وزارة المالية
قطاع مكتب الوزير
الإدارة المركزية لمركز المعلومات والتوثيق
الإدارة العامة المركزية للمعلومات الإحصائية

دراسة عن
الجرائم المعلوماتية والالكترونية عبر شبكة الانترنت وسبل مواجهتها

إعداد : جورج اسحق حنين — مدير إدارة جمع البيانات
مراجعة و إشراف/أ٠عاطف سعيد شبانه — مدير عام
إدارة المعلومات الإحصائية

متابعة/ أ٠ عادل إسماعيل السيد هلال — رئيس الإدارة المركزية
لمركز المعلومات والتوثيق

مقدمة

مع النمو المستمر للثورة المعلوماتية الذي يعيشه عصرنا ويشهده حاضرنا أصبحنا نواجه العديد من الأخطار والمشاكل التي تنشأ بشكل تلقائي مع أي تطور حضاري وتقني ، فدخول الإنترنت في عالمنا وتمكن الصغير والكبير والجاهل والمتعلم من استخدامه دون أي قيود أو رقابة أدى إلى زيادة هذه الأخطار وتفشى النهب والسرقات الإلكترونية بشكل ملحوظ

ولحفظ الحدود وزيادة الحماية وجب سن القوانين التي ترغم المجرمين على التزام حدودهم وكان أكبر عائق يواجه هذه القوانين هو تطبيقها على أرض الواقع وبشكل فعلي وذلك بسبب جهل الناس بها لأنها قوانين مستجدة وحديثة لجرائم غير معهودة وليست كغيرها من الجرائم فكان من أهم خطوات تطبيق هذه القوانين هو توعية الناس بالجرائم الإلكترونية وما تسببه من أضرار.

في هذه الدراسة سنركز على أحد أهم الأخطار في عصرنا الحاضر وهي الجرائم الإلكترونية أو مايطلق عليها (بجرائم أصحاب الياقات البيضاء whit collar)وأهدافها وكيفية مواجهتها.

وسوف نقوم بتعريف شامل بالجرائم الإلكترونية ووصفها ومنفذي هذه العمليات وكذلك أنواعها وأصنافها وبعد ذلك تأتي وسائلها و طرق الوقاية منها في الحياة العملية .

أهم النقاط التي سوف يتم مناقشتها وعرضها بهذه الدراسة

- مقدمة
- ماهية الجريمة الإلكترونية
- تعريف الجريمة الإلكترونية
- خصائص وسمات الجرائم المعلوماتية
- صعوبات تواجه مكافحة الجرائم المعلوماتية
- منفذي الجريمة الإلكترونية
- أهم سمات مرتكبي الجرائم المعلوماتية
- أهداف الجرائم الإلكترونية
- أنواع الجرائم الإلكترونية والمعلوماتية
- استراتيجيه وزارة الداخلية لمواجهة الجرائم الالكترونية
- أسباب صعوبة إثبات الجرائم الإلكترونية
- عرض نماذج لأهم الجرائم الالكترونية
- كيفية الإبلاغ عن الجرائم الإلكترونية
- وسائل الجرائم الإلكترونية وطرق الوقاية منها
- التأمين الالكتروني للبرامج والبيانات والاتصالات

- توصيات – الخاتمة – المراجع

منهجية الدراسة

مشكلة الدراسة الأساسية تنصب على:-

العديد من الأخطار والمشاكل التي تنشأ بشكل تلقائي لمستخدمي شبكة الإنترنت الأمر الذي أدي بدوره إلى زيادة وتفشى النهب والسرقات الإلكترونية والمعلوماتية بشكل ملحوظ ٠

أهمية الدراسة تبرز في :-

الجرائم الالكترونية ظاهرة إجرامية مستجدة نسبياً تقرع في جنباتها أجراس الخطر لتنبه العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عنها والتي تستهدف البيانات والمعلومات والبرامج الالكترونية بكافة أنواعها فهي جرائم التقنية العالية التي تنشأ في الخفاء ويقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية وتوجه للنيل من المعلومات المنقولة عبر الانترنت والتي تمس الحياة الخاصة للأفراد وقد تهدد أيضاً الأمن القومي وتشيع فقدان الثقة بالتقنية الحديثة

الهدف من الدراسة :-

١- التعرف على ماهية الجرائم الإلكترونية

٢- أهداف الجرائم الإلكترونية

٣- تصنيفات وأنواع الجرائم الإلكترونية

٤- وسائل الجرائم الالكترونية وطرق الوقاية منها

ماهية الجريمة الإلكترونية

في عصرنا الحاضر الذي يشهد ثورة معلوماتية ضخمة حيث تتسابق العلوم والاكتشافات في الظهور و كل يوم تظهر منافسة قوية وجادة في المجال الإليكتروني ففي بداية الأمر ظهرت شبكة (الإنترنت) باستخداماتها المحدودة غير أنها توسعت وانتشرت انتشاراً سريعاً في وقت قياسي وقد أصبح مستخدميها من جميع الفئات العمرية وعلى مختلف مستويات تعليمهم ومن هنا دق ناقوس الخطر حيث أن هذه الشبكة بقيت بدون حراسة وبدون قيود أو حدود لردع الأعمال السيئة التي مصدرها دائماً الإنسان وكنتيجة حتمية لأي تقدم تقني مستحدث أدى إلى ظهور ما يسمى بالجرائم الإلكترونية والمعلوماتية التي أتت لتنبه المجتمعات على ضراوة خطرها ، حيث انه قد توسع مجالها وظهر محترفوها يسرقون وينهبون ويخربون مما أدى بالمجتمعات إلى الإقرار بوجوب أخذ موقف صارم تجاه تلك الجرائم واللجوء السريع إلى إيجاد الحلول التي كان جوهرها هو معرفة ماهية الجريمة الإلكترونية والغرض منها ومعرفة صورها وكيفية الوقاية منها ومن أصحابها ، لأن أول خطوات العلاج هو معرفة المرض ولذلك برزت أهمية معرفة الجرائم الإلكترونية وضرورة تثقيف العوام من الناس وإلمامهم بخطرها وأهدافها .

إن أجهزة الكمبيوتر بحد ذاتها هي مصدر ضخم للألغام الموقوتة التي قد تنفجر في وجه صاحبها عندما يحاول الضغط عليها أو الكشف عنها ولكن تلك الألغام هي وسائل إلكترونية تختبئ تحت صور أو ملفات أو برمجيات صغيرة وقد تزداد المصيبة وتتراكم عندما نعلم أن تلك الألغام قد تستخدم وسيلة ضد أصدقائك الذين تعرفهم أو قمت بتعريفهم في ملفاتك الشخصية أو لأقرب الأقرباء .

تعريف الجريمة الإلكترونية:

- أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام القانون٠

- كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب ٠

- الجرائم التي تلعب فيها البيانات التكنولوجية والبرامج والمعلومات دوراً رئيسياً ٠

- أي فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية ٠

- كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول الي المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه ٠

- أي جريمة يكون متطلباً لاختراقها توافر معرفة تقنية الحاسب لدي فاعلها

- كل فعل أو امتناع من شأنه الاعتداء علي الأحوال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ٠

- كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها ٠

فالجريمة الإلكترونية بصفة عامة هي كل فعل ضار يأتيه الفرد أو الجماعة عبر استعماله الأجهزة الإلكترونية، ويكون لهذا الفعل أثر ضار على غيره من الأفراد.

وصف الجريمة الإلكترونية :

الجريمة الإلكترونية هي الجريمة ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني مرتبط بأي شكل بالأجهزة الإلكترونية و يتسبب في حصول المجرم على فوائد مع تحميل الضحية خسارة ودائماْ يكون هدف هذه الجرائم هو سرقة وقرصنة المعلومات

الموجودة في الأجهزة أو تهدف إلى ابتزاز الأشخاص بمعلوماتهم المخزنة على أجهزتهم المسروقة .

خصائص وسمات الجرائم المعلوماتية :

- سهولة ارتكاب الجريمة بعيداً عن الرقابة الأمنية
- صعوبة التحكم في تحديد حجم الضرر الناجم عنها قياساً بالجرائم التقليدية
- مرتكبها من بين فئات متعددة تجعل من التنبه بالمشتبه بهم أمراً صعباً
- تنطوي علي سلوكيات غير مألوفة عن المجتمع
- سهولة إتلاف الأدلة من قبل الجناة
- جريمة عابرة للحدود لاتعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني عليه

صعوبات تواجه مكافحة الجرائم المعلوماتية :

١- صعوبة التوصل إلي الأدلة الرقمية والتحفظ بها

٢- القصور التشريعي في تعريف مفهوم الجريمة المعلوماتية

٣- عدم وجود مفهوم قانوني دولي مشترك لتعريف الجريمة المعلوماتية

٤- قصور النصوص التشريعية الخاصة بمواجهة تلك الجرائم

٥- قصور التعاون الدولي بين الدول في مجالات المكافحة

منفذي الجريمة الإلكترونية :

تتنوع أعمار منفذي الجرائم الإلكترونية مع اختلاف دوافعهم فهناك من منفذي تلك الجرائم الأطفال والمراهقين الذين تكون في الغالب دوافعهم لمجرد التسلية غير

مدركين حجم الأضرار التي يقومون بها، وهناك المحترفين والمختصين والإرهابيين الذين من الممكن ان تحطم أعمالهم شركات ضخمة وتضر بدول كبيرة .

أهم سمات مرتكبي الجرائم المعلوماتية :

١- شخص ذو مهارات فنية عالية متخصص في الإجرام المعلوماتي

٢- شخص قادر عي استخدام خبراته في الاختراقات وتغيير المعلومات

٣- شخص قادر علي تقليد البرامج أو تحويل أموال

٤- شخص محترف في التعامل مع شبكات الانترنت

٥- شخص غير عنيف لأن تلك الجريمة لاتلجأ للعنف في ارتكابها

٦- شخص يتمتع بذكاء حيث يمكنه التغلب علي كثير من العقبات التي تواجه أثناء ارتكابه الجريمة

٧- شخص اجتماعي له القدرة علي التكيف مع الآخرين

أهداف الجرائم الإلكترونية :

يمكن عرض بعض أهداف الجرائم الإلكترونية ببضعة نقاط أهمها:

١- التمكن من الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.

٢- التمكن من الوصول عن طريق الشبكة العنكبوتية(الانترنت) إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها .

٣- الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها .

٤- الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات اختراق وهدم المواقع على الشبكة العنكبوتية وتزوير بطاقات الائتمان وسرقة الحسابات المصرفية ، الخ ...

أنواع الجرائم الإلكترونية والمعلوماتية

١-جرائم التخريب المعلوماتي لمراكز ومكونات نظم المعلومات الالكترونية :-

- التخريب المادي :

وتتم تلك الجرائم من خلال الاختراق أو التفجير أو الإغراق بالمياه أو امتناع عن العمل وما يترتب عليه الأضرار بهذه الأجهزة والمعدات وإتلافها أو تعطيلها عن العمل من كفاءتها ٠

- التخريب المنطقي:

وتستهدف تلك النوعية من الجرائم نظم التشغيل والبرامج والتطبيقات وكذا قواعد البيانات وتتم بواسطة برامج خبيثة تصيب مكونات النظام المعلوماتي بالشلل التام أو الجزئي طبقاً لنوعية تلك البرامج ومنها مايسمي (بالجرائم المنطقية والفيروسات)والتي قد تستخدم لأغراض الحماية أو التخريب ٠

٢- جرائم التجسس والقرصنة الالكترونية:

تعتمد أساليب جرائم التجسس الالكتروني علي ما يلي :-

أساليب تقليدية كسرقة أو نسخ الوسائط الممغنطة أو الضوئية التي تختزن فيها البيانات أو استقطاب وتعيين بعض العاملين بمركز المعلومات للكشف عن البيانات المخزنة داخل الحاسبات وذلك من خلال الرشوة أو التهديد أياً كان نوعه ٠

أساليب فنية تعتمد علي فكر تكنولوجي وتقنيات تكنولوجية حديثة وبرامج متطورة معدة خصيصاً لعمليات التجسس ومثالها ما يحدث في حالات التصنت والاختراق ٠

القرصنة الالكترونية ومن أمثلتها جرائم التقليد – سرقة برامج المصدر النسخ المباشر للبرامج – النسخ غير القانوني للبرامج ٠

٣- جرائم النصب والتلاعب الالكتروني :

يتم تنفيذ هذه الجرائم من خلال عدة أساليب أهمها :

*التلاعب في مرحة إدخال البيانات وتتم في المراحل الأولية لتشغيل نظام المعلومات الالكترونية حيث يعتمد مرتكبي الجريمة وهم من العاملين بمركز المعلومات إلي إدخال بيانات غير صحيحة أو مزورة أو محرفة أو منع إدخال بيانات حقيقية ووثائق معينة ٠

*التلاعب حال إعداد وتطوير البرامج ويتم من خلال إجراء عدد من التعديلات القانونية أثناء فترة تنفيذها لتصحيح أخطاء لم يتم من قبل اكتشافها أو إذا ما أقتضي الأمر تطوير تلك البرامج ففي هاتين المرحلتين يمكن لمرتكبي الجريمة من إدخال بعض التعديلات غير المرخص بها وذلك تحقيق ما يصبو إليه من أهداف غير مشروعة ٠

*التلاعب في نظم المعالجة الالكترونية للبيانات عن بعد وذلك نظراً لربط أكثر المراكز المعلوماتية في العالم بشبكات اتصالات متنوعة (تلفونية لاسلكية – ضوئية) قد أدي ذلك إلي سهولة الاتصال بالحاسبات المركزية وإمكانية التلاعب في نظم معلوماتها ٠

*أمثلة لجرائم النصب والتلاعب الالكتروني والمعلوماتي ما يلي :

- الجرائم التي تستهدف اختراق أنظمة التحويل الالكتروني للأموال والودائع المصرفية
- جرائم الاحتيال عن طريق البريد الاليكتروني
- جرائم غسيل الأموال عبر شبكة الانترنت
- جرائم القمار فكثيراً ما تتم عمليات غسيل الأموال مع أندية القمار عي شبكة الانترنت
- جرائم المخدرات واستخدام البريد الالكتروني في عقد صفقات بيع أو شرائها

ومن الملاحظ أن جرائم النصب والاحتيال المعلوماتي تتسبب في أضرار جسيمة فعلي سبيل المثال في الولايات المتحدة الأمريكية (يقدر إجمالي الخسائر السنوية الناجمة عن الاحتيال المعلوماتي ما بين ١٠٠ مليون دولار إلي ٣ بليون دولار)

٤- الجرائم المتعلقة بخصوصية وسلامة الأفراد والجرائم المخلة بالآداب العامة:

- جرائم انتهاك حرمة وخصوصية بيانات ومعلومات الأفراد والتدخل في شئونهم الخصوصية
- الجرائم الالكترونية المتعلقة بالاعتداء النفسي مثال (تأجير القتلة والترويج لعمليات الانتحار الجماعي والترويج لعمليات بيع الأعضاء البشرية)
- الترويج لعمليات الشذوذ الجنسي وتجارة الرقيق الأبيض وإشباع الرغبات الجنسية وبث صور وأفلام ومحادثات مخلة بالحياء والآداب العامة
- التشهير والإساءة للغير من خلال عرض صور ومعلومات كاذبة
- الاستغلال الجنسي والتجاري للأطفال فضلاً عن التحرش الجنسي بهم

٥-الجرائم المعلوماتية السياسية:

- إنشاء مواقع الكترونية ذات اتجاهات متطرفة ومتعصبة يعملان علي استغلال الأديان والمتاجرة بها وتبادل الاتصالات والمعلومات بين عناصر الجماعات لارتكاب أنشطة معادية وهدامة تجاه الدولة
- إنشاء مواقع اليكترونية ذات اتجاهات تهدف لإثارة البلبلة والمعارضة ضد أنظمة الحكم
- التوسع في استخدام البريد الاليكتروني لتبادل الرسائل بين عناصر تلك الجماعات بطريقة مؤمنة ٠

استراتيجيه وزارة الداخلية لمواجهة الجرائم الالكترونية

إدراكا من وزارة الداخلية لخطورة تلك النوعية من الجرائم الاليكترونية وتداعياتها السلبية علي مسيرة التنمية الاجتماعية والاقتصادية فقد اصدرت القرار رقم ١٣٥٠٧ لسنة ٢٠٠٢بانشاء إدارة لمكافحة جرائم الحاسبات وشبكات المعلومات والتوثيق للأخذ بزمام المبادرة لمواجهة تلك الجرائم والحد من خطورتها وضبط مرتكبيها وتقديمهم للعدالة ٠

وكان الهدف من تكوين تلك الإدارة هو ضبط مختلف صور الخروج علي الشرعية فيما يمس الأمن القومي وأمن الأفراد باستخدام الحواسب الآلية في مصر وذلك تداعياً لوجود مشروع الحكومة الالكترونية حيث ظهرت ضرورتها القصوى مع بدء ميكنة العمل بالحاسبات في مختلف الوزارات ومصالح وهيئات الدولة ٠

** أهم بنود خطة العمل لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات والتوثيق :-

- ضبط ومكافحة جرائم الانترنت بشني صورها وأنماطها

- تقديم المساعدات الفنية والأدلة المادية لضبط جرائم الانترنت لأجهزة الشرطة

- حصر ومتابعة مقاهي الانترنت ووضع الضوابط لها لتسجيل بيانات مستخدمي شبكة الانترنت وأعداد قاعدة بيانات وذلك لخدمة الهدف الأساسي للإدارة (ضبط ومكافحة جرائم الانترنت)

- التعاون (المحلي ، الإقليمي ، الدولي) مع كافة الأجهزة المعنية الحكومية وغير الحكومية لتنمية الوعي المعلوماتي بخطورة تلك الجرائم

- إعداد قاعدة بيانات بجرائم المعلومات التي تدخل في نطاق اختصاص إدارة ضبط ومكافحة جرائم الانترنت

دور وزارة الداخلية في مواجهة الجرائم المعلوماتية

١- التوعية المستمرة للضباط والعاملين في جميع جهات الوزارة ٠

٢- تم إنشاء مجلة الكترونية متخصصة في مجال الحاسبات وبثها لجميع جهات الوزارة عن طريق شبكة الانترنت ٠

٣- تم إنشاء موقع علي شبكة الانترنت وتخصيص صفحة لتلقي بلاغات وشكاوي المواطنين ٠

٤- عقد الندوات المتخصصة في بعض مجالات إساءة استخدام التكنولوجيا الحديثة

٥- المشاركة في المؤتمرات والندوات المنعقدة محلياً وعالمياً في مجال الجريمة المعلوماتية ٠

٦- صقل الخبرات العملية والعلمية للضباط والعاملين عن طريق الدورات التدريبية محلياً ودولياً ٠

٧- المشاركة في وضع مقترحات التشريعات الجديدة لحماية استخدامات الحاسبات والانترنت ٠

٨- التنسيق مع الأجهزة النوعية المختصة بأعمال المكافحة وتبادل المعلومات ٠

٩- تم إنشاء قواعد بيانات تخدم أعمال المكافحة والملفات والسجلات الخاصة بذلك ٠

١٠-التنسيق مع الجهات المعنية بإصدار التراخيص لمزاولة أنشطة تكنولوجيا المعلومات٠

***<u>كيفية الابلاغ عن الجرائم الألكترونية :</u>

- عبر الموقع الالكتروني لوزارة الداخلية علي شبكة الانترنت

www.moiegypt.gov.eg

- إخطار إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بمقر وزارة الداخلية بشارع الشيخ ريحان عن طريق الحضور الشخصي أو تليفونيا ٢٧٩٢٨٤٨٤- ٢٧٩٢٦٠٧١ أو عن طريق الخط الساخن رقم (١٠٨)

أسباب مدي صعوبة الإثبات في هذه الجرائم

جرائم الكمبيوتر هي تلك الجرائم التي تقع على الحقوق بكافة أنواعها والمنصوص عليها في القانون سواء كانت حقوق مالية أو معنوية٠

في ظل إثبات تلك الجريمة التي لا تكون من أي شخص فالمجرم هنا مجرم ليس بعادي و لا يمكن إثبات الجرم بالوسائل والطرق التقليدية من هنا لابد من تفعيل دور الشرطة باستخدامهم طرق ووسائل تقنية وعلمية حديثة وغير تقليدية وذلك لمواجهة مجرمي الكمبيوتر لأنهم ليسوا سوى بشر مارسوا الإجرام بالطريقة الذكية.

في بعض الأحيان يسهل الوصول إلى الفاعل خاصة باستخدام الوسائل الحديثة بالوصول إلي مكان الكمبيوتر (خاصة إذا كان ثابت) أما إذا كان المكان مقهى مثلا أو كمبيوتر (يسهل استخدامه بغير المستخدم) ربما يصعب الوصول إلى الفاعل الحقيقي لذلك يجب وضع قانون خاص بالمقاهي التي تستخدم الانترنت والتي يسهل استخدمها من قبل الغير بحيث يكتب صاحب المقهى اسم المستخدم رقم الجهاز الذي يستخدمه٠

لكن المشكلة تكمن في الخدمة الجديدة إذا كان الجهاز لاب توب والخدمة لاسلكي فيمكن الوصول لهم لكن بصعوبة خاصة مثل خدمات الانترنت الموجودة في بعض المطارات وبعض السفن

من الحقائق المسلم بها أن التقدم العلمي له تأثيره البالغ على القانون وعلى الواقع الذي يطبق عليه هذا القانون ، ولكي تتحقق الفائدة المرجوة من هذا التقدم فإن القانون يجب ألا ينفصل عن الواقع الذي يفرزه ويطبق عليه بل يجب أن يكون متجاوبا معه ومتطورا بتطوره.

ولا شك في أن التطور الحالي الذي لحق ثورة الاتصالات وما أفرزته هذه الثورة من وسائل الكترونية متقدمة ومتعددة قد انعكس أثره على الجرائم التي تمخضت عن ذلك بحيث تميزت هذه الجرائم بطبيعة خاصة من حيث الوسائل التي ترتكب بها ومن حيث من تقع عليهم الجريمة ومن حيث الجناة الذين يرتكبونها على النحو سالف الإشارة إليه، بحيث يمكن القول أن الأساس في خطر هذه الجرائم يكمن في أنها في طبيعتها

تجمع بين الذكاء الاصطناعي والذكاء البشري مما يجعل إثباتها جنائيا قد يكون في منتهى الصعوبة.

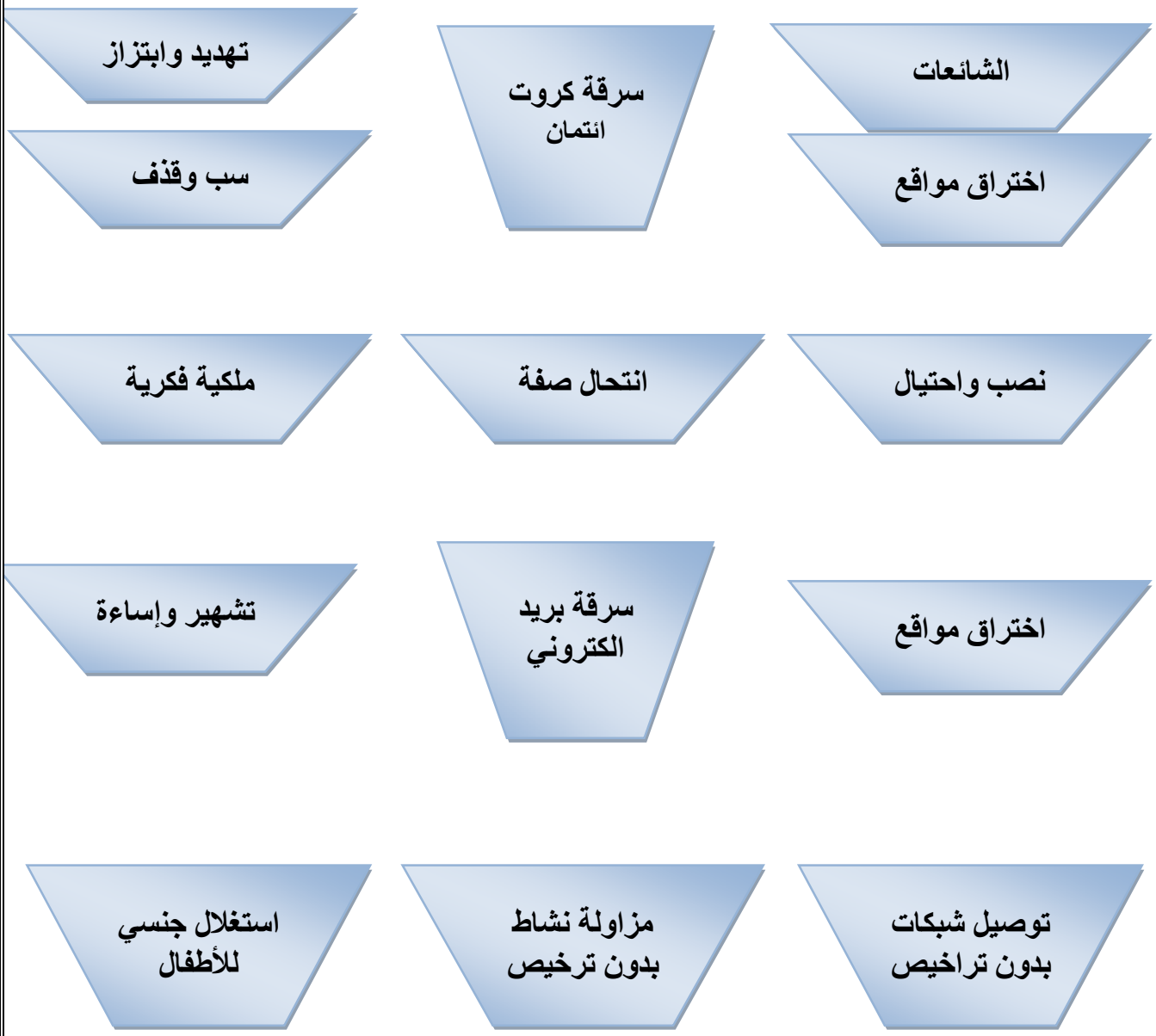
إن التطور الحالي الذي انعكس أثره على قانون العقوبات قد انعكس أثره أيضا على قانون الإجراءات الجنائية بحيث أن هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن استيعاب الجرائم المستحدثة التي ترتكب بالوسائل الإلكترونية، كما وأن الإثبات الجنائي وهو أحد الموضوعات الهامة لهذا القانون قد تأثر بدوره بالتطور الهائل الذي لحق بالأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة، الأمر الذي يتعين معه تغير النظرة إلى طرق الإثبات الجنائي لكي تقترب الحقيقة العلمية في واقعها الحالي من الحقيقة القضائية .

أخيراً ٠٠فإثبات الجرائم التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية سيتأثر بطبيعة هذه الجرائم وبالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن ارتكابها، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم، أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالأفراد وبالمجتمع.

* * *صعوبة إثبات الجرائم الإلكترونية ترجع إلى خمسة أمور هي :-

- أولاً: أنها كجريمة لا تترك أثر لها بعد ارتكابها.
- ثانياً: صعوبة الاحتفاظ الفني بآثارها إن وجدت.
- ثالثاً: أنها تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.
- رابعاً: أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.
- خامساً: أنها تعتمد على قمة الذكاء في ارتكابهالأن أهم خطوة في مكافحة جرائم الإنترنت هي تحديد هذه الجرائم أولاً ومن ثم تحديد الجهة التي يجب أن تتعامل مع هذه الجرائم والعمل على تأهيل منسوبيها بما يتناسب وطبيعة هذه الجرائم المستجدة ويأتي بعد ذلك وضع تعليمات مكافحتها والتعامل معها والعقوبات المقترحة ومن ثم يركز على التعاون الدولي لمكافحة هذه الجرائم ٠

عرض نماذج لأهم الجرائم الالكترونية



وسائل الجرائم الإلكترونية
وطرق الوقاية منها

(أ) أهم وسائل الجرائم الإلكترونية هي :

١- صناعة ونشر الفيروسات وهي من أكثر الجرائم انتشارا وشيوعاً على الإنترنت.

٢- إيقاف بعض الخدمات من خلال إغراقها بعدد هائل من الطلبات مما يؤدي الى سقوط من يقوم بأدائها وتوقف عمله فوراً .

٣- انتحال الشخصية.

٤- تشويه السمعة وذلك بنشر معلومات حصل عليها المجرم بطريقة غير قانونية وتكون هذه الأعمال لأهداف مادية أو سياسية أو اجتماعية.

٥- النصب والاحتيال كبيع السلع او الخدمات الوهمية .

(ب) أهم طرق الوقاية من القرصنة والجرائم الإلكترونية هي :

١- أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.

٢- تجنب فتح أي رسالة إلكترونية مجهولة المصدر بل المسارعة إلى إلغائها.

٣- وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تصعّب من عملية القرصنة الوصول إليه من هذه المواصفات (بأن يحتوي على أكثر من ثمانية أحرف ، أن يكون متنوع الحروف والرموز واللغات).

٤- الحرص على المعلومات الشخصية والحاسب الشخصي وذلك بوضع برامج الحماية المناسبة .

التأمين الالكتروني للبرامج والبيانات والاتصالات

- برامج الحماية من الفيروسات (Anti virus scanning) حماية الحواسب من الشبكات والرسائل الالكترونية والملفات التي يتم تحميلها من شبكة الانترنت أو أي مستخدم داخل الشبكة حيث تقوم هذه البرامج بمنع الفيروسات من الدخول لذاكرة الحاسب واكتشافها وإيقاف آثارها التدميرية ٠

- أهمية استحداث وسائل تأمينية إلكترونية تمثلت في استخدام بصمات (أصابع ، صوت ، عين ، خط) لتحديد هوية المستخدم ومنع أية محاولات نفاذ غير شرعية لنظم المعلومات الالكترونية٠

- مجموعة من البرامج الخاصة لمراقبة الصلاحيات الممنوحة لكل مستخدم أو متعامل مع أجهزة الحاسبات أو شبكات المعلومات كما أن هذه البرامج يمكن أن يصدر عنها إنذارات تنبيه لتحجيم الضرر ٠

- التشفير للمعلومات والمقصود هو تغيير مظهرها بحيث يختفي معناها الحقيقي بحيث تكون غير مفهومة لمن يتلصص عيها من مرتكبي الجرائم التكنولوجية ٠

- التوقيع الالكتروني (E- signature) له أهميته في توفير الحماية اللازمة للتعاملات الاقتصادية والمالية علي شبكة الانترنت ويتم ذلك من خلال مجموعة من البرامج ومفاتيح الشفرة الخاصة والعامة والتي تشكل منظومة أمنية دقيقة لضمان أمن وسرية أداء الصفقات الالكترونية عبر الشبكة ٠

التوصيات

١- سد الثغرات التشريعية لمواجهة كافة أشكال الجرائم الالكترونية٠

٢- إتباع الإجراءات التأمينية التكنولوجية وغيرها من الأساليب والسياسات التأمينية

٣- تفعيل وتطوير دور الأجهزة الأمنية والقضائية لمواجهة تلك الجرائم ٠

٤- تفعيل دور الأسرة ورجال الدين والأجهزة التربوية ومراكز الشباب في توعية النشء والشباب للاستفادة من الجوانب للاستفادة من الجوانب الايجابية لاستخدامات وسائل التقنية الحديثة ٠

٥- المشاركة في الجهود الإقليمية والدولية لمواجهة الاستخدام السيئ لشبكة الانترنت ٠

٦- تفعيل دور المؤسسات العلمية علي شبكة الانترنت ومراكز البحث العلمي ودعمها مادياً وبشرياً وفنياً لتمكين الشباب من الحصول علي المعلومات والمعرفة اللازمة بأمان ٠

٧- الاهتمام بدراسة علوم الأزمات والكوارث التكنولوجية لإعداد خطط وقائية وأمنية وعلاجية لهذه الأزمات ٠

الخاتمة

عندما ظهرت شبكة الإنترنت ودخلت جميع المجالات كالكمبيوتر بدءًا من الاستعمال الفردي ثم المؤسسي والحكومي كوسيلة مساعدة في تسهيل حياة الناس اليومية انتقلت جرائم الكمبيوتر لتدخل فضاء الإنترنت فظهر ما عرف بجرائم الإنترنت ٠

ويقسّم باحثين متخصصين في جرائم الانترنت تلك الجرائم ضمن فئات متعددة منها ما يتعلق بجهاز الكمبيوتر كإتلاف وتشويه البيانات والتلاعب في المعلومات المخزنة، وأخرى تتعلق بالشخصيات أو البيانات المتصلة بالحياة الخاصة، بالإضافة إلى جرائم ترتبط بحقوق الملكية الفكرية لبرامج الكمبيوتر، وانتحال شخصية أخرى بطريقة غير شرعية على الإنترنت، والمضايقة والملاحقة، والتغرير والاستدراج وهما من أشهر جرائم الإنترنت وأكثرها انتشارًا خاصة بين أوساط صغار السن من مستخدمي الشبكة.

وأيضاً صناعة ونشر الإباحية مما يحضُّ القاصرين على أنشطة جنسية غير مشروعة حيث أن صناعة الإباحية من أشهر الصناعات الحالية وأكثرها رواجًا خاصة في الدول الغربية والأسيوية علاوة على عمليات النصب والاحتيال نظرًا لأن الإنترنت مجال رحب تمارس فيه جميع أشكال التعاملات إلا أن هذه الميزة قد شابتها سلبيات عديدة أبرزها إمكانية النصب والاحتيال بخرق هذه التعاملات.

وقد واكب ثورة تكنولوجيا المعلومات والاتصالات والتوسع في استخدام شبكة المعلومات الدولية (الانترنت) ظهور نوعية جديدة من الجرائم المعلوماتية أو الجرائم الالكترونية ، هذه الجرائم أصبحت تهدد أمن وسلامة الأفراد والمؤسسات فالمعلومات تتزايد يومياً ولا تتناقص فالمعلومات تعتبر مصدر قوة اقتصادية وسياسية وعسكرية واجتماعية ومع تزايد المعلومات واستخدام شبكة الانترنت في تبادلها وبالتالي تزايدت صور الاعتداءات والتهديدات وظهور العديد من القضايا المختلفة ٠

ولا شك أن ازدهار الحضارة وانتشار التقدم التقني ساعد في تسهيل الكثير والكثير من أمور حياتنا ولكنه في نفس الوقت جلب لنا العديد من المخاطر والأضرار المتعلقة بالحاسب وشبكة الانترنت ، من هنا قد ألحت الضرورة من خلال هذه الدراسة إلي التنبه ونشر التوعية والتعريف بهذه الجرائم عن طريق شرحها وتحليلها للناس وبيان وسائل وطرق الوقاية منها .

المراجع

١- الجرائم المعلوماتية والرقمية للحاسب والانترنت

د/ يوسف المصري

٢ - الجريمة الالكترونية للمؤلف أ/ مصطفى سماره

(المجلة المعلوماتية العدد ٢٩ لعام ٢٠٠٨)

٣- أخطر الجرائم الالكترونية وطرق الوقاية منها

(مقالة علمية ١٨ /مارس/ ٢٠١٥ مقال و حوار أ/ مي عبد ربه عبد المنعم)

٤ -الجرائم المعلوماتية والاستخدام الآمن لشبكة الانترنت

مستشار / كمال نجيب

٥- مقالات في أمن المعلومات

الكاتبة: سمية بنت عبد الرحمن بن سليمان آل حمدان