراسة:

يتحدد الهدف الرئيسي للدراسة في تحديد جهود منظمات مكافحة الجريمة في ردع الجريمة المعلوماتية لتحقيق الامن السيبراني، ويمكن تحقيق هذا الهدف من خلال مجموعة من الأهداف الفرعية:

- تحديد الجرائم المعلوماتية الأكثر انتشارًا في المجتمع المصري.

- تحديد دور منظمات مكافحة الجريمة في ردع الجريمة المعلوماتية.
- تحديد الصعوبات التي تواجه المنظمات الحكومية في مواجهة الجريمة المعلوماتية.
- الوصول إلى آليات مقترحة لتعزيز دور المنظمات في تحقيق الامن السيبراني.

ثامنًا: فروض الدراسة:

- من المتوقع ان يكون مستوي وقوع الجرائم المعلوماتية في المجتمع المصري " مرتفع".
- من المتوقع أن يكون مستوي أداء منظمات مكافحة الجريمة المعلوماتية " متوسط".
- من المتوقع أن يكون مستوى جهود المنظمات في تحقيق الأمن السيبرانى "متوسط".
- من المتوقع أن يكون مستوى متطلبات تحقيق الأمن السيبرانى مرتفع".

تاسعًا: الإجراءات المنهجية:

أ- نوع الدراسة: تعد هذه الدراسة من الدراسات الوصفية التي تصور الواقع وتُشخصه وتُسهم وتُحلل ظواهره، وكذلك فالدراسات الوصفية لديها القدرة على تقديم بعض التفسيرات العلمية والمنطقية للظاهرة محل الدراسة، لذا فالدراسة الحالية تستهدف تحديد الدور الذي تقوم به منظمات مكافحة الجريمة المعلوماتية في تحقيق الامن السيبرانى.

ب- المنهج المستخدم: اعتمدت الدراسة على منهج المسح الاجتماعي من أهم المناهج الرئيسية التي تستخدم فى البحوث الوصفية كما يعتبر الأكثر ملائمة وتناسبًا مع مقتضيات وأهداف الدراسة الحالية، حيث انه يعتمد منهج البحث الاجتماعي على عدد الخبراء في منظمات مكافحة الجريمة المحددة في المجال المكاني.

ج- حدود الدراسة:

1- الحدود المكانية للدراسة:

تمثلت الحدود المكانية للدراسة في:

المنظمة	عدد الخبراء
وحدة مكافحة الجرائم الالكترونية.	4
المجلس الأعلى للأمن السيبرانى.	4
النقابة العامة للمحاميين.	4
مؤسسة إعلاميات مصر للتنمية.	4
المركز العربي للتدريب والدراسات الإعلامية	4

أسباب التطبيق على منظمة وحدة مكافحة الجرائم الالكترونية، المجلس الأعلى للأمن السيبرانى:

- تلك المؤسسات الحكومية مختصة في مكافحة الجريمة المعلوماتية.
- تستهدف تحقيق الأمن السيبرانى وهو الموضوع الذي تناولته الباحثة.
- المجالات المكانية التي تم ذكرها هي التي تستهدف الباحثة التطبيق عليها نظرًا لأنها تشير إلى موضوع دراستها.

2- الحدود البشرية:

- الخبراء فى منظمات مكافحة الجريمة المعلوماتية وعددهم (20) مفردة، وهم من تنطبق عليهم شروط العينة على ان يكونوا خبراء في مكافحة الجريمة المعلوماتية حيث لا تقل أعمارهم عن 40عام.
- حصر شامل للخبراء بمنظمات مكافحة الجرائم الالكترونية من الخبراء محل الدراسة وعددهم (٢٠).

الحدود الزمنية:

بحث في فترة اعداد البحث بجانبيها النظري والميداني والتي تتضمن (٣شهور).

أدوات الدراسة

تمثلت أدوات جمع البيانات في:

استبانة للخبراء حول دور مؤسسات مكافحة الجريمة المعلوماتية في ردع الجريمة لتحقيق الامن السيبراني.

مكونة من (٧) أبعاد.

وتتمثل محاور وأبعاد استمارة الاستبيان على:

- البيانات التعريفية لمجتمع البحث من السادة الخبراء فى منظمات مكافحة الجريمة المعلوماتية.
- الجرائم المعلوماتية التي تُرتكب بشكل كثيف في المجتمع المصري.
- أهداف الجرائم المعلوماتية (أهداف مادية – أهداف اجتماعية).
- جهود الوقاية من الجرائم المعلوماتية.
- متطلبات تحقيق الأمن السيبرانى فى المجتمع المصري (متطلبات خاصة بالعاملين – متطلبات تمويلية – متطلبات – متطلبات مجتمعية).

1لمقترحات التي يمكن من خلالها تعزيز دور المنظمات الحكومية في تحقيق الأمن السيبراني.

وصف الاستبيان: اعتمد الاستبيان على التدرج الثلاثي بحيث تكون الاستجابة لكل عبارة (نعم – لا – إلى حد ما).

عاشرًا: الأساليب الإحصائية المستخدمة فى إطار البحث:

المعالجة البيانات تم استخدام البرنامج الإحصائي للعلوم الاجتماعية (spss)، حيث تم الإجابة على اسئلة البحث من خلال:

التكرارات والنسب المئوية.

مجموع الأوزان.

حساب المتوسطات الحسابية.

معاملات الارتباط (بيرسون – سبيرمان) لحساب صدق وثبات أدوات البحث.

الحادى عشر: مناقشة نتائج الدراسة:

جدول رقم (1) يوضح توزيع الخبراء بمؤسسات مكافحة الجريمة المعلوماتية طبقا للنوع ن= 20

م	الجنس	ك	%	الترتيب
1	ذكر	15	75	1
2	أنثي	5	25	2
مجـ		20	%100	

يتضح من نتائج الجدول السابق أن نسبة الذكور من العاملين بمؤسسات مكافحة الجريمة المعلوماتية بلغت (75%)، في حين بلغت نسبة الاناث (25%)، وقد يرجع ذلك إلى شغف الذكور بالمجال التقنى أكثر من النساء.

جدول رقم (2) يوضح توزيع الخبراء بمؤسسات مكافحة الجريمة المعلوماتية طبقا للعمر ن= 20

م	العمر	ك	%	الترتيب
1	40 سنة	8	40	2
2	50 سنة	11	55	1
3	60 سنة	1	5	3
مجـ		20	%100	

يتضح من نتائج الجدول السابق أن نسبة العاملين بمؤسسات مكافحة الجريمة المعلوماتية في عمر (50 سنة) بلغت (55%)، في حين بلغت نسبة من هم في سن (40 سنة) (40%)، يليهم من هم في سن (60 سنة) بنسبة (5%)، وقد يرجع ذلك إلى ان عينة الدراسة تستهدف الخبراء.

جدول رقم (3) يوضح توزيع العاملين بمؤسسات مكافحة الجريمة المعلوماتية طبقا للمؤهل الدراسي ن= 20

م	المؤهل الدراسي	ك	%	الترتيب
1	بكالوريوس	15	75	1
2	دبلوم	3	15	2
3	ماجستير	2	10	3
مجـ		20	%100	

يتضح من نتائج الجدول السابق أن نسبة العاملين بمؤسسات مكافحة الجريمة المعلوماتية الحاصلين على البكالوريوس بلغت (75%)، في حين بلغت نسبة الحاصلين على الدبلومة (15%)، يليهم الذين حصلوا على الماجستير بنسبة (10%)، وقد يرجع ذلك إلى ان تخصص الجريمة المعلوماتية يعتبر حديث العهد، وبالتالي الحاصلين فيه على الماجستير والدكتوراه عدد قليل.

جدول رقم (4) يوضح توزيع الخبراء بمؤسسات مكافحة الجريمة المعلوماتية طبقا لعدد سنوات الخبرة ن= 20

م	عدد سنوات الخبرة	ك	%	الترتيب
1	10 سنوات	12	60	1
2	20 سنة	8	40	2
مجـ		20	%100	

يتضح من نتائج الجدول السابق أن الخبراء بمؤسسات مكافحة الجريمة المعلوماتية ممن لديهم عدد سنوات الخبرة (10 سنوات) بلغت نسبتهم (60%)، في حين بلغت نسبة من لديهم عدد سنوات خبرة تصل لـــ (20 سنة) (40%)، وقد يرجع ذلك إلى ان مجال الجريمة المعلوماتية حديث العهد وبالتالي عدد الخبراء فيه قليل.

جدول رقم (5) يوضح توزيع الخبراء بمؤسسات مكافحة الجريمة المعلوماتية طبقا للتصنيف الوظيفي ن= 20

م	التصنيف الوظيفي	ك	%	الترتيب
1	قطاع حكومي	9	45	2
2	قطاع خاص	11	55	1
مجـ		20	%100	

يتضح من نتائج الجدول السابق أن نسبة العاملين بمؤسسات مكافحة الجريمة المعلوماتية في القطاع الخاص بلغت (55%)، في حين بلغت نسبة ن الخبراء بمؤسسات مكافحة الجريمة المعلوماتية في القطاع الحكومي (45%).

جدول رقم (6) يوضح توزيع اسهامات الخبراء بمؤسسات مكافحة الجريمة المعلوماتية ن= 20

م	الاسهامات	ك	%	الترتيب
2	الأبحاث العلمية	1	8.3	4
3	تنظيم ورش العمل	2	16.7	3
4	تنظيم الندوات	3	25	2
5	المشاركة في الدورات التدريبية	6	50	1
مجـ		12	%100	

يتضح من نتائج الجدول السابق أن نسبة العاملين بمؤسسات مكافحة الجريمة المعلوماتية الذين شاركوا في الدورات التدريبية بلغت (50%)، في حين بلغت نسبة من شاركوا في تنظيم الندوات (25%)، يليهم الذين شاركوا في تنظيم ورش العمل بنسبة بلغت (16.7%)، وقد بلغت نسبة الذين قدموا أبحاث علمية نسبة (8.3%)، وقد يرجع ذلك إلى ان مجال الجريمة المعلوماتية يحتاج إلى الدورات التدريبية بشكل كثيف.

جدول رقم (7) يوضح توزيع الخبراء بمؤسسات مكافحة الجريمة المعلوماتية طبقا للذين حصلوا على دورات تدريبية ن= 20

م	حصلت على دورات تدريبية	ك	%	الترتيب
1	نعم	6	30	2
2	لا	14	70	1
مجـ		20	%100	

يتضح من نتائج الجدول السابق أن نسبة العاملين بمؤسسات مكافحة الجريمة المعلوماتية الذين حصلوا على دورات تدريبية بلغت (30%)، في حين أن نسبة الذين لم يحصوا على دورات تدريبية بلغت (70%)، وقد يرجع ذلك إلى إلى المجال حديث العهد ولم تكن تتوافر فيه الدورات التدريبية اللازمة.

جدول رقم (8) يوضح توزيع الخبراء بمؤسسات مكافحة الجريمة المعلوماتية طبقا للدورة التي حصلوا عليها ن= 20

م	اسم الدورة	ك	%	الترتيب
2	دورة ICDL	4	20	1
3	دورة في مجال التنمية البشرية	1	5	2
4	دورة تسجيل البيانات	1	5	2
5	دورة مديرين إدارات الجهاز المركزي للتنظيم والإدارة	1	5	2

يتضح من نتائج الجدول السابق أن نسبة العاملين بمؤسسات مكافحة الجريمة المعلوماتية الذين حصلوا على دورة ICDl بلغت (20%)، يليها الدورات الأخرى بنسبة (5%) لكل دورة بمعدل شخص واحد فقط لكل دورة من الدورات (تسجيل البيانات، التنمية البشرية، دورة مديرين الادارات).

جدول رقم (9) يوضح مستوي الجرائم المعلوماتية التي تُرتكب بشكل كثيف في المجتمع المصري ن= 20

م	العبارات	الاستجابات						مج الأوزان	س-	ع	الترتيب
		نعم		إلى حد ما		لا					
		ك	%	ك	%	ك	%				
1	التحرش الالكتروني من خلال خاصية التعليق على المنشور او من خلال المحادثات على تطبيقات المحادثة المختلفة.	14	70	5	25	1	5	53	2.65	0.59	2
2	انتهاك حقوق الملكية الفكرية من خلال سرقة الأعمال الأدبية.	7	35	9	45	4	20	43	2.15	0.74	8
3	تشويه سمعة الآخرين من خلال السب والقذف وتلفيق مشكلات لهم.	13	65	5	25	2	10	51	2.55	0.68	3
4	الاحتيال والنصب مثل سرقة أرقام البطاقات الائتمانية.	7	35	13	65	-	-	47	2.35	0.48	4
5	انتحال وسرقة هوية الأشخاص من خلال انشاء حسابات مزيفة بأسماء شخصيات عامة او غير عامة على مواقع التواصل الاجتماعي المختلفة.	7	35	10	50	3	15	44	2.20	0.69	5
6	الابتزاز الالكتروني من خلال تهديد الأشخاص بنشر معلوماتهم الشخصية.	15	75	4	20	1	5	54	2.70	0.57	1
7	الإرهاب الالكتروني	8	40	8	40	4	20	44	2.20	0.76	6
8	الاختراق الالكتروني من خلال فتح حسابات شخصية لأفراد محددين بدون علمهم.	10	50	4	20	6	30	44	2.20	0.89	7
	المتوسط الحسابي والانحراف المعياري للبعد ككل								2.37	0.28	مرتفع

توضح نتائج الجدول السابق مستوي الجرائم المعلوماتية التي تُرتكب بشكل كثيف في المجتمع المصري وتمثلت النتائج الواردة فيما يلي: حيث جاء في الترتيب الأول الإبتزاز الالكتروني من خلال تهديد الأشخاص بنشر معلوماتهم الشخصية بمتوسط (2.70)، ثم جاء في الترتيب الثاني التحرش الالكتروني من خلال خاصية التعليق على المنشور او من خلال المحادثات على تطبيقات المحادثة المختلفة بمتوسط (2.65)، وفي الترتيب الثالث تشويه سمعة الآخرين من خلال السب والقذف وتلفيق مشكلات لهم بمتوسط (2.55)، ثم

جاء في الترتيب الرابع الأحتيال والنصب مثل سرقة أرقام البطاقات الإئتمانية بمتوسط (2.35)، وبالترتيب الخامس جاء انتحال وسرقة هوية الأشخاص من خلال انشاء حسابات مزيفة بأسماء شخصيات عامة او غير عامة على مواقع التواصل الاجتماعي المختلفة بمتوسط (2.20)، وبالترتيب السادس جاء الإرهاب الالكتروني بمتوسط (2.20) وانحراف معياري (0.76)، وبالترتيب السابع جاء الاختراق الالكتروني من خلال فتح حسابات شخصية لأفراد محددين بدون علمهم بمتوسط (2.20) وانحراف معياري (0.89)، وجاء بنهاية الترتيب انتهاك حقوق الملكية الفكرية من خلال سرقة الأعمال الأدبية. بمتوسط (2.15)، وفى هذا النطاق أكدت دراسة كساب (٢٠٢٠) أن جريمة النصب والاحتيال على المواطنين في صدارة الجرائم المعلوماتية، كما جاءت جريمة الانتهاك الشخصي لحرمة الحاسب الالي، وجريمة النصب والاحتيال على المواطنين، جريمة الاعتداء على الأموال، جريمة التحريض على ارتكاب أعمال تخريبية بمؤسسات الدولة والارهاب الالكتروني في صدارة جرائم الاعتداءات ضد مؤسسات الدولة.

وبالنظر إلى الجدول السابق نجد نتائجه تشير إلى أن المتوسط العام لمستوي الجرائم المعلوماتية التي تُرتكب بشكل كثيف في المجتمع المصري "مرتفع" حيث بلغ المتوسط الحسابي (2.37) أي أنه يقع في الفئة (3:2.34).

جدول رقم (10) يوضح مستوي الأهداف المادية والاجتماعية للجريمة المعلوماتية ن= 20

م	أهداف	العبارات	الاستجابات						مج الأوزان	س-	ع	الترتيب
			نعم		إلى حد ما		لا					
			ك	%	ك	%	ك	%				
1	مادية	سرقة حسابات بنكية	13	65	5	25	2	10	51	2.55	0.68	1
2		تحقيق المكاسب المالية من خلال النصب على الآخرين.	12	60	8	40	-	-	52	2.60	0.50	2
		المتوسط الحسابي والانحراف المعياري للبعد								2.57	0.43	مرتفع
1	اجتماعية	الوصول إلى معلومات عن جهات حكومية او خاصة.	13	65	6	30	1	5	52	2.60	0.59	1
2		التشهير بأفراد بعينهم بغرض الانتقام منهم.	11	55	6	30	3	15	48	2.40	0.75	2
3		تتبُع معلومات أشخاص بعينهم للوصول إلى معلومات عن حياتهم الشخصية	3	15	13	65	4	20	39	1.95	0.60	3
		المتوسط الحسابي والانحراف المعياري للبعد								2.31	0.35	متوسط
		المستوي العام للأبعاد ككل								2.44		مرتفع

توضح نتائج الجدول السابق مستوي الأهداف المادية والاجتماعية للجريمة المعلوماتية وتمثلت النتائج الواردة فيما يلي:

- بالنسبة للأهداف المادية جاء في الترتيب الأول سرقة حسابات بنكية بمتوسط (2.55)، ثم جاء في الترتيب الثاني تحقيق المكاسب المالية من خلال النصب على الآخرين. بمتوسط (2.60).

وبالنسبة للأهداف الاجتماعية جاء في الترتيب الأول الوصول إلى معلومات عن جهات حكومية او خاصة. بمتوسط (2.60)، ثم جاء في الترتيب الثاني التشهير بافراد بعينهم بغرض الإنتقام منهم. بمتوسط (2.40)، وجاء بنهاية الترتيب تتبُع معلومات أشخاص بعينهم للوصول إلى معلومات عن حياتهم الشخصية بمتوسط (1.95)، وفى هذا النطاق استهدفت دراسة سلطان(٢٠٢١) إلى معرفة أشكال الجرائم الإلكترونية وسمات دوافع مرتكبيها، بالإضافة إلى الكشف عن معدل ودوافع مشاهدة الشباب الجامعي المصري للآمال الدرامية العربية التي تحتوي على جرائم الكترونية، وعما اذا كانت هناك علاقة ارتباط بين معدل مشاهدة تلك الأعمال الدرامية واتجاهات الشباب نحو الجريمة الالكترونية، وقد توصلت الدراسة إلى مجموعة من النتائج أهمها تفوق الذكور مرتكبي الجرائم الالكترونية، كما أظهرت الدراسة ان النسبة الأكبر من الشباب في عينة الدراسة لديهم مواقف محايدة تجاه الجرائم الالكترونية.

وبالنظر إلى الجدول السابق نجد نتائجه تشير إلى أن المتوسط العام لمستوي الأهداف المادية والاجتماعية للجريمة المعلوماتية "مرتفع" حيث بلغ المتوسط الحسابي (2.44) أي أنه يقع في الفئة (3:2.34).

جدول رقم (11) يوضح مستوي أداء منظمات مكافحة الجريمة المعلوماتية ن= 20

م	العبارات	الاستجابات						مج الأوزان	س-	ع	الترتيب
		نعم		إلى حد ما		لا					
		ك	%	ك	%	ك	%				
1	عقد دورات تدريبية للعاملين حول مكافحة الجريمة المعلوماتية.	15	75	4	20	1	5	54	2.70	0.57	1
2	تسهيل إجراءات الإبلاغ عن الجرائم المعلوماتية على الجمهور.	12	60	7	35	1	5	51	2.55	0.60	2
3	عقد ندو ات تثقيفية للجمهور بأحدث طرق ارتكاب الجريمة المعلوماتية للوقاية منها.	10	50	7	35	3	15	47	2.35	0.74	4

م	العبارات	الاستجابات						مج الأوزان	س-	ع	الترتيب
		نعم		إلى حد ما		لا					
		ك	%	ك	%	ك	%				
4	توعية الجمهور عن عدم إفشاء معلوماتهم وصورهم الشخصية على مواقع التواصل الاجتماعي مع شخصيات غير معروفة واقعيًا.	11	55	8	40	1	5	50	2.50	0.60	3
5	توعية الجمهور بعدم الاحتفاظ على بيانات شخصية على الجوال او جهاز الحاسوب.	6	30	12	60	2	10	44	2.20	0.61	5
المتوسط الحسابي والانحراف المعياري للبعد ككل									2.46	0.35	مرتفع

توضح نتائج الجدول السابق مستوي جهود الوقاية من الجرائم المعلوماتية وتمثلت النتائج الواردة فيما يلي: جاء في الترتيب الأول عقد دورات تدريبية للعاملين حول مكافحة الجريمة المعلوماتية بمتوسط (2.70)، ثم جاء في الترتيب الثاني تسهيل إجراءات الإبلاغ عن الجرائم المعلوماتية على الجمهور بمتوسط (2.55)، وفي الترتيب الثالث توعية الجمهور عن عدم إفشاء معلوماتهم وصورهم الشخصية على مواقع التواصل الاجتماعي مع شخصيات غير معروفة واقعيًا بمتوسط (2.50)، ثم جاء في الترتيب الرابع عقد ندوات تثقيفية للجمهور بأحدث طرق ارتكاب الجريمة المعلوماتية للوقاية منها بمتوسط (2.35)، وجاء بنهاية الترتيب توعية الجمهور بعدم الاحتفاظ على بيانات شخصية على الجوال او جهاز الحاسوب بمتوسط (2.20). وبالنظر إلى الجدول السابق نجد نتائجه تشير إلى أن المتوسط العام لمستوي آليات الوقاية من الجرائم المعلوماتية "مرتفع" حيث بلغ المتوسط الحسابي (2.46) أي أنه يقع في الفئة (3:2.34)، وفى هذا النطاق سعت دراسة (حميد، ٢٠١٩): لوضع رؤية استراتيجية لمكافحة الجرائم السيبرية، باستخدام الاستبيان كاداه لجمع البيانات، باستخدام المنهج الوصفي والتحليلي، 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.

جدول رقم (12) يوضح جهود المنظمات في تحقيق الأمن السيبراني وفقًا للبعد التقني ن= 20

م	العبارات	الاستجابات						مج الأوزان	س-	ع	الترتيب
		نعم		إلى حد ما		لا					
		ك	%	ك	%	ك	%				
1	حماية المعلومات والبيانات لدى الجهات المختلفة.	17	85	3	15	-	-	57	2.85	0.36	1
2	تأمين البنية التحتية للاتصالات والمعلومات بشكل متكامل.	8	40	12	60	-	-	48	2.40	0.50	3
3	توفير البيئة الآمنة لتقديم الخدمات الإلكترونية المتكاملة.	10	50	8	40	2	10	48	2.40	0.68	4
4	مكافحة الإرهاب السيبرانى والذي يستهدف التخريب والإرهاب.	12	60	8	40	-	-	52	2.60	0.50	2
5	مواجهة الحروب السيبرانية والتي تتعلق بحملات التخريب وتعطيل الإنترنت.	8	40	11	55	1	5	47	2.35	0.58	5
6	مكافحة التجسس الالكتروني والتي يتم فيها الحصول على معلومات سرية بطرق غير مشروعة.	9	45	9	45	2	10	47	2.35	0.67	6
7	مواجهة الجرائم التي تحتاج إلى وجود الأمن السيبرانى مثل تهريب المخدرات وغسيل الأموال.	7	35	10	50	3	15	44	2.20	0.69	8
8	تبادل الخبرات بين خبراء حماية البيانات والأمن السيبراني .	6	30	13	65	1	5	45	2.25	0.55	7
9	التعامل مع التهديدات الرقمية الناشئة، والتي تسبب في اختراقات للأنظمة وتسريب للبيانات على حد سواء .	3	15	15	75	2	10	41	2.05	0.51	9
	المتوسط الحسابي والانحراف المعياري للبعد ككل								2.38	0.22	مرتفع

توضح نتائج الجدول السابق مستوي جهود المنظمات في تحقيق الأمن السيبراني وفقا للبعد التقني وتمثلت النتائج الواردة فيما يلي: حيث جاء في الترتيب الأول حماية المعلومات والبيانات لدى الجهات المختلفة بمتوسط (2.85)، ثم جاء في الترتيب الثاني مكافحة الأرهاب السيبرانى والذى يستهدف التخريب والإرهاب بمتوسط (2.60)، وفي الترتيب الثالث تأمين البنية التحتية للأتصالات والمعلومات بشكل متكامل بمتوسط (2.40) بانحراف معياري (0.50)، ثم جاء في الترتيب الرابع توفير البيئة الآمنة لتقديم الخدمات الألكترونية المتكاملة بمتوسط (2.40) وانحراف معياري (0.68)، وجاء بنهاية الترتيب التعامل مع التهديدات الرقمية الناشئة، والتي تسبب في اختراقات للأنظمة وتسريب للبيانات على حد سواء بمتوسط (2.05)، وفى هذا النطاق سعت دراسة (الشهري،

٢٠١٩): لوضع رؤية استراتيجية للحد من الجرائم الالكترونية لتعزيز الأمن السيبراني، ومن خلال التعرف على طبيعة تلك الجرائم وأسبابها والوقوف على التهديدات والمخاطر التي تعترض الأمن السيبراني، باستخدام المنهج الوصفي، وبالاعتماد على أداتي الاستبيان و S.W.O.T كأدوات لجمع البيانات، وتوصلت الدراسة إلى عدة نتائج لعل من أبرزها : الجرائم الالكترونية التي لا تعترف بأي حدود مكانية أو زمانية، وأن التقنيات الحديثة وفرت فرصًا غير مسبوقة لانتشارها، وأن انتهاك السياسيات الأمنية الخاصة بالأمن السيبراني تمثل أهم التهديدات التي تواجه الفضاء السيبراني، وتمثلت ملامح الرؤي المقترحة في تطبيقات التشريعات والأنظمة في مواجهة تلك الجرائم من خلال انشاء المزيد من المحاكم المختصة، تطوير التقنيات الحالية لرفع كفاءة رصد تلك الجرائم وملاحقتها، تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم الالكترونية والأمن السيبراني.

وبالنظر إلى الجدول السابق نجد نتائجه تشير إلى أن المتوسط العام لمستوي جهود المنظمات في تحقيق الأمن السيبراني وفقا للبعد التقني "مرتفع" حيث بلغ المتوسط الحسابي (2.38) أي أنه يقع في الفئة (3:2.34).

جدول رقم (13) يوضح جهود المنظمات في تحقيق الأمن السيبراني وفقًا للبعد الاداري ن= 20

م	العبارات	الاستجابات						مج الأوزان	س-	ع	الترتيب
		نعم		إلى حد ما		لا					
		ك	%	ك	%	ك	%				
1	اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.	14	70	5	25	1	5	53	2.65	0.58	1
2	تحسين قدرة المؤسسة على الامتثال للقوانين واللوائح والمعايير التي تخص كلا من الأمن السيبراني وحماية البيانات .	8	40	11	55	1	5	47	2.35	0.58	2
3	التنسيق بين وزارة الداخلية ووزارة الاتصالات وتكنولوجيا المعلومات في مجال الأمن السيبراني.	9	45	9	45	2	10	47	2.35	0.67	3
	المتوسط الحسابي والانحراف المعياري للبعد ككل								2.45	0.44	مرتفع

توضح نتائج الجدول السابق مستوي جهود المنظمات في تحقيق الأمن السيبراني وفقا للبعد الاداري وتمثلت النتائج الواردة فيما يلي: جاء في الترتيب الأول اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة بمتوسط (2.65)، ثم جاء في الترتيب الثاني تحسين قدرة المؤسسة على الامتثال للقوانين واللوائح والمعايير التي تخص كلا من الأمن السيبراني وحماية البيانات بمتوسط (2.35) وانحراف معياري (0.58)، وفي الترتيب الثالث التنسيق بين وزارة الداخلية ووزارة الاتصالات وتكنولوجيا المعلومات في مجال الأمن السيبراني بمتوسط (2.35) وانحراف (0.67). **وبالنظر إلى الجدول السابق نجد نتائجه تشير إلى أن المتوسط العام لمستوي جهود المنظمات في تحقيق الأمن السيبراني وفقا للبعد الاداري "مرتفع" حيث بلغ المتوسط الحسابي (2.45) أي أنه يقع في الفئة (3:2.34)، وهذا ما أكدته نظرية المنظمات واستفادت منه الباحثة وهو تحديد احتياجات ومتطلبات منظمات مكافحة الجريمة المعلوماتية في تحقيق أهدافها.**

جدول رقم (14) يوضح جهود المنظمات في تحقيق الأمن السيبراني وفقا للبعد التمويلي ن= 20

م	العبارات	الاستجابات						مج الأوزان	س-	ع	الترتيب
		نعم		إلى حد ما		لا					
		ك	%	ك	%	ك	%				
1	توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.	10	50	10	50	-	-	50	2.50	0.51	2
2	توفير الأجهزة الحديثة المزودة بأحدث التقنيات لمواجهة خطر الجريمة المعلوماتية.	7	35	12	60	1	5	46	2.30	0.57	3
3	توفير الإمكانيات لجميع الكوادر البشرية العاملة في مجال الأمن السيبراني.	13	65	7	35	-	-	53	2.65	0.48	1
	المتوسط الحسابي والانحراف المعياري للبعد ككل								2.48	0.41	مرتفع

توضح نتائج الجدول السابق مستوي جهود المنظمات في تحقيق الأمن السيبراني وفقا للبعد التمويلي وتمثلت النتائج الواردة فيما يلي: جاء في الترتيب الأول توفير الإمكانيات لجميع الكوادر البشرية العاملة في مجال الأمن السيبراني بمتوسط (2.65)، ثم

جاء في الترتيب الثاني توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين بمتوسط (2.50)، وفي الترتيب الثالث توفير الأجهزة الحديثة المزودة بأحدث التقنيات لمواجهة خطر الجريمة المعلوماتية بمتوسط (2.30). **وبالنظر إلى الجدول السابق نجد نتائجه تشير إلى أن المتوسط العام لمستوي جهود المنظمات في تحقيق الأمن السيبراني وفقا للبعد التمويلي "مرتفع" حيث بلغ المتوسط الحسابي (2.48) أي أنه يقع في الفئة (3:2.34).**

أثبتت نتائج الدراسة عدم صحة الفرض الثالث وذلك لأن النتائج تشير إلى أن المتوسط العام لمستوي جهود المنظمات في تحقيق الأمن السيبراني مرتفع وذلك يأتي وفقا لكلا المؤشرات (التقنية والإدارية والتمويلية).

جدول رقم (15) يوضح مستوي متطلبات تحقيق الأمن السيبراني في المجتمع المصري ن= 20

م	المتطلبات	العبارات	الاستجابات						مج الأوزان	س-	ع	الترتيب
			نعم		إلى حد ما		لا					
			ك	%	ك	%	ك	%				
1	العاملين	عقد الدورات التدريبية للعاملين في مكافحة الجريمة المعلوماتية.	15	75	5	25	-	-	55	2.75	0.44	1
2		تنمية مهارات العاملين في مجال مكافحة الجريمة السيبرية	15	75	4	20	1	5	54	2.70	0.57	2
3		متابعة أحداث الأساليب التكنولوجية وتطورات مواقع التواصل الاجتماعي.	11	55	8	40	1	5	50	2.50	0.60	3
المتوسط الحسابي والانحراف المعياري للبعد										2.65	0.41	مرتفع
1	التمويلية	العمل على زيادة الموارد المالية لمواجهة الجرائم المعلوماتية.	15	75	4	20	1	5	54	2.70	0.57	1
2		تطوير أجهزة الحاسوب والأجهزة المستخدمة في رصد وتتبع الجرائم.	10	50	8	40	2	10	48	2.40	0.68	2
3		الاستعانة بالخبراء الأكاديمين في مجال الجرائم السيبرية.	12	60	4	20	4	20	48	2.40	0.82	3
المتوسط الحسابي والانحراف المعياري للبعد										2.50	0.59	مرتفع
1	المجتمعية	توعية المواطنون بضرورة الإبلاغ على الجرائم التي تُرتكب في حقهم.	18	90	1	5	1	5	57	2.85	0.48	1

م	المتطلبات	العبارات	الاستجابات						مج الأوزان	س-	ع	الترتيب
			نعم		إلى حد ما		لا					
			ك	%	ك	%	ك	%				
2		التشبيك بين مؤسسات المجتمع الحكومية والأهلية لتنفيذ ندوات لتوعية المواطنون بحقوقهم الشخصية.	12	60	8	40	-	-	52	2.60	0.50	2
3		توعية الشباب في الجامعات والمدارس بمخاطر الجريمة السيبرية.	13	65	6	30	1	5	52	2.60	0.59	3
المتوسط الحسابي والانحراف المعياري للبعد									52	2.60	0.36	مرتفع
1	التشريعية	تعديل التشريعات القانونية بما يتناسب مع سرعة التقدم التكنولوجي الهائل في مجال الجريمة المعلوماتية.	17	85	3	15	-	-	57	2.85	0.36	1
2		تسهيل الإجراءات القانونية ليتمكنوا الضحايا من الحصول على حقوقهم.	13	65	6	30	1	5	52	2.60	0.59	2
المتوسط الحسابي والانحراف المعياري للبعد									52	2.72	0.41	مرتفع
المتوسط الحسابي والمستوي العام للأبعاد ككل										2.64		مرتفع

توضح نتائج الجدول السابق مستوي متطلبات تحقيق الأمن السيبراني في المجتمع المصري وقد جاءت النتائج كالتالي:

- أوضحت النتائج الواردة الخاصة بالمتطلبات الخاصة بالعاملين: أنه جاء في الترتيب الأول عقد الدورات التدريبية للعاملين في مكافحة الجريمة المعلوماتية بمتوسط (2.75)، ثم جاء في الترتيب الثاني تنمية مهارات العاملين في مجال مكافحة الجريمة السيبرية بتغيراتها بمتوسط (2.70)، وفي الترتيب الثالث متابعة أحداث الأساليب التكنولوجية وتطورات مواقع التواصل الاجتماعي بمتوسط (2.50)، وكان المستوي العام للبعد "مرتفع" بمتوسط حسابي (2.65).
- أظهرت النتائج الواردة الخاصة بالمتطلبات التمويلية: أنه جاء في الترتيب الأول العمل على زيادة الموارد المالية لمواجهة الجرائم المعلوماتية بمتوسط (2.70)، ثم جاء في الترتيب تطوير أجهزة الحاسوب والأجهزة المستخدمة في رصد وتتبع الجرائم بمتوسط (2.40) وانحراف معياري (0.68)، وفي الترتيب الثالث الاستعانة بالخبراء الأكاديمين في مجال الجرائم السيبرية بمتوسط (2.40) وانحراف معياري (0.82) وكان المستوي العام للبعد "مرتفع" بمتوسط حسابي (2.50).

- أوضحت النتائج الواردة الخاصة بالمتطلبات المجتمعية: أنه جاء في الترتيب الأول توعية المواطنون بضرورة الإبلاغ على الجرائم التي تُرتكب في حقهم بمتوسط (2.85)، ثم جاء في الترتيب الثاني التشبيك بين مؤسسات المجتمع الحكومية والأهلية لتنفيذ ندوات لتوعية المواطنون بحقوقهم الشخصية بمتوسط (2.60) وانحراف معياري (0.50)، وفي الترتيب الثالث توعية الشباب في الجامعات والمدارس بمخاطر الجريمة السيبرية بمتوسط (2.60) وانحراف معياري (0.59) وكان المستوي العام للبعد "مرتفع" بمتوسط حسابي (2.68).
- أوضحت النتائج الواردة الخاصة بالمتطلبات التشريعية: أنه جاء في الترتيب الأول تعديل التشريعات القانونية بما يتناسب مع سرعة التقدم التكنولوجي الهائل في مجال الجريمة المعلوماتية بمتوسط (2.85)، ثم جاء في الترتيب الثاني تسهيل الإجراءات القانونية ليتمكنوا الضحايا من الحصول على حقوقهم بمتوسط (2.60) وكان المستوي العام للبعد "مرتفع" بمتوسط حسابي (2.72).

وبالنظر إلى الجدول السابق نجد نتائجه تشير إلى أن المتوسط العام لمستوي متطلبات تحقيق الأمن السيبراني في المجتمع المصري والتي تحددت في المتطلبات (الخاصة بالعاملين، المتطلبات التمويلية، المتطلبات المجتمعية، المتطلبات التشريعية) "مرتفع" حيث بلغ المتوسط الحسابي (2.64) أي أنه يقع في الفئة (3:2.34)، وهذا ما استفادت منه الباحثة فى نظرية المنظمات وهى ضرورة تحديد المتطلبات التقنية، الإدارية والتمويلية.

توصيات:

1) عقد مؤتمرات دولية تستهدف تحديد الجرائم المعلوماتية الأكثر ارتكابًا على المستوى الدولي والمحلى.
2) توعية الشباب والجمهور بأهم البرامج والسُبل والآليات التى من خلالها يمكن الحفاظ على سرية المعلومات.
3) توعية الشباب والجمهور بالنتائج المترتبة على ارتكاب الجريمة المعلوماتية والعقوبات التى نص عليها القانون.

4) تنمية وعى الجمهور بضرورة الإبلاغ عن الجريمة المعلوماتية وعدم الخوف او الخجل او الحرج من الإبلاغ كما فى جرائم التحرش الإلكتروني والابتزاز الإلكتروني.
5) استخدام الوسائل الإعلامية فى توعية الجمهور بالتدابير التى لابد من اتخاذها فى حالة التعرض لأي شكل من أشكال الجريمة المعلوماتية.
6) تخطيط سياسات على المستوى الدولي تشمل عقوبات صارمة على مرتكبي الجرائم المعلوماتية نظرًا لمخاطر الجريمة المعلوماتية.
7) الاعتماد على أساليب وتقنيات متطورة ومواكبة أخر التطورات بشكل يومي لسرعة اكتشاف مرتكب الجريمة.
8) تنمية وعر الأفراد بخطورة الجريمة الالكترونية، والحفاظ على معلوماتهم السرية مثل الحسابات البنكية والرقم القومي وغيرها.
9) الحفاظ على كلمة السر واختيارها بشكل معقد، عدم حفظ الصور والبيانات الشخصية على الهواتف المحمولة وعلى مواقع التواصل الإجتماعى.
10) سرعة إبلاغ الجهات الأمنية عن الجريمة المعلوماتية مع استيفاء جميع البيانات والمعلومات التى تسهل الوصول إلى مرتكب الجريمة.
11) عدم النقر على أى روابط على الانترنت تحسبًا من الاختراق الإلكتروني.
12) تحديث برامج الحماية الخاصة بأجهزة الحاسوب.
13) حماية أجهزة الحاسوب والموبايلات بكلمات سرية معقدة.
14) عدم ترك الأجهزة الشخصية (لاب توب- موبايل – تابلت – اى باد) فى حيازة أى شخص مهما كانت درجة الثقة فى أى شخص.
15) أجهزة الحاسوب الخاصة بالشركات لابد من سرية المعلومات الخاصة بالعمل عليها.
16) الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب.
17) فصل الحاسوب عن الانترنت فى حالة عدم الحاجة إليه.
18) تغيير كلمة المرور الخاصة بالحسابات الخاصة بك كل فترة، ولا تترك معلوماتك الشخصية متاحة للجميع.

مراجع البحث:

إبراهيم، خالد (٢٠٠٨). أمن الجريمة الالكترونية، القاهرة، الدار المصرية اللبنانية للطباعة والنشر والتوزيع، الطبعة (١).
ابن داوود، عبد العزيز (٢٠٢٠). الجرائم السيبرانية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المملكة العربية السعودية، المجلد (٩)، العدد (٣).
احسان، شيرين (٢٠١٦). العلاقة بين جهود منظمات مكافحة الجرائم الالكترونية وتحقيق الامن الاجتماعي، أطروحة دكتوراه غير منشورة، كلية الخدمة الاجتماعية، جامعة حلوان.
اسكندر، ماجد عزيز (٢٠٢٠). تهديدات الفضاء السيبراني للأمن القومي، رسالة ماجستير غير منشورة، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.
إسماعيل، محمد (٢٠٢٢). الجريمة الالكترونية، عبر الموقع الالكتروني بتاريخ ١-٧، في الساعة ٣:٣٥م، تم الاطلاع عليها في يوم الخميس ٢-٢-٢٠٢٣، في الساعة ٣:٢٢ص.
أشرف، حسن (٢٠١٥). الجريمة المعلوماتية أو الإلكترونية: أنواعها وخصائصها وطرق الوقاية منها، الأكاديمية العربية للعلوم المالية والمصرفية – مركز البحوث المالية والمصرفية.
البداينة، ذياب (٢٠٠٦). دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي، عمان الدورة التدريبية لمكافحة الجرائم الإرهابية المعلوماتية، المنعقدة بكلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية.
البداينة، ذياب (٢٠١٤). الجرائم الإلكترونية المفهوم والأسباب، عمان، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية.
الحق، محمد (٢٠١٩). رؤية استراتيجية لمكافحة الجرائم السيبرانية، المجلة العربية الدولية للمعلوماتية، المجل د7، العدد (١٢).
الحمامي، عمر (٢٠١٠). الحماية الجنائية للمعلومات، القاهرة، دار النهضة العربية.
الحوامدة، لورنس (٢٠١٧). الجرائم المعلوماتية أركانها وآلية مكافحتها: دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد 4، العدد(١).
الدريبي، عبد العال(٢٠١٣). الجريمة المعلوماتية تعريفها أسبابها وخصائصها، طرابلس، مقال منشور بالمركز العربي لأبحاث الفضاء الإلكتروني، بتاريخ ١٣-١.
الدورة التثقيفية لأكاديمية ناصر العسكرية العُليا للدراسات، (٢٠٢١) القاهرة، الاستراتيجية والامن القومي، الدورة رقم (٦٨).
الربيعة، صالح (٢٠١٨). الأمن الرقمي وحماية المستخدم من مخاطر الانترنت، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية.
الشهري، على(٢٠١٩). رؤية استراتيجية للحد من الجرائم الالكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة دكتوراه غير منشورة، جامعة نايف العربية للعلوم الأمنية: كلية العلوم الاستراتيجية.
الشوا، محمد (١٩٩٤). ثورة المعلومات وانعكاسها على قانون العقوبات، دار النهضة العربية، القاهرة.
العادلي، محمد (٢٠٠٦). الجرائم المعلوماتية (ماهيتها وصورها)، مسقط، ورشة عمل إقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية.
العبيدي، صدام،(٢٠١٩). جرائم الأنترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية، كتاب رقمي، www.almanhal.com
القهوجي، علي (٢٠١٩). الحماية الجنائية لبرامج الحاسب الألي، بيروت، الطبعة الاولي، الدار الجامعية.
الكعبي، محمد (٢٠٠٩). الجرائم الناشئة عن استخدام الغير مشروع لشبكة الانترنت، القاهرة، دار النهضة العربية، الطبعة الثانية.
النبهان، محمد (١٩٨٩). مكافحة الإجرام المنظم، جامعة نايف العربية للعلوم العربية والأمنية. https://almerja.com/reading.php?idm=178023
بطيخ، حاتم (٢٠٢١). تطور السياسة التشريعية فى مجال مكافحة جرائم تقني المعلومات، القاهرة، جامعة عين شمس.
تقرير الاتحاد الدولي للاتصالات، 2022، https://www.itu.int/itu-d/sites/statistics/ar/

جابر، ضرغام (٢٠١٧). جريمة التجسس المعلوماتي "دراسة مقارنة"، جمهورية مصر العربية، المركز العربي للدراسات والبحوث العلمية.
حسن، خالد (٢٠١٩). الدليل الرقمي ودوره في اثبات الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية.
حمد، بن عبد الله (٢٠١٧). تقنيات التعليم ومهارات الاتصال، الرياض، روابط للنشر وتقنية المعلومات.
رستم، هشام (١٩٩٩). الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي، كلية الشرطة، العدد (٢).
رياض حمدوش (٢٠٠٨). تطور مفهوم الأمن والدراسات الأمنية في منظورات العلاقات الدولية، بحث منشور، الملتقي الدولي الجزائر والأمن – واقع وآفاق، جامعة منتوري، قسم العلوم السياسية، قسطنطينية، الجزائر.
سلطان، أحمد (٢٠٢١). العلاقة بين تعرض الشباب الجامعي المصري للدراما العربية واتجاهاتهم نحو الجريمة الالكترونية، رسالة ماجستير غير منشورة، كلية الاعلام، قسم الإذاعة والتليفزيون، جامعة القاهرة.
شتا، السيد (٢٠٠٤). الانحراف الاجتماعي الانماط والتكلفة، الإسكندرية، المكتبة المصرية للطباعة والنشر والتوزيع.
شوارب، اميرة (٢٠١٨). إدراك الجمهور المصري لجرائم الانترنت وعلاقته باستراتيجيات مواجهتها، رسالة ماجستير غير منشورة، قسم الصحافة، جامعة القاهرة.
صابر، محمد، الإدارة العامة لتكنولوجيا المعلومات، في الساعة ١٢:١٤.
صادق، نبيل (١٩٩٨). طريقة تنظيم المجتمع في الخدمة الاجتماعية، القاهرة، دار الثقافة للطباعة والنشر.
عبد الله، عبد العزيز (٢٠١١). التفتيش في الجرائم المعلوماتية، تخصص السياسة الجنائية، كلية الدراسات العُليا، جامعة نايف العربية للعلوم الأمنية.
عفيفي، هند (٢٠٢٢). الأثار الاجتماعية للقرصنة الالكترونية، أطروحة دكتوراه غير منشورة، كلية الآداب، قسم اجتماع، جامعة عين شمس.
على، علي (٢٠٢٠). الصراع والامن الجيوسيبراني في الساحة الدولية، دراسة في استراتيجيات الاشتباك الرقمي، عمان، دار أمجد للنشر والتوزيع.
عمر، ممدوح (٢٠٠٨). حماية الحياة الخاصة والقانون الجنائي، القاهرة، دار النهضة العربية، القاهرة.
قرار وزير الداخلية المصري(٢٠٠٢). الرقيم ١٣٥٠٧ بشأن إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للإدارة العامة للمعلومات والتوثيق، القاهرة.
كساب، أحمد (٢٠٢٠). التغطية الصحفية الالكترونية للجرائم المعلوماتية وعلاقتها باستخدام الشباب المصري لشبكة الانترنت، رسالة ماجستير غير منشورة، كلية الاعلام، قسم الصحافة، جامعة القاهرة.
محمد، أميمة (٢٠١٩)، الوعي المجتمعي بالجرائم المعلوماتية لدى الطالبة الجامعية من منظور طريقة تنظيم المجتمع في الخدمة الاجتماعية، مجلة كلية الخدمة الاجتماعية، الجمعية المصرية للأخصائيين الاجتماعيين، العدد (٦١)، المجلد (٣).
محمد، ايناس (٢٠٢١). دور الأمن السيبراني في مواجهة الإرهاب الالكتروني، بحوث ومقالات، مجلة العلوم القانونية والاقتصادية، المجلد (٦٤)، العدد (١) يوليو، كلية الحقوق، جامعة عين شمس.
منجود، هالة، التخطيط لتنمية وعى الشباب الجامعي بمخاطر الجرائم الالكترونية، المقالة (٤)، المجلد (٦٠)، العدد (٢)، مجلة كلية الخدمة الاجتماعية، جامعة حلوان.
ناصيف، على (٢٠١٧)، ممارسة برنامج مقترح من منظور خدمة الجماعة لتنمية وعى الشباب بمخاطر الجريمة الالكترونية، مجلة كلية الخدمة الاجتماعية، العدد (٥٨)، مجلد (٣)، ٢٠١٧.
يوسف، صغير(٢٠١٣). الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير غير منشورة، تخصص القانون الدولي والأعمال، كلية الحقوق والعلوم السياسية https://www.vetogate.com/4889668
Criminality contract electronic IN; Le contract .Cornine, Mascala (2000) journees , Henri electronique, Travaux de l'association CAPITANT national paris.
Elnaim, Bushra (2013). Cybercrime in kingdom of Saudi Arabic: The Threat To day and the Expected Future Article in journal of information & Knowledge Management. January, Vol.3 No. 12,

e – Crime solutions and crime displacement .G Smith, Russell,(2003) Australian institute of criminology, Canberra Act, ,.

Computer crime and computer fraud: University of .Kunz, Michael,(2004) Mary land, -.

Organization for Social Change (Oxford, University .Martin, Rein (2015) Press,).

Fouad, Noran Shafik (2021) Securing higher education against cyber threats; from an institutional risk to a national policy challenge, Journal of cyber policy 6;2 137-154