المعلومات بين المخاطر وارتكاب الجرائم في البيئة الرقمية

إعداد

محمود عبدالمنعم السيد أحمد قورة

mgoura٠@gmail.com

باحث دكتوراه بقسم المكتبات والمعلومات

كلية الآداب – جامعة طنطا

إشراف

أ.د/ أحمد عبادة العربي

أستاذ المكتبات والمعلومات بكلية الآداب جامعة طنطا

د/ هبة صلاح الدين النموري

مدرس المكتبات والمعلومات بكلية الآداب جامعة طنطا

٢٠٢٤

المستخلص:
إن للتطورات التكنولوجية أثر كبير في جميع المجالات وخاصة في مجال المعلومات، حيث ساعدت التكنولوجيا علي حفظ ونشر المعلومات بشكل أيسر وأسرع من النظام التقليدي، ومع ظهور تلك التطورات ظهرت العديد من الأدوات والدوافع التي تهدد أمن المعلومات وتسعي علي الحصول علي المعلومات بالطرق غير الشرعية حيث عرفت بالجرائم المعلوماتية.

ولذا هدفت الدراسة إلي التعرف علي الجريمة المعلوماتية وأهم أنواعها، والأدوات المستخدمة لارتكابها، والخصائص التي تميزها عن غيرها من الجرائم التقليدية، فضلاً عن التعرف علي نظم مكافحة الجريمة المعلوماتية، وأهم الهيئات المختصة لمكافحتها، مع وضع الحلول للحد من الجريمة المعلوماتية ومخاطرها.

اعتمدت الدراسة علي المنهج الوصفي التحليلي الذي يسعي إلي حل المشكلات وتقديم مجموعة من الحلول المبتكره لها، وتوصلت الدراسة إلي العديد من النتائج أهمها:

ضرورة حماية البنية التحتية المصرية عن طريق التدريب المستمر للكوادر المتخصصة في مكافحة وملاحقة المجرمين مع إنشاء نظم معلومات أخري تحتوي علي أعلي درجات الأمان، ويجب توفير الأمن والحماية للأدوات المعلوماتية عن طريق إعداد النسخ الاحتياطية وحفظها في أماكن أخري آمنة مع إعداد الخطط اللازمة لمواجهة الأزمات المفاجأة التي قد تخل بالنظام المعلوماتي، وضرورة التعاون الدولي لوضع نظام فعال يمكن من خلاله تبادل الخبرات بين المتخصصين ووضع آليات للحد من الجريمة المعلوماتية ومخاطرها الدولية التي تجتاح الدول، كما يجب وضع مجموعة من المسابقات التنافسية للمواهب التي لديها إمكانات تقنية عالية والتي تهدف إلي تخصيص جوائز قيمة لأكثر المواهب التي تضع نظام آمن أو برامج لحماية الأنظمة التي تم اختراقها علي أيدي مجرمين.

التمهيد:

تعتبر المعلومات هي الأداة الرئيسية للجريمة المعلوماتية، فقبل أن يفكر المجرم المعلوماتي في جريمته فإنه يعمل علي جمع أكبر قدر ممكن من المعلومات حول النظام الذي يستهدفه، وذلك باستخداك الحواسب الآلية التي تعتبر الوسيلة التي يقوم المجرم المعلوماتي بتنفيذ جريمته من خلالها، الأمر الذي يتطلب استخدام شبكة الانترنت التي تعد النواة التي يعتمد عليها المجرم المعلوماتي في إرسال أو جمع المعلومات عن النظام المستهدف سواء كان شخص أو جه أو هيئة.

مشكلة الدراسة:

لقد كان للتطور التكنولوجي أثراً واضحاً في زيادة عدد المستخدمين للتكنولوجيا والأجهزة الحديثة مما جعل الأشخاص والهيئات والمؤسسات تحتفظ بمعلوماتها عبر أجهزة الحاسوب، حيث ثمة علاقة قوية بين استخدام الحواسب الآلية وارتكاب بعض الجرائم المعلوماتية الإلكترونية التي تهدد تلك المؤسسات التي من المحتمل أن تأخذ الحذر وتحافظ علي أمن واستقرار المعلومات أو العكس، إذا فإن الحاسوب هو المحور الرئيسي والأساسي للجريمة المعلوماتية سواء كان محلاً للجريمة المعلوماتية أو مجرد وسيلة لها.
لذا ظهرت الحاجه الماسة إلي التعرف علي المخاطر التي تهدد أمن المعلومات وارتكاب الجرائم المعلوماتية في البيئة الرقمية، والتعرف علي أهم الدوافع والأدوات التي تساعد المجرم المعلوماتي علي تنفيذ جريمته، والعمل علي الحد منها وتوفير بعض النتائج التي تساعد المؤسسات المعلوماتية في الحفاظ علي أمن وسلامة معلوماتها.

أهمية الدراسة:

تستهدف الجريمة المعلوماتية المعلومات بشكل رئيسي، حيث أن المجتمع المعلوماتي لا يعترف بحدود زمانية أو مكانية، فهو مجتمع منفتح عبر شبكات تخترق المكان والزمان، وهنا تظهر أهمية الدراسة في استيعاب هذا النوع من المخاطر المستحدثة والعمل علي الحد منها داخل المؤسسات والهيئات المعلوماتية وزيادة الوعي للمستخدمين للحواسب الآلية مع أخذ الحيطة والحذر ، وإدراكهم للمخاطر التي من الممكن أن تحط بهم.

أهداف الدراسة:

تسعي الدراسة إلي تحقيق الأهداف التالية:

١- رصد الجريمة المعلوماتية وأنواعها وخصائصها.
٢- إبراز أدوات ارتكاب الجريمة المعلوماتية.
٣- رصد نظم مكافحة الجريمة المعلوماتية.
٤- التعرف علي أهم الهيئات المختصة لمكافحة الجريمة المعلوماتية.
٥- وضع الحلول للحد من الجريمة المعلوماتية.

تساؤلات الدراسة:

في ضوء الأهداف السابقة تسعي الدراسة للإجابة عن التساؤلات التالية:

١- ما هي الجريمة المعلوماتية وأنواعها وأهم خصائصها؟
٢- ما الأدوات المستخدمة في ارتكاب الجريمة المعلوماتية؟
٣- ما نظم مكافحة الجرائم المعلوماتية؟
٤- ما أهم الهيئات المختصة لمكافحة الجريمة المعلوماتية؟
٥- ما الحلول المقترحة للحد من الجرائم المعلوماتية؟

حدود الدراسة:

- **الحدود الموضوعية:**

تسعي الدراسة إلي التعرف علي المخاطر التي تهدد أمن المعلومات وارتكاب الجرائم المعلوماتية الإلكترونية في البيئة الرقمية.

- **الحدود الزمنية:**

تجري الدراسة في عام ٢٠٢٤م.

منهج الدراسة:

المنهج الوصفي التحليلي:

سوف يتم من خلال هذا المنهج تحديد ماهية الجريمة المعلوماتية في البيئة الرقمية وأهم الدوافع والأدوات المستخدمة في ارتكاب تلك الجريمة، فضلا عن التعرف علي النظم والهيئات المختصة في مكافحة تلك الجرائم، وأفضل الوسائل والحلول للحد منها.

مصطلحات الدراسة:

١- الجريمة المعلوماتية:

هو فعل أو تصرف إجرامي يقوم المجرم المعلوماتي باستخدام الحاسب الآلي كأداة رئيسية لارتكاب جريمته.
أو التصرف الغير مشروع الذي يرتكب من خلال الحواسيب. **(وردة، ٢٠١٨)**

٢- البيئة الرقمية:

هي المجتمع اللاورقي أو الرقمي والذي أثر بشكل جذري علي هوية وقيمة المعلومات.
أو هي استخدام التقنيات والتكنولوجيا الحديثة في إنجاز المهام والأنشطة المختلفة. **(طرفي،٢٠١٢)**

أولاً: مفهوم الجريمة المعلوماتية:

إن للجريمة المعلوماتية مسميات عديدة منها (جرائم الحاسب الآلي ـ الجرائم المستحدثة ـ الجريمة الإلكترونية ـ جرائم الانترنت)
إن من نتائج التقدم الحضاري الذي اجتاح العالم الحديث هي تقنية المعلومات التي أحدثت ثورة هائلة في استخدام الحواسب الآلية والانترنت للأغراض المختلفة، وساهمت أيضلً في تطوير العديد من السلوكيات التي تعد إجراماً مما يؤثر علي المجتمعات المختلفة.
لقد حاول العديد من المختصين وضع مفهوم واضح وثابت للجريمة المعلوماتية إلا أنه لا يمكن حصره في مفهوم ثابت، **ومما سبق يمكن تعريف الجريمة المعلوماتية علي أنها:**

فعل إجرامي يتم فيه استخدام الحاسب الآلي بطريقة مباشرة أو غير مباشرة لوسيلة أو هدف لتنفيذ الفعل المقصود.
ويمكن تعريفها أيضاً علي أنها أي جريمة يستخدم فيها المجرم المعلوماتي الحاسب الآلي لارتكابها.
وبمعني أشمل يمكن تعريفها علي أنها الجرائم التي ترتكب في البيئة الرقمية الإلكترونية. (القرعان،٢٠١٦)
ومما سبق يمكن القول بأنه لا يمكن لأي شخص عادي ارتكاب الجريمة المعلوماتية لأنها تتطلب العلم بعلوم بالحاسب الآلي، والإلمام بتقنيات المعلومات والذي قد يكون هو الآخر هدفاً، ولا تزال الجرائم المعلوماتية في تطور هائل نظراً لتطور البيئة الواقعة فيها.

ثانياً: أنواع الجريمة المعلوماتية:

أ) الجرائم التي تقع علي الأشخاص:

١- جريمة انتحال الشخصية:

هي انتحال شخصية أحد الأفراد علي شبكة الانترنت والتصرف بحرية تحت اسمه واستغلاله أسوء استغلال. (الجنيهي، ٢٠٠٥)

٢- جريمة الملاحقة / المضايقة:

وهي المساحات المتاحة علي الفضاء الرقمي والتي تتيح لمستخدميها تبادل المحادثات والمناقشات بين بعضهم البعض.
مثل (رسائل التهديد والتخويف). (الشوابكه، ٢٠٠٤)

٣- جرائم الاستدراج والتغرير:

وهي أحد أشهر الجرائم المعلوماتية والتي يقوم بها المجرم المعلوماتي باستدراج ضحيته عن طريق معلومات وهمية واقناعه بزواج أو صداقه وذلك لمحاولة ابتزازه مستقبلاً. (شيباني، ٢٠١٦)

٤- جريمة التشهير وتشويه السمعة:

هي عبارة عن مجموعة من المواقع التي تهدف إلي التشهير ونشر الشائعات لمجموعة من الرموز في مختلف المجالات.

مثل (نشر المعلومات الغير صحيحه عن أشخاص بعينهم – إرسال الملفات والصور المفبركه لأشخاص ليس فيهم ذلك ..إلخ).

٥- جرائم الأخلاق والآداب العامة:

إن نشر المواد المخلة بالآداب العامة يعد جريمة يعاقب عليها القانون.

مثل (محاولة إفساد الآخرين). (حشمان، ٢٠١٩)

ب) جرائم الأموال: ومن أنواعها

١- جرائم الفيروسات:

وهي عبارة عن برامج مصممة للتأثير علي جميع برامج الحاسب الآلي سواء بنسخها أو بحذفها نهائياً من الجهاز أو تعطيلها عن العمل. (شيباني، ٢٠١٦)

٢- جرائم الاختراق:

هي عملية الدخول الغير مصرح بها إلي الشبكات أو الأجهزة الأخري حيث يستخدم المجرم المعلوماتي مجموعة من البرامج المخصصة لذلك ويكون لديه القدرة علي تخطي أية اجراءات.

٣- جرائم تعطيل الشبكات:

والتي تتم عن طريق إرسال عدد محدد من الرسائل بطريقه فنية محدودة مما يؤدي إلي تعطيل الشبكة أو الجهاز عن تأدية عمله. (حشمان، ٢٠١٩)

٤- جرائم النصب والاحتيال:

ساعدت البيئة الرقمية علي سرعة التواصل عن طريق الحاسب الآلي كل شخص بإسمه الأمر الذي فتح المجال أمام المجرمين أن ينتحلوا الشخصيات ويقومون بعمليات مصب بأسماء مستعارة. (**Sabillon, ٢٠١٦**)

ثالثاً: خصائص الجريمة المعلوماتية في البيئة الرقمية:

تستهدف الجريمة المعلوماتية المعلومات بالدرجة الأولي مما يجعل لها خصائص تميزها عن غيرها من الجرائم، وهي :

١- الحدود الجغرافية (التنفيذ عن بعد):

إن شبكة الانترنت ألغت الحدود الجغرافية بين الدول، حيث سعت الدول المتقدمة إلي إنتاج ونشر هذه الأجهزة بين الدول بغرض الربح المادي، مما سهل وسيلة المجرم المعلوماتي الذي يسعي وراء الربح في مجتمع منفتح علي الشبكات والتكنولوجيا يوماً بعد يوم. (سعدات، ٢٠١٥)

٢- البيئة الرقمية:

إن وقوع الجرائم المعلوماتية في بيئة رقمية يصعب من عملية اكتشاف مرتكبيها، فلا يوجد أي دليل مادي أو دليل مرئي حيث تغلب عليها صفة الرقمية. (عمر، ٢٠١٣)

٣- أكثر من مجرم:

عادة ما تتطلب الجريمة المعلوماتية شخصان أو أكثر أحدهم متخصص في تقنيات الحاسوب والأنظمة، والآخر هدفه كسب الأموال والمعلومات، وقد يكون هناك شخص متخصص مسئول عن الحماية والهجمات المضادة. (المومني، ٢٠١٠)

٤- الإبلاغ عن الجريمة:

تحاول المؤسسات المعلوماتية والهيئات والشركات أن تتجنب الإساءة لسمعتها وعدم هز الثقة مع عملائها مما يمنعهم عن الإبلاغ عن تلك الجريمة. (الأسدي، ٢٠١٤)

٥- سريعة الارتكاب والتطور:

إن الجريمة المعلوماتية تحتاج فقط إلي قدر معين من التفكير الذهني وضغطة زر واحدة قد تكون كافية لتنفيذ جريمته، فضلاً عن توافر البرامج اللازمة لتنفيذ ما يحتاجه في ظل التطور التكنولوجي الذي ساعد علي سرعة ارتكاب الجرائم المعلوماتية. (وردة،٢٠١٨)

شكل (١) خصائص الجريمة المعلوماتية

رابعاً: أدوات ارتكاب الجريمة المعلوماتية:

يتطلب ارتكاب الجريمة المعلوماتية مجموعة من الأدوات، أهمها:

١- البيانات والمعلومات:

فقبل أن يقوم المجرم المعلوماتي بارتكاب جريمته فإنه أولاً يقوم بجمع المعلومات الكافية حول النظام المعلوماتي المستهدف. **(Azzam, ٢٠١٤)**

٢- الحاسوب:

يعتبر الحاسب الآلي هو أحد أهم الأدوات للمجرم المعلوماتي حيث يقوم من خلالها بارتكاب جريمته عن طريق إرسال الفيروسات أو المواقع التي من خلالها يستطيع أن يصل إلي تلف في النظام أو أنشطة البرامج المتاحة علي الحاسوب. (الأسدي، ٢٠١٤).

٣- شبكة الانترنت:

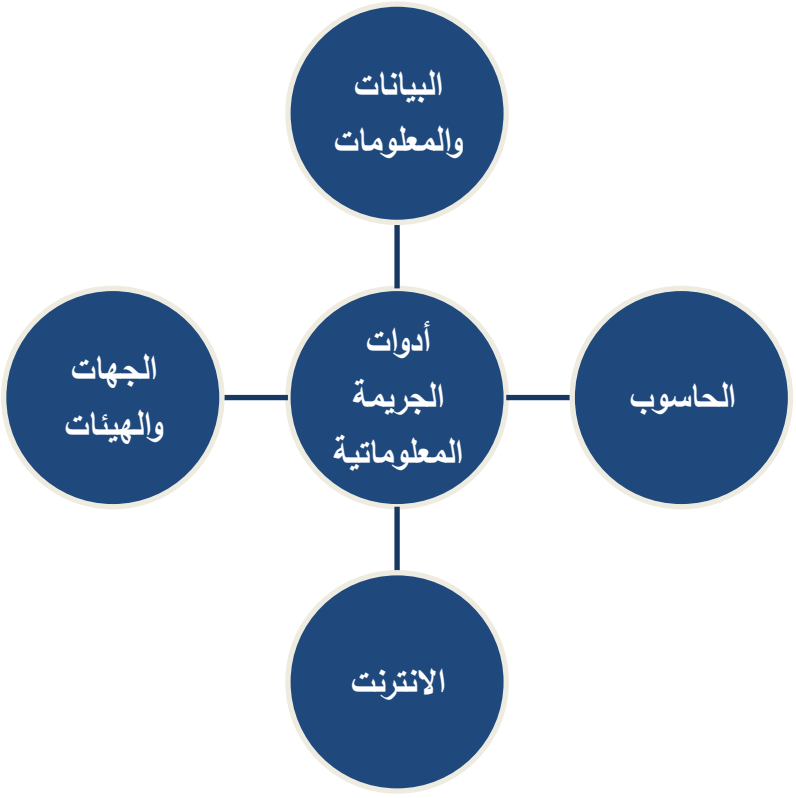
إن استخدام الحاسب الآلي بدون الانترنت لن يساعد المجرم المعلوماتي في إلغاء الحدود الجغرافية، وبالتالي فإن الانترنت هو المكمل الأساسي للحاسب الآلي للوصول للمواقع والأنظمة. **(Das, ٢٠١٣)**

٤- الجهات والهيئات والأشخاص:

تستهدف الجرائم المعلوماتية أشخاص أو هيئات بعينها.

وتنقسم إلي:

١. جرائم مباشرة: **مثل (الابتزاز ـ التهديد ـ التشهير)**
٢. جرائم غير مباشرة: **مثل (الحصول علي المعلومات الخاصة) (Holt, ٢٠١٥)**



شكل (٢) أدوات الجريمة المعلوماتية

خامساً: نظم مكافحة الجريمة المعلوماتية:

وضحت هيئة الاتصالات وتقنية المعلومات نظم مكافحة الجريمة المعلوماتية علي أنها:

١) المصطلحات:

- الشخص.
- النظام المعلوماتي.
- الشبكة المعلوماتية.
- البيانات.
- برامج الحاسب الآلي.
- الحاسب الآلي.
- الدخول غير المشروع.
- الجريمة المعلوماتية.
- المواقع الإلكترونية.

٢) الحد من وقوع الجرائم: عن طريق

- تحقيق أمن المعلومات.
- حفظ الحقوق.
- الالتزام بالآداب والأخلاق.
- حماية الاقتصاد الوطني.

٣) السجن عام والغرامة لمرتكبي الجرائم التالية:

- التصنت عن طريق الشبكة المعلوماتية.
- دخول غير مشروع علي المواقع الإلكترونية أو لتهديد شخص وابتزازه.
- المساس بالحياة الخاصة، والتشهير بالآخرين.

٤) السجن ثلاث سنوات والغرامة لمرتكبي الجرائم التالية:

- الاستيلاء علي الأموال لنفسه أو لغيره.
- الدخول إلي بيانات بنكية أو ائتمانية.

٥) السجن أربع سنوات والغرامة لمرتكبي الجرائم التالية:

- الدخول غير المشروع لحذف بيانات أو تدميرها.
- تعطيل أو تدمير الشبكة المعلوماتية أو إيقافها عن العمل.
- إنشاء المواقع علي الشبكة المخلة بالآداب أو بغرض الاتجار بالممنوعات.
- تشويش أو تعطيل الوصول للخدمات.

٦) السجن خمس سنوات والغرامة لمرتكبي الجرائم التالية:

- المساس بالنظام العام أو القيم الدينية.
- الاتجار بالجنس البشري.

٧) السجن عشر سنوات والغرامة لمرتكبي الجرائم التالية:

- إنشاء مواقع لمنظمات إرهابية.

- الدخول غير المشروع للحصول علي المعلومات الخاصة بالأمن الداخلي أو الخارجي.

٨) **السجن أو الغرامة عن نصف حدها لمرتكبي الجرائم التالية:**

- العصابات المنظمة.
- استغلال السلطة.
- التغرير بالقصر واستغلالهم.
- الإدانة في جرائم مماثلة.

٩) **معاقبة كل من حرض أو ساعد أو اتفق علي ارتكاب أي من الجرائم المنصوص عليها بما لا يتجاوز نصف الحد الأعلي للعقوبه.**

١٠) الشروع في الجرائم يتوجب نصف الحد الأعلي للعقوبه.

١١) الإعفاء من الجريمة بمجرد إبلاغ السلطة بالجريمة.

١٢) تطبيق هذا النظام لا يخل بالأحكام الواردة في الأنظمة ذات العلاقه.

١٣) يجوز الحكم بمصادرة الأجهزة والبرامج أو أي أداة من أدوات ارتكاب الجريمة المعلوماتية.

سادساً: الهيئات المختصة لمكافحة الجريمة المعلوماتية:

قام المؤتمر الأول لجمعيات قانون الانترنت المقام في القاهرة عام ٢٠٠٤م بوضع حجر الأساس لإنشاء هيئات مختصة لمكافحة الجريمة المعلوماتية، ومنذ ذلك المؤتمر وتم تأسيس الجمعية المصرية لمكافحة الجريمة المعلوماتية والمكونة من نخبة القضاه والمحاماه والمحاسبون والوكلاء للنائب العام والإعلاميين والمهندسيين؛ وهي جمعية غير حكومية صادرة عام ٢٠٠٥م

إن انتشار تقنية المعلومات والاتصال أدي إلي ظهور العديد من الجرائم المعلوماتية المرتبطة بالحواسيب، حيث تشكل خطراً علي سرية الأنظمة الحاسبية وسلامتها.

إن التحقيق في الجرائم المعلوماتية يتطلب تتبع الأنظمة الإجرامية من خلال مجموعة متنوعة من مقدمي خدمات الحواسيب الآلية، وبالتالي فإنه لابد من توضيح الأهداف المرجوه من الجمعية وهي:

١- نشر الثقافة الاجتماعية القانونية والاقتصادية للتعريف بالجرائم المعلوماتية.
٢- تنمية الكوادر البشرية لمواجهة الجرائم المعلوماتية.
٣- تقديم المساعدات والدعم للأشخاص والمنظمات التي تسعي إلي مكافحة الجرائم المعلوماتية.
٤- حضور المؤتمرات والندوات المتعلقة بالجرائم المعلوماتية، والجرائم الناشئة عن استخدام الانترنت.
٥- العمل علي تشجيع البحث العلمي في مجال الجرائم المعلوماتية.
٦- إنشاء قاعدة إحصائية للجرائم المعلوماتية. (الجواري، ٢٠٢٣)

شكل (٣) المجرم المعلوماتي والمستهدف

أما بخصوص الأنشطة فتتمثل في:

١- مكافحة جميع أشكال الجرائم المعلوماتية من (أجهزة ـ شبكات ـ معلومات ـ برامج ـ بيانات ـ وسائل الاتصال ..إلخ)
٢- نشر الوعي بقانون الانترنت الخاص بالجريمة المعلوماتية.
٣- تقديم الاستفسارات والإستشارات وإعداد الأدلة اللازمة للحد من الجريمة المعلوماتية.
٤- إصدار النشرات والدوريات وبثها علي الانترنت.
٥- إنشاء مؤسسات تدريبية للعمل علي تثقيف المجتمع بالجريمة المعلوماتية ومخاطرها.

سابعاً: الحلول المقترحة للحد من الجريمة المعلوماتية:

يمكن تقديم مجموعة من المقترحات التي تساعد في الحد من الجريمة المعلوماتية في النقاط التالية:

١) تنمية الضمير لدي الأفراد:

يعد الضمير هو المحدد الأساسي والرئيسي للأفراد للواجبات والممنوعات، فالضمير هو المعيار الرئيسي للأفراد من قيم وأخلاقيات ومبادئ تجعله يرضي عن تصرفاته ويقبلها أو ما يود أن يقوم به، ويتحكم أيضاً فيما يقبله أو يرفضه من تصرفات أو سلوكيات تدور حوله، وبالتالي لابد من تنمية الضمير لدي الأفراد للحد من الجريمة المعلوماتية ومخاطرها في البيئة الرقمية.

٢) التعاون الدولي:

إن التعاون الدولي أحد أبرز الحلول التي قد تساعد في الحد من الجريمة المعلوماتية في المجتمع المعلوماتي، كما هو موضح في الآتي:

- وجود نظام فعال يمكن من خلاله استخدام آليات للتعاون الدولي في مكافحة الجرائم المعلوماتية عن طريق تبادل الخبرات وتكوين مجموعة من المتخصصين والاستشاريين.
- إيجاد تشريع دولي مخصص لمكافحة الجريمة المعلوماتية.

- تبني نظام معلوماتي موحد معتمد علي إنشاء مكتب للتوثيق الإلكتروني وتسجيل جميع البرامج المعلوماتية وحفظها لاستخدامها كدليل إثبات وإدانته للمجرم المعلوماتي.
- إدراج الجريمة المعلوماتية لاختصاص المحاكم الجنائية الدولية.

٣) البنية التحتية الوطنية:

إن من الضروري حماية البنية التحتية للدول من مخاطر الجريمة المعلوماتية علي المجتمع الإقليمي والدولي؛ وذلك من خلال الآتي:

- صياغة سياسية واضحة ومحكمة للحد من اختراق الأنظمة المعلوماتية.
- التقييم المستمر من متخصصين لمنع اختراق شبكات المعلومات وزيادة الأمان وسد الثغرات.
- التدريب المستمر للكوادر المعلوماتية لتطويرهم بالأمن المعلوماتي، ومنع اختراق الأنظمة.
- تصميم نظم معلومات بديلة تحتوي علي أعلي درجات الأمان.
- تجهيز الكوادر المتخصصة للقدرة علي تحديد موقع الثغرات ومعالجتها وزيادة أمنها.

٤) الارتقاء بالأمن المعلوماتي:

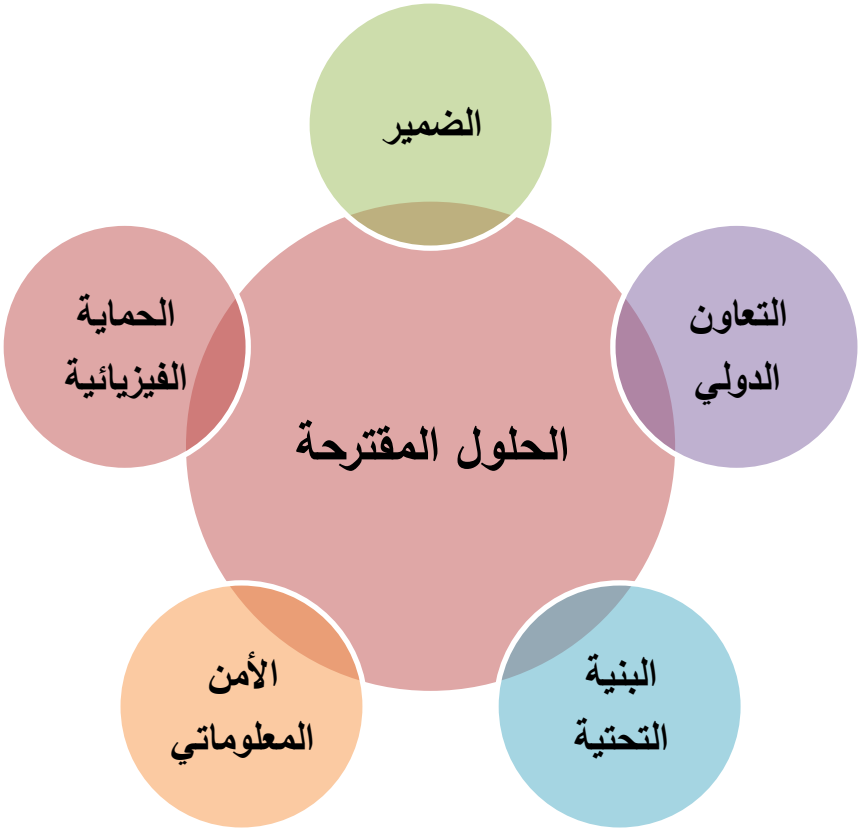
ضرورة الارتقاء بالأمن المعلوماتي من خلال الآتي:

- عزل المعلومات الهامة عن النظم والشبكات لضمان حمايتها.
- تجهيز مجموعة تقنيات متقدمة لحماية الأنظمة المعلوماتية
  مثل (برامج مكافحة الفيروسات والديدان المعلوماتية – الجدار الناري)
- إعداد سياسات أمنية لضمان الأمن المعلوماتي للأنظمة.

٥) الحماية الفيزيائية:

يجب توفير الحماية والأمان للأدوات المعلوماتية من خلال ما يلي:

- إعداد الخطط لتجاوز الأزمات المفاجأة التي قد تحل بالنظام المعلوماتي.
- إعداد نسخ احتياطية للمعلومات وحفظها في أماكن آمنة.
- وضع سياسات أمنية للدخول والخروج من النظم.
- إعداد التطبيقات الملائمة والبرمجيات اللازمة.



شكل (٤) الحلول المقترحة للحد من الجريمة المعلوماتية

ثامناً: الخاتمة:

وتشتمل علي

١) النتائج :

توصلت الدراسة إلي العديد من النتائج، وهي:

- يمكن استنتاج أولاً أن الجريمة المعلوماتية ليس لها مفهوم ثابت، مما أثر علي الأفعال التي يمكن أن تندرج تحت مفهومها، ويرجع السبب وراء ذلك لسرعة التطور والانتشار الهائل الذي تشهده الجريمة المعلوماتية وعدم القدرة علي إيقافها أو الحد منها في وقت قياسي، الأمر الذي سعت الدراسة إلي تحقيقه.
- ضرورة حماية البنية التحتية المصرية عن طريق التدريب المستمر للكوادر المتخصصة في مكافحة وملاحقة المجرمين مع إنشاء نظم معلومات أخري تحتوي علي أعلي درجات الأمان.
- يجب توفير الأمن والحماية للأدوات المعلوماتية عن طريق إعداد النسخ الاحتياطية وحفظها في أماكن أخري آمنة مع إعداد الخطط اللازمة لمواجهة الأزمات المفاجأة التي قد تخل بالنظام المعلوماتي.
- تعد الجرائم المعلوماتية من الجرائم التي تمس الأخلاق العامة، ولها صوراً وأنواع متعددة كل منها يثير مشكلات مختلفة.
- سعت الجمعية المصرية لمكافحة الجريمة المعلوماتية سواء كانت (أجهزة – شبكات – نظم معلومات – وسائل اتصال)
- ضرورة الارتقائ بالأمن المعلوماتي عن طريق عزل المعلومات الهامة عن النظم والشبكات لضمان حمايتها من مخاطر الجرائم المعلوماتية.
- أن الجريمة المعلوماتية لها خصائص وسمات مختلفة تميزها عن غيرها من الجرائم التقليدية الأخري، ويرجع السبب وراء ذلك للبيئة الرقمية التي تتعايش فيها، مما ساعد المجرم المعلوماتي علي اكتساب صفات معينة تميزه عن غيره من المجرمين التقليديين.

- الجرائم المعلوماتية من الجرائم العابرة للحدود فهي غير مقيدة بمكان أو دولة محددة أو زمان معين.
- هي من الجرائم التي تتطلب الذكاء والسرعة ولا تتطلب أي عنف علي الإطلاق، حيث تتعامل الجريمة المعلوماتية مع مجرم يتصف بالدهاء والبديهة والذكاء ولديه أهداف تخطيطية لووصول معلومات محددة.
- هي جريمة صعبة الاثبات لأنها تختلف عن الجرائم التقليدية، ويصعب تحديد مكان ارتكابها وصعوبة تحديد الجاني.
- يجب أخذ الحيطة والحذر في استخدام التطبيقات وأخذ نسخة من المعلومات الهامة ووضعها في نظام آمن.

- ضرورة التعاون الدولي لوضع نظام فعال يمكن من خلاله تبادل الخبرات بين المتخصصين ووضع آليات للحد من الجريمة المعلوماتية ومخاطرها الدولية التي تجتاح الدول.

٢) التوصيات:

ومما سبق يمكن الخروج بمجموعة من التوصيات

- وضع مجموعة من المسابقات التنافسية للمواهب التي لديها إمكانات تقنية عالية والتي تهدف إلي تخصيص جوائز قيمة لأكثر المواهب التي تضع نظام آمن أو برامج لحماية الأنظمة التي تم اختراقها علي أيدي مجرمين، الأمر الذي سيخلق بيئة تنافسية ومجال لإخراج المواهب وأيضاً استغلال مواهبهم بطريقة شرعية وآمنة بدلاً من أن يكونوا عرضة للاستغلال من المجرمين.
- ضرورة تكثيف واستمرار الحملات التوعوية بالجرائم المعلوماتية من أجل حماية الشباب والأطفال من مخاطرها وأيضاً تكوين خلفية كافية للتعامل مع هذا النوع من الجرائم سواء للشباب أو الأطفال.
- ضرورة حجب المواقع والبرامج التي تخالف القوانين وتهدف إلي استدراج المستفيدين للحصول علي معلومات تساعدهم في الاختراق الأمني أو في تحقيق أهدافهم الإجرامية.

٣) المراجع:

أولاً: المراجع العربية:

- الجنيهي، منير محمد (٢٠٠٥). جرائم الانترنت والحاسب الآلي ووسائل مكافحتها. دار الفكر الجامعي: الأسكندرية. ٤٢ص.
- الجواي، حميد أسعد (٢٠٢٣). الجريمة المعلوماتية. مجلة بلاد الرافدينللعلزم الإنسانية والاجتماعية. ١٢١-١٣٠ص.
- حشمان، عمار (٢٠١٩). الجريمة المعلوماتية في التشريع الجزائري، رسالة ماجستير، جامعة قاصدي مرياح – ورقلة، كلية العلوم الاقتصادية، قسم علوم التيسي. ص٦.
- سعدات، محمود فتوح محمد (٢٠١٥). خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية: المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية. جامعة الإمام محمد بن سور. ص ص ٣٤-٤٩ص.
- الشوابكة، محمد أمين أحمد (٢٠٠٤). جرائم الحاسوب الأولي والانترنت. دار الثقافة للنشر والتوزيع، ط١. عمان. ٤٥ص.
- شيباني، عبدالكريم (٢٠١٦). الحماية الإجرائية والموضوعية للجريمة المعلوماتية، رسالة ماجستير. كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، ص١٩.
- طرفي، حياة (٢٠١٢). المكتبات وحق المؤلف في ظل البيئة الرقمية: دراسة ميدانية بمكتبات جامعة محمد خيضر بسكرة. علم المكتبات: جامعة منثوري.

- عمر، رشاد (٢٠١٣). المشاكل القانونية في الجرائم المعلوماتية: دراسة تحليلية مقارنة. الأسكندرية: المكتب الجامعي الحديث. ص ص ١٥-١٧.
- القرعان، محمود أحمد (٢٠١٦). الجريمة الإلكترونية. عمان: دار وائل للنشر والتوزيع. ص١٩.
- المومني، نهلة عبدالقادر (٢٠١٠). الجرائم المعلوماتية. ط٢. عمان. دار الثقافة للنشر والتوزيع. ص٤٩.
- نبيه، نسرين عبدالحميد (٢٠٠٨). الجريمة المعلوماتية والمجرم المعلوماتي. الأسكندرية: منشأة العارف. ص ٥١.
- وردة، بوالناية (٢٠١٨). أمن المعلومات في البيئة الرقمية من منظور أعضاء هيئة التدريس بجامعة ٨ ماي – قالمة؛ نعيمة بن ضيق الله. أطروحة ماجستير. جامعة ماي بقالمة، كلية العلوم الإنسانية والاجتماعية. قسم علوم الإعلام وعلم المكتبات. ١٥٦ص.

ثانياً: المراجع الأجنبية:

- Azzam, adel (٢٠١٤). Jurisdiction in cybercrimes: A comparative Study, Journal of law, policy and Globalization, Vol.٢٢.
- Das, Sumanjit (٢٠١٣). Impact of Cybercrime: Issues and Challenges .International journal of engineering sciences emerging technologies ٦ (٢), ١٤٢ – ١٥٣.
- Holt, Thomas (٢٠١٥). Cybercrime in progress: theory and prevention of technology enabled offenses. Routledge.Vol ٢٧٨.
- Sabillon, Regner (٢٠١٦). Cybercrimes and cybercriminals: A comprehensive study. International journal of computer networks and communications security. ٤ (٦).

Abstract

Information between risk and crime in the digital environment

Technological developments have had a significant impact in all fields, especially in the field of information. Technology has helped to preserve and disseminate information more easily and faster than the traditional system. With the advent of these developments, many tools and motives have emerged that threaten the security of information and seek to obtain information by illegal means.

The aim of the study is therefore to identify the most important types of information crime, the tools used to commit it, the characteristics that distinguish it from other traditional crimes, as well as the systems for combating information crime and the most important bodies for combating it, and to develop solutions to reduce the risks and risks of information crime.

The study was based on a descriptive and analytical approach that seeks to solve problems and offer them a set of innovative solutions. The study found many results, the most important of which are:

The need to protect Egyptian infrastructure through continuous training of cadres specialized in combating and prosecuting criminals and the establishment of other information systems containing the highest levels of safety and the security and protection of information tools must be provided through the preparation and storage of backups in other safe places with plans to deal with sudden crises that may disturb the information system, and the need for international cooperation to develop an effective system through which expertise can be exchanged among specialists and mechanisms to reduce international information crime and its risks to States and a set of competitive competitions for talent with high technical potential aimed at allocating valuable prizes to the most talented who set up a security system or programs to protect systems hacked by criminals.

Information between risk and crime in the digital environment

Preparation

Mahmoud Abd Elmoneim El Sayed Ahmed Qoura

PhD researcher, Department of Libraries and Information
Faculty of Arts - Tanta University

Supervision

A.Dr. Ahmed Ebada Al-Arabi

Professor of Libraries and Information,
Faculty of Arts, Tanta University

٢٠٢٤