سمات وأنماط المجرم المعلوماتي في جرائم الاحتيال الالكتروني

تحت إشراف

أ.د أحمد شوقي عمر أبو خطوة

أستاذ القانون الجنائي

كلية الحقوق _ جامعة المنصورة

إعداد الباحث

عبد الله سيف عبيد سالم آل على

باحث دكتوراه

سمات وأنماط المجرم المعلوماتي في جرائم الاحتيال الالكتروني

مقدمة:

أصبح العالم اليوم أمام ثورة حقيقية هي ثورة المعلومات، والعالم الرقمي وصار الناس أحيانا مختارين وفي أحايين أخرى مضطرين للتعامل مع هذا العالم الجديد أو مجتمع المعلومات كما يحلو للبعض ان يسميه ، وما لبث الناس قليلا وهم يفيقون من صدمة ثورة المعلومات الجامحة حتى دهمتهم ثورة جديدة خلقها ذلك التزاوج أو الاتحاد الفريد بين هذا الجهاز وأنظمة الاتصالات الحديثة ،لنصل في نهاية القرن الماضي وبدايات هذا القرن الي ما يسمى التواصل عبر شبكة الأنترنت العالمية، التي حطمت الحدود بين الدول وقصرت المسافات بين الأفراد والجماعات، واختصرت الزمن عبر شبكة لا مرئية ،أو محسوسة ،سميت بشبكة الأنترنت العالمية ،أو ((الشبكة العنكبوتية)) أو ((الفضاء السبراني)) والتي بدأ استعمالها للأمور العسكرية اولا في الولايات المتحدة الأمريكية منذ عام ١٩٦٩، وبدأ العالم العربي يتعرف عليها في أواخر الثمانينات وبدأت تنتشر فيه تدريجيا.

فقد كان للتقدم الإلكتروني الكبير والسريع الأثر على عملية ربط العالم بشبكات إلكترونية جعلت منه خلية مترابطة بشكل قوي. لكن هذه الشبكة فور ظهورها رافقتها موجات كبيرة من الخروقات والاعتداءات الغير متوقعة، الأمر الذي تسبب في ظهور العديد من الجرائم المستحدثة، وأيضا استخدام الوسائل التقنية الحديثة في ارتكاب الجرائم التقليدية ولقد كان الاحتيال الالكتروني في إحدى الصور الاجرامية المستحدثة والتي تحتاج إلى المواجهة القانونية والأمنية حتى يمكن الحد منها ومواجهتها بالنظر إلى تأثيرها الضار على أفراد المجتمع وعلى حجم التجارة الالكترونية التي اتسع حجم التعامل بها خاصة في مجال الأنشطة التجارية والحكومية،[1] وبذلك يتحدد موضوع الدراسة في المواجهة القانونية والأمنية للاحتيال الالكتروني.

---

[1] الغش التجاري في المجتمع الإلكتروني – ورقة عمل مقدمة إلى الندوة الرابعة لمكافحة الغش التجاري والتقليد في دول مجلس التعاون الخليجي , من الغرفة التجارية الصناعية بالرياض خلال الفترة ٢٠-٢١ سبتمبر عام ٢٠٠٥م.

أهمية موضوع البحث:

تكمن أهمية الدراســـة في حماية المجتمع وأفراده من قراصنة الحاسب الآلي ومواقع التواصل الاجتماعي وفق منظومة عمل متكاملة تؤدي للحد من احتيالهم الالكتروني وتوفير أقصـــى درجات الأمان لمستخدمي وســـائل التواصـــل الاجتماعي وفرض رقابة على القراصنة الذين يتربصون بالضحايا لممارسة الاحتيال عليهم .

كما يكتســـب موضوع البحث أهمية متزايدة بسبب استغلال وسائل الاتصالات الحديثة كالفاكس والإنترنت وســـائر صـــور الاتصال الالكتروني عبر الأقمار الصناعية التي استغلها مرتكبو الجرائم لتسهيل ارتكابهم لجرائم الاحتيال الالكتروني..

ولموضـــوع البحث أهمية من الناحية النظرية والعملية لكونه يمس كثيرا من مصالح المجتمع وعلى وجه الخصوص استخدام الاحتيال على المصارف من خلال التعامل الإلكتروني والسحب من الأرصدة بواسطة البطاقة الممغنطة أو الدفع الالكتروني وكل الجرائم الاحتيالية عبر الانترنيت.

أهداف البحث

تهدف الدراسة إلى محاور نظرية وأخرى عملية ويبدو ذلك كالآتي:

الاهداف النظرية العلمية:

١. التعريف بالجريمة الإلكترونية متضمنة الاحتيال الاليكتروني.
٢. التعريف بالوسائل الاحتيالية والاحتيال الالكتروني.
٣. زيادة الوعي العام للمتعاملين مع وسائل التواصل الاجتماعي.
٤. كيفية التحكم والسيطرة في جرائم الاحتيال الالكتروني المصاحبة لوسائل التواصل الاجتماعي.

الاهداف العملية:

١. التعريف بالاحتيال الالكتروني لأجل تحديد وسائل مواجهته قانونيا وأمنيا.

٢. الوقوف على عوامل الاحتيال الالكتروني بما يساعد في الحد منه وعدم ارتكاب جرائم الاحتيال الالكتروني.

٣. تقييم وسائل المواجهة المطبقة قانونيا وأمنيا لمواجهة الاحتيال الالكتروني للوصول إلى أفضل الوسائل لمواجهته .

مشكلة البحث

مشكلة البحث تعود إلى ما يتميز به من صفة فنية ، ومفردات ومصطلحات جديدة كالبرامج والبيانات التي تشـــكل محلا للاعتداء أو تستخدم كوسيلة للاعتداء ، وهي جرائم ذات طبيعة خاصة متميزة ، وذلك راجع إلى عدة عوامل منها طبيعة النظام المعلوماتي وحداثة ظهور الحاسب الآلي وتقنية تشغيله ، ولهذا أصبح لا يكفي أن يكون الباحث متخصصا في القانون ، بل يتعين عليه أن يكون ملما بالجوانب الفنية للحاسب الآلي والإنترنت ليتمكن من إيجاد الحلول للتحديات والمشـــاكل القانونية التي تثيرها شبكة الاتصال والمعلومات وجرائمها الإلكترونية ومنها جرائم الاحتيال الالكتروني.

فقد برزت على السطح جرائم الاحتيال الالكتروني بما تحمله في طياتها من الكثير من أشكال الاحتيال و التي تمثل هاجسا للأمن والمجتمع على حد سواء، فلقد غيرت شبكة الإنترنت حياتنا، فوفرت فرصا هائلة للتعلم، المشاركة، الاتصال، التسوق و المعاملات البنكية، ومع ذلك ازدادت حركة مرور المجرمين عبر الإنترنت حيث يبلغ ضحايا الاحتيال عبر الإنترنت الملايين من الأبرياء في كل عام.

فمشكلة هذا البحث تتحدد في الطبيعة المميزة لوسائل الاحتيال الالكتروني ، فهي قد تتم بطرق فنية محكمة يصعب كشفها وبالتالي فإن ذلك سينعكس على الأساليب المواجهة لمثل هذا النوع من الجرائم الذي يتميز بالطبيعة المعنوية والفنية المعقدة ، ولذلك فإن هذه الدراسة ستحاول أن تساعد على إيجاد حلول تساعد في كشف الاحتيال الالكتروني حتى يمكن الحد من ارتكابها واستطاعة الوصول إلى الأدلة التي تثبتها وتسندها إلى مرتكبيها.

منهجية البحث

االعتمد البحث على المنهج الوصفي التحليلي لتغطية أدبيات الدراسة.

المبحث الأول

ماهية وملامح الاحتيال الالكتروني

أن ثورة المعلومات و الاتصالات و انتشار الشبكات الاجتماعية تعد ظاهرة تستحق الاهتمام و الدراسة لمعرفة آثارها على التواصل الاجتماعي في محيط الاسرة ، لذلك تعد موضوعات الشبكات الاجتماعية و التواصل الاجتماعي من الموضوعات الهامة ومن ثم فإن العالم بحاجة إلى تقديم تقييم اجتماعي موضوعي لها لكي يتم ابراز تداعياتها على العلاقات في محيط الاسرة حيث أصبحت هذه التقنية في متناول كافة فئات المجتمع من أطفال – مراهقين – بالغين – و طريقة استخدامهم لهذه التقنية وابتعادهم عن الجو الأسري و التأثير الكبير لمثل هذه التقنيات في التأثير على الجوانب الاجتماعية و النفسية – الدينية – العادات و التقاليد المجتمعية – وكذلك الجوانب التربوية وانخفاض العلاقات الاسرية بين افرادها.[1]

لذلك نتناول هذا المبحث في الوقوف على الاحتيال الالكتروني كواحدة من الجرائم الالكترونية الهامة التي تصيب المجتمع في مقتل.

من خلال مطلبين:

المطلب الأول: ماهية جريمة الاحتيال الالكتروني

المطلب الثاني: أشكال وأساليب الاحتيال الالكتروني

---

(١) آل علي، فيصل محمود، ٢٠١٩، أثر التقنيات الحديثة على العلاقات الاسرية في مجتمع دولة الامارات العربية المتحدة، جامعة الملك محمد الخامس، كلية الآداب والعلوم الإنسانية، قسم علم الاجتماع، بحث مقدم لدرجة الدكتوراه في علم الاجتماع، المغرب.

المطلب الأول

ماهية جريمة الاحتيال الالكتروني

تمهيد وتقسيم:

تعرف جريمة الاحتيال الالكتروني بانها " نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه " وتعريفها بانها " كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات "[1] او هي " أي نمط من انماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات " او هي " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة واساءة استخدام المخرجات اضافة الى أفعال أخرى تشكل جرائم اكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر "[2]

تعرف الاحتيال عبر الإنترنت: بأنه أي نوع من أنواع الخدع أو الحيل التي تستخدم خدمة أو أكثر من خدمات الشبكة الانترنت ، كـــغرف المحادثة أو البريد الإلكتروني أو منتديات الإنترنت أو أي موقع من مواقع الويب من أجل توجيه نداءات خادعة إلى ضحايا محتملين على شبكة الانترنت. يهدف احتيال الإنترنت في العادة إلى الاحتيال على المستخدمين عن طريق سلب أموالهم (إما بسرقة أرقام بطاقات ائتمانهم أو بجعلهم يرسلون حوالات مالية أو شيكات) أو دفعهم إلى الكشف عن معلومات شخصية بغرض التجسس أو انتحال الشخصية أو الحصول على معلومات حسابهم إن كانوا من أصحاب النفوذ والسلطة أو الأثرياء او الموظفين في وظائف حساسة وهامة, بغرض الابتزاز.

ولقد تحول هذا النوع من الاحتيال إلى تجارة مربحة قدرت بملايين الدولارات، و تتوزع شبكات الاحتيال حول العالم وخصوصا في ساحل العاج وغانا وجنوب أفريقيا وهولندا وذلك يؤكد ان جرائم الكمبيوتر قد

---

[1] قشوش، هدى، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،١٩٩٢، ص ٨.

[2] مكتب المحاسبة العامة للولايات المتحدة الامريكية GOA

ترتكب عن طريق حاسب آلي في دولة ما، في حين يتحقق الفعل الاجرامي في دولة أخرى" فجرائم الكمبيوتر والانترنت، لا تحدها حدود .[1]

هناك تعريف للجرائم الإلكترونية المتعلقة بالآداب العامة عن طريق تصنيفها " بأنها تلك الجرائم التي يكون موضعها الاحتيال المعلوماتي وجرائم التعرض لحرمة الحياة الخاصة وجرائم التخريب والتعدي على برامج الحاسب الآلي والمعلوماتي وهي جرائم تستهدف المصالح العامة والمصالح الخاصة التي تهم المجتمع".

كما نجد أن جرائم الكمبيوتر والانترنت نوع من الإجرام المعاصر يثير الكثير من المشكلات في نواحي عديدة أهمها صعوبة التحاق هذه الجرائم وصعوبة إثباتها، فهذا النوع من الإجرام يتسم بالمكر والحيلة والدهاء والغش والاحتيال باستخدام تقنيات معلوماتية عالية الكفاءة والتي أصبحت لسهولة استخدامها وسرعة انتشارها من الوسائل لارتكاب هذه النوعية من الجرائم.[2]

أما جريمة الكمبيوتر ، فقد صك الفقهاء والدارسون لها عددا ليس بالقليل من التعريفات، تتمايز وتتباين تبعا لموضع العلم المنتمية اليه وتبعا لمعيار التعريف ذاته ، فاختلفت بين أولئك الباحثين في الظاهرة الاجرامية الناشئة عن استخدام الكمبيوتر من الوجهة التقنية وأولئك الباحثين في ذات الظاهرة من الوجهة القانونية ، وفي الطائفة الأخيرة – محل اهتمامنا الرئيسي– تباينت التعريفات تبعا لموضوع الدراسة (القانونية) ذاته ، وتعددت حسب ما اذا كانت الدراسة متعلقة بالقانون الجنائي أم متصلة بالحياة الخاصة أم متعلقة بحقوق الملكية الفكرية (حق التأليف على البرامج).

---

[1] (Ulrich Seiber) – جرائم الحاسب الآلي والجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال، ترجمة الدكتور سامي الشوا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، ٢٥–٢٨، تشرين أول/أكتوبر ١٩٩٣ – والورقة المذكورة بذاتها من أوراق التحضير للمؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات – (البرازيل ٤ – ٩ أيلول ١٩٩٤).ص٨.

[2] حجازي، عبدالفتاح بيومي، مبادىء الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى ، ٢٠٠٦م ، ص ١٥.

تتميز الجريمة الإلكترونية في مجال المعالجة الآلية للمعلومات بالآتي :

١ – مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها ، في حين أن مرتكب الجريمة التقليدية في – الغالب – شخص أمي بسيط ، متوسط التعليم .

٢– مرتكب الجريمة الإلكترونية – في الغالب – يكون متكيفا اجتماعيا وقادرا ماديا ، باعثه من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي،[1] في حين أن مرتكب الجريمة التقليدية – غالبا – ما يكون غير متكيف اجتماعيا وباعثه من ارتكابه الجريمة هو النفع المادي السريع .

٣– تقع الجريمة الإلكترونية في مجال المعالجة الآلية للمعلومات وتستهدف المعنويات لا الماديات ، وهي بالتالي أقل عنفاً وأكثر صعوبة في الإثبات لأن الجاني مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه ، وهذا يعسر إجراءات اكتشاف الجريمة ومعرفة مرتكبها ، بخلاف الجريمة التقليدية التي عادة ما تترك وراءها دليلا ماديا أو شهادة شهود أو غيرها من أدلة الإثبات ، كما أن موضوع التفتيش والضبط قد يتطلب أحيانا امتداده إلى أشخاص آخرين غير المشتبه فيه أو المتهم .

٤– الجريمة الإلكترونية ذات بعد دولي ، أي أنها عابرة للحدود ، فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية ، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.

تتميز الجرائم المرتكبة بواسطة الكمبيوتر كأداة أو كهدف للجريمة بالخصائص التالية:

---

[1] إذا كان الدافع إلى ارتكاب الجريمة تحقيق النفع المادي ، فإن المبالغ التي يمكن تحقيقها تكون طائلة تفوق ما يتحصل عليه مرتكب الجريمة التقليدية بأضعاف مضعفة .

١. سرعة التنفيذ: لا يتطلب تنفيذ الجريمة عبر الهاتف الوقت الكبير، وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعني إنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

٢. التنفيذ عن بعد: لا تتطلب جرائم الكمبيوتر في أغلبها (إلا جرائم سرقة معدات الكمبيوتر) وجود الفاعل في مكان الجريمة.بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول للشبكة المعنية أو اعترض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب...الخ.

٣. إخفاء الجريمة:أن الجرائم التي تقع على الكمبيوتر أو بواسطته كجرائم (الإنترنت) جرائم مخفية، إلا انه يمكن أن تلاحظ آثارها، والتخمين بوقوعهاوتظهر في كل فعل أو امتناع يخالف السياسة الاقتصادية للدولة، أو يضر الاقتصاد الوطني، أو يهدده بالخطر، إذا ما جرمه القانون ، وعاقــب عليه بعقوبات جزائية.[1]

٤. الجاذبية: نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الأجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويلا مسارها أو استخدام أرقام بطاقات الدفع االلكتروني وهي عبارة عن بطاقة بلاستيكية صادرة من مؤسسة ما تُمنح لأحد عملائها، بحيث تسمح له بإجراء معاملات مالية تتمثل في دفع قيمة الخدمات أو المشتريات التي يحصل عليها، أو سحب مبالغ نقدية من حسابه، وفقاً لشروط فنية وقانونية خاصة بكل نمط من الأنماط المختلفة لبطاقات الائتمان ، كما قد تقوم البطاقة الائتمانية بوظائف أخرى وهي كونها أداة ائتمان في بعض أنواعها وأداة ضمان للشيكات في أنواع أخرى.[2]

---

[1] مليكة، جرجس يوسف ، مكانة الركن المعنوي في الجرائم الاقتصادية ، دراسة مقارنة ، المؤسسة الحديثة للكتاب ، لبنان ، ٢٠٠٥ ، ص ٧.

[2] قورة، نائلــة عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، بيروت ، الطبعة الأولى ، ٢٠٠٥ ، ص ٥٠٨.

٥. عابرة للدول:إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، وأصبحت ساحتها العالم أجمع.

ففي مجتمع المعلومات تذوب الحدود الجغرافية بين الدول، لارتباط العالم بشبكة واحدة، حيث أن أغلب الجرائم المرتكبة عبر شبكة الإنترنت، يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى،وقد يكون الضرر المترتب عن الجريمة ليس واقعا على المجني عليه داخل إقليم دولة الجاني،وتعارض المواد المعروضة مع الثقافات المتلقية لها خاصة إذا كانت تتعارض في الدين والعرف والاجتماعي والنظام الأخلاقي والسياسي للدولة.

جرائم ناعمة: تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح.إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا،فنقل بيانات من كمبيوتر إلى أخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.

٧. صعوبة إثباتها:تتميز جرائم الإنترنت عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي(بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة.

٨. التلوث الثقافي: لا يتوقف تأثير الجرائم المتصلة بالكمبيوتر عند الأثر المادي الناجم عنها وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمغلقة.

٩. عالمية الجريمة والنظام العدلي:نظرا لارتباط المجتمع الدولي إلكترونيا،فقد أصبح مجتمعنا تخيليا مما أدى إلى أن تكون ساحة المجتمع الدولي بكافة دوله ومجتمعاته مكانا لارتكاب الجريمة من كل مكان ،

مما أن تطلب أن تمارس الدول المتطورة وخاصة الصناعية على الدول النامية من أجل سن تشريعات جديدة لمكافحة الجرائم المتصلة بالكمبيوتر مما استدعى أن تكون القوانين ذات صبغة عالمية.

١٠. لا يتم – في الغالب الأعم – الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير. لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة ؛ بل وبعد وقت طويل من ارتكابها،زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها . فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة ؛ والعدد الذي تم اكتشافه ؛ هو رقم خطير . فالفجوة بين عدد هذه الجرائم الحقيقي ؛ وما تم اكتشافه : فجوة كبيرة .

١١. من الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقني ؛ كما أنه من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها.

١٢. لذا فهذه الجرائم لا تترك أثرا لها بعد ارتكابها، علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت . فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الانترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها.

١٣. تعتمد هذه الجرائم على قمة الذكاء في ارتكابها ؛ ويصعب على المحقق التقليدي التعامل مع هذه الجرائم . إذ يصعب عليه متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليها . فهي جرائم تتسم بالغموض ؛ وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية .

١٤. الوصول للحقيقة بشأنها تستوجب الاستعانة بخبرة فنية عالية المستوى.

١٥. عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم ؛ فهذه الجرائم هي صورة صادقة من صور العولمة ؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة ؛ ومن الناحية الزمنية تختلف المواقيت بين الدول ؛ الأمر الذي يثير التساؤل حول : تحديد القانون الواجب التطبيق على هذه الجريمة.

المطلب الثاني

أشكال وأساليب الاحتيال الالكتروني

أولا: أشكال الاحتيال الالكتروني

تتعدد أشكال الاحتيال التي يرتكبها مرتكبو جرائم الالحتيال الالكتروني وسنشير فيما يلي إلى أهمها:

أولا: فيروسات التتبع

(Key Loggers) هي عبارة برامج تعمل على تتبع مستخدم الكمبيوتر والتقاط حركته على لوحة المفاتيح. وتستخدم هذه النظم من قبل قراصنة للحصول على كلمات السر أو مفاتيح التشفير وبالتالي تجاوز الإجراءات الأمنية الأخرى، لاجل إرتكاب جرائمهم في الخداع الالكتروني.

ثانيا: حصان طروادة (Trojan) :

حصان طروادة هو برنامج مشروع، ولكنه يقوم بأداء أنشطة غير مشروعة عندما يعمل، بحيث يمكن استخدامه لتحديد موقع معلومات كلمة المرور أو جعل النظام أكثر عرضة للدخول في المستقبل أو ببساطة تدمير البرامج أو البيانات الموجودة على القرص الثابت. يشبه حصان طروادة الفيروس، إلا أنه لا يكرر نفسه. وهو يبقى في الكمبيوتر لإحداث الضرر أو السماح لشخص ما من موقع بعيد بالسيطرة على جهاز الكمبيوتر. تتسلل أحصنة طروادة في كثير من الأحيان كملحق مع لعبة مجانية أو أداة أخرى.[1]

---

[1] هو جهاز صمم لاغراض نبيلة لمعرفة ما يقوم به الأبناء أو الموظفين على جهاز الحاسب في غياب الوالدين أو المدراء وذلك من خلال ما يكتبوه على لوحة المفاتيح إلا أنه سرعان ما أسي استخدامه.

ثالثا: ستورم بوتنت:

ستورم بوتنت هي شبكة من حواسيب الزومبي، أي البوتنت، المرتبطة فيما بينها بالستورم وورم والتي يتم التحكم بها عن بعد، وهي نوع من حصان طروادة الذي ينتشر عن طريق البريد الإلكتروني.

في عام ٢٠٠٧، كان يعمل الستورم بونيت على ما بين مليون وخمسون مليون جهاز حاسوب مما يعادل ٨٪ من البرمجيات الخبيثة العاملة ضمن أجهزة ويندوز .وانكفاء انتشار البوتنت حتى وصل إلى ٨٥ ألف حاسوب عام ٢٠٠٨. لم يعرف مصدر هذا البوتنت أو من طوره وله كفاءه عالية في إخفاء نفسه كما يملك خاصية حماية نفسه من التحكم به أو بحديد مساره أو مصدره. كما تصميمه يجعله القيام بعمليات حسابية تفوق قدرة أسرع الحواسب الفائقة وتعتبر مكتب الاستخبارات الفدرالي الأميركي أن هذا الوت نت خطرا كبيرا علة المصارف وفي عمليات الاحتيال وسرقة المعلومات الشخصية للمستخدمين.[1]

رابعا: شبكة الروبوت بالإنجليزية (Botnet)

هي مجموعة ضخمة (يبلغ تعدادها بالآلاف وقد يصل للملايين) من الأجهزة التي تم اختراقها عن طريق الإنترنت كل واحد منها يسمى بوت تخدم مكون البوتنت أو ما يسمى بسيد البوت .(Bot Master) يستخدم سيد البوت قناة أوامر وتحكم (Command and Control Channel C&C) لإدارة شبكته وتنفيذ هجماته، وتسمية البوتنت هذه مشتقة من كلمة (Robot Network) أي شبكات الروبوت حيث أن الأجهزة تخدم سيد البوت دون اختيارها، تماماً مثل أجهزة الروبوت. وبمجرد أن ينضم الجهاز لشبكة الروبوت فإن سيد البوت يستطيع التجسس على صاحب الجهاز دون أن يشعر بذلك، ويستطيع خداعه والاحتيال عليه بهذه الطريقة الماكرة.

ثانيا: أساليب الاحتيال الالكتروني

---

[1] غودين، شارون، (سبتمبر ١٨, ٢٠٠٧. "Storm Worm Botnet Attacks Anti-Spam Firms" . InformationWeekمجلة إنفورمايشون وكذلك راجع ، دنيس فيشر (٢٠٠٧-١٠-٢٢ "Experts predict Storm Trojan's reign to continue يتنباء الإختصاصيون باستمرار الستورم) Search Security ."(مجلة سيكيوريتي سيرتش)

تتعدد الوسائل المستخدمة في الاحتيال الالكتروني وسنذكر فيما يلي أهمها:-

١. الاحتيال من خلال الرسائل الإلكترونية:

يعد البريد الإلكتروني من وسائل الاتصال الحديثة الهامة التي تقدمها شبكة الانترنت للاتصال بين الأفراد والشركات والهيئات، فقد أصبح الآن ممكنا لشخص ما أن يرسل لآخر رسالة إلكترونية عبر الانترنت.[2]

وبتطور البريد الإلكتروني، تم استهداف المستخدمين عن طريق أساليب احتيال الكترونية عالمية تهدف إلى جمع المعلومات الشخصية والمالية الهامة من الضحايا، وهذه الحيل تأتي على شكل عروض غير شرعية عن طريق رسائل بريد الكتروني تشجع المستخدمين على شراء سلع أو خدمات شعبية بأسعار مخفضة (أو قبل أن تكون متاحة لعامة الناس)، مع عدم وجود أي نية لتسليم هذه المشتريات، عادة، ويتم تصميم رسائل البريد الإلكتروني هذه بشكل أساسي للحصول على معلومات بطاقات الائتمان أو الحساب المصرفي.

كذلك فإن رسائل الاحتيال الإلكترونية قد تأتي في شكل طلب مساعدة يقدم عادة مبلغ كبير من المال أو مكافآت مغرية في مقابل مساعدة مالية "قصيرة المدى، وكأحد الأمثلة الشائعة مثلا أن يطلب "المرسل" من المتلقي توفير رقم حساب مصرفي من أجل الاحتفاظ بمبالغ كبيرة من المال حتى يتمكن "المرسل" من استردادها. في المقابل، هو وعد المستلم بالحصول على نسبة مئوية من المبلغ. ويقوم "المرسل" باستخدام رقم الحساب المصرفي لنشاط احتيالي، ولن يحصل المستلم على أي من الأموال الموعودة أبدا.

٢. الاحتيال عن طريق الحصول على عنوان البريد الالكتروني:-

المحتالون لن يستهدفوا شخصاً بعينه، ولكنهم يقومون بإرسال آلاف الرسائل الإلكترونية إلى عناوين بشكل عشوائي، على أمل أن ينجحوا في الاحتيال ولو على القليل منهم. كما أنهم يبحثون على صفحات الانترنت على عناوين صحيحة ليستفيدوا منها، ثم يتبادلون هذه المعلومات مع بعضهم البعض لمعرفة إذا كانت قد نشرت في أي وقت مضى على منتدى الانترنت، أو إذا تم نشر شيء على شبكة الإنترنت، فهناك فرصة

---

[2] حجازي، عبدالفتاح بيومي، الأحداث والانترنت، دراسة متعمقة عن أثر الانترنت في انحراف الأحداث، دار الكتب القانونية، القاهرة، ٢٠٠٧م ص ١٦٨ وما بعدها.

جيدة بأن يستخدم عنوانك في الاحتيال، إذا كنت قد تعرّضت للاحتيال من قبل، فإن عنوانك بشكل طبيعي سيضاف الى قائمة " الضحايا السهلة " ومن المحتمل أن تتلقى المزيد من عمليات الاحتيال.[1]

٣. التصيد الالكتروني (Phishing) :

التصيد هو نوع من أنواع احتيال الهندسة الاجتماعية، حيث يحاول المهاجم ملاحقة ضحاياه ودفعهم لتقديم معلومات قيمة، ومن أبرز وسائل هجمات التصيد الرسائل الإلكترونية، حيث يصمم المهاجم رسالة تبدو وكأنها من جهة موثوقة بالنسبة للمستقبل، وقد تكون الرسالة من بنك معين، أو على شكل تحذير من حادثة أمنية معينة، أو إرسال رابط يطالب المستخدم باستعادة كلمة المرور، وتشير بعض الإحصائيات قبل سنوات عدة، إلى أن بعض خدع التصيّد هذه انطلت على 5%من مستقبلي هذه الرسائل، وعددهم مليونا مستخدم، تم خداعهم ليقوموا بإفشاء معلوماتهم السرية لمواقع مصرفية مزيفة ومواقع بطاقات الائتمان، ما تسبب لهم بخسائر مادية مباشرة، قدرت بنحو ١,٢ مليار دولار أميركي[١].

وتستخدم رسائل الاحتيال الإلكترونية من قبل المجرمين للخداع من خلال مواقع مزيفة، تشبه المواقع الأصلية للمؤسسات المالية، وتطلب منكم الكشف عن معلوماتكم الشخصية مثل رقم الحساب ورقم بطاقة الائتمان والرقم السري ورقم التعريف الشخصي وغيرها من المعلومات.

وأكثر الأنواع شيوعا من رسائل التصيد الإلكتروني تلك التي تظهر على شكل رسالة أمنية تطلب من مستقبليها تأكيد التفاصيل الشخصية أو توجه لهم أسئلة أمنية، ويتم بعد ذلك إرسال التفاصيل التي قمتم بتأكيدها إلى المجرمين، ومن ثم فيقود الرابط إلى صفحة تبدو وكأنها تابعة لموقع إلكتروني للبنك، وباتباع المستخدم لهذا الرابط سيكون ملزماً بإدخال اسم المستخدم وكلمة المرور كي يدخل إلى حسابه وإنشاء كلمة مرور جديدة. وما يحصل على أرض الواقع هو تعقب المهاجم للمستخدم لكشف بياناته المصرفية الإلكترونية.

---

[1] الاحتيال الالكتروني بواسطة البريد الالكتروني، موقع سامبا: على الرابط:-https://dxb.samba.com/ar/security-center/security-center/phishing-faqs.aspx

[١] http://www.albayan.ae/science-today/education-com/2014-01-03-1.2032994

جريدة البيان الاماراتية بتاريخ ٣يناير ٢٠١٤.

٤. الاحتيال عبر أجهزة الصراف الآلي:-

من أمثلـــة التلـــاعب والتحايل في منطقتنا العربية التي تحدث بالاحتيال الإلكتروني تلك التي نفذت على عدد قليل من أجهزه الصراف الآلي لعدد من البنوك العاملة، فقد تبين أنه تم التوصل الى عصابة من المحتالين في أُمور الكمبيوتر تمكنت من إدخال جهاز قارئ إلكتروني في فتحة إدخال البطاقة في ستة من أجهزة الصـــرف الآلي وتمكنت من خلال هذا الجهاز من تسجيل بيانات مجموعة من البطاقات وقد حُدِدَت الخسارة بِـــ ١,٦ مليون درهم إلى تاريخ إصدار البيان.[1]

٥. الاحتيال بوسيلة مسح البطاقات:

يقوم المجرمون في هذه الوسيلة بتركيب أجهزة على جهاز الصراف الآلي للحصول على تفاصيل حساب البطاقة وتسجيل الرقم السري الذي قام العميل بإدخاله. ثم يتم استخدام هذه المعلومات لإجراء عمليات سحب نقدي غير مشروعة باستخدام بطاقات مزورة، وساعدت بيئة تكنولوجيا المعلومات على ابتكار كافة وسائل الاحتيال والخداع والتخفي أثناء ممارسة هذه الأنشطة، فمنها ما يتعلق ارتكابه بشكل مباشر بالبطاقة أو مستندات استخراجها أو التاجر أو البنك، ومنها ما يتم ارتكابه بشكل غير مباشر مستهدفاً بيانات البطاقة لدى حاملها أو البنك المصدر لها.[2]

٥. الاحتيال بالتتبع البصري لمستخدمي بطاقات الصرف الآلي:

وذلك بالنظر من أعلى الكتف بحيث يتظاهر المجرمون بمساعدة العملاء في استخدام أجهزة الصراف الآلي، ولكنهم في الواقع يحفظون الرقم السري بهذه الطريقة.

٦. الاحتيال عن طريق إدارات النقد التشغيلي:-

---

[1] (البنك المركزي الإماراتي، ٢٠٠٣) بيان صحفي عن مصرف الإمارات العربية المتحدة المركزي في اجتماعه بتاريخ ٢٠٠٣/٦/٢٢.

[2] محمد، نجاح فوزي ، "وعي المواطن العربي تجاه جرائم الاحتيال ، "بطاقات الدفع الالكتروني نموذجاً" ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، ١٤٢٨ هـــ ، ٢٠٠٧ م، ص٩٥.

ويتم الاحتيال بهذه الطريقة في الوجهات السياحية التي يوجد فيها عدد قليل من البنوك وأجهزة الصراف الآلي حيث يعرض المجرمون تقديم خدماتهم على السياح بتوجيههم إلى تجار معنيين يستخدمون أجهزة نقاط البيع لإصدار النقد، ويقوم التاجر بمسح تفاصيل حساب البطاقة ويستخدم جهاز مزيف للحصول على الرقم السري لحاملي البطاقات، ثم يتم استخدام هذه المعلومات لإجراء عمليات سحب نقدي غير مشروعة باستخدام بطاقات مزورة.

٧. الاحتيال عبر الرسائل النصية القصيرة (Smashing) :

الاحتيال عبر الرسائل النصية القصيرة (Smashing) هو عبارة عن هجوم أمني يتم من خلاله خداع المستخدم على الهاتف النقال أو غيرها من الأجهزة المحمولة الأخرى، عبر عملية احتيال متقدمة يتم فيها استخدام تكنولوجيا الجيل الجديد لإقناع أصحاب الهواتف بأنهم قد ربحوا جائزة يانصيب أوروبية، وذلك في محاولة للحصول على بعض التفاصيل الشخصية مثل رقم الحساب المصرفي ورقم بطاقة الائتمان.

ولقد كثرت أساليب الخداع التي يوهم أصحابها المستخدمين بفوزهم بجوائز مالية قيّمة من غير مرجعية أساسية لها، حيث بيّنت بلاغات عديدة بأنها جوائز وهمية تستهدف إمّا الاستيلاء على الرصيد المالي أو الدخول في شبكة معقدة من الاتصالات والرسائل الهاتفية الخادعة، والتي تنتهي في النهاية باستنزاف مبالغ مالية من غير عائد حقيقي ومثالا لذلك فقد سجلت 365 قضية نصب هاتفي تعاملت معها شرطة أبوظبي في ٢٠١٢م فقط.

وتشير العديد من العوامل إلى أن هذه العملية الاحتيالية تعد متقدمة وغير مسبوقة، فبالرغم من أن الجهات المختصة قد قامت بحجب الأرقام الأصلية بعد تتبعها، إلا أن المحتالين قاموا بتغيير الأرقام مرة ثانية أرسلوا رسائل نصية أخرى إلى العملاء.

٨. سرقة الهوية:

تحدث سرقة الهوية حينما يسرق شخص ما معلوماتك الشخصية ويستخدمها للادعاء بأنه أنت دون علمك، وتحدث هذه السرقة عندما يحصل أحد المجرمين على المعلومات الشخصية لبعض الأشخاص، وذلك لسرقة المال من حساباتهم، بفتح بطاقات ائتمان جديدة، وطلب الحصول على قروض، وتقع جريمة تزوير الهويات

الخاصة للأفراد أو للأشخاص الاعتبارية للمواقع والشركات، استغلالًا للنفوذ والشهرة والثقة الاعتبارية لكثير من الشخصيات والمواقع .[1]

المبحث الثاني

السمات الخاصة بمرتكبي جرائم الاحتيال الإلكتروني

تمهيد وتقسيم:

تعتبر الجريمة المعلوماتية محصلة تعاون وعمل بين مجموعة من العوامل تتمثل في فقد المعلومات والاعتداء على سلامة النظام والمال المادي والمعنوي باستخدام تقنية الأنظمة المعلوماتية ، فضلاً عن الأحداث الطبيعية التي تهدد النظام المعلوماتي والتي يطلق عليها مخاطر المعلوماتية. ومن الطبيعي أن يكون الشخص مرتكب جرائم الاحتيال المالي ، على دراية كافية بمعطيات الحاسب الآلي ، ولكن يتوقف أسلوب ارتكاب الجريمة على مدى ثقافة ومهارة هذا الشخص بالنسبة لبرامج وشبكات الحاسب ، والشخص مرتكب جرائم الاحتيال المالي أو جرائم المعلوماتية رغم أنه يتميز ببعض السمات الخاصة ، إلا أنه في النهاية لا يخرج عن كونه مرتكباً لفعل إجرامي يتطلب توقيع العقاب عليه ، كل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين. فالمجرم المعلوماتي ينتمي في أكثر الحالات إلى وسط اجتماعي متميز ، كما أنه على درجة من العلم والمعرفة ، وإن كان ليس من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي ، إلا أنه دائماً يبرر الجريمة ، بل إنه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق.

وسنتنازل هذا المبحث من خلال مطلبين:

المطلب الأول: شخصية المجرم المعلوماتي وخصائصه

---

[1] الصاعدي، سلطان مسفر مبارك ، الشبكات الاجتماعية خطر أم فرصة، الألوكة، ٢٣ أبريل ٢٠١٢، متاحة على الرابط التالي: http://www.alukah.net/publications_competitions/0/4040/

المطلب الثاني: أنماط المجرم المعلوماتي ودوافع ارتكاب الجريمة

المطلب الأول

شخصية المجرم المعلوماتي وخصائصه

الجريمة المعلوماتية وارتباطها بمجرم معين له مواصفات ومؤهلات معينة تمكنه من التلاعب بالمواقع الالكترونية والانترنيت وقد انتشر التعامل مع الانترنيت بما زاد عدد مجرمي المعلومات وأصبحت الجريمة المعلوماتية في تنامي مقارنة بالجرائم التي كانت سائدة قبل ظهور الانترنيت، وقد ثبت من خلال الإحصائيات العالمية أن معدلات الجرائم وحالات الانتحار في أمريكا وأوروبا قد انخفضت بعد اتساع قاعدة المشتركين في شبكة الإنترنت.[1]

أولا: شخصية المجرم المعلوماتي:

المجرم المعلوماتي شخصية جديدة في عالم الجريمة ، فهو ليس مجرد سارق أو محتال عادي ، ولكنه مجرم ذو مهارات تقنية عالية ، ملم بالإمكانيات المستخدمة في النظام المعلوماتي ، قادر على استخدام هذه الإمكانيات في اختراق الشفرة السرية للنظام لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات ، فشخصية المجرم المعلوماتي وميكانيكية ارتكابه للجريمة لها سماتها الخاصة بهذا النوع الجديد من الإجرام ، لذلك هو يمثل بالنسبة للمجموعات التقليدية للإجرام شخصية مستقلة بذاتها ، فهو من ناحية إنسان ذكي ، ومن ناحية أخرى إنسان اجتماعي.

---

[1] الصغير، جميل عبد الباقي، الانترنت و القانون الجنائي ، دار النهضة العربية ، القاهرة ، ٢٠٠١ ، ص١٣ وما بعدها.

- المجرم المعلوماتي إنسان ذكي:

إجرام المعلوماتية هو إجرام الأذكياء ، بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف ، فإذا كان من السهل تصور العنف في الإجرام الموجه ضد مكونات النظام المعلوماتي المادية والذي يحدث غالباً في إطار العمليات الإرهابية ، فإنه لا يمكن أن يتصور أن يكون هناك أي عنف في الإجرام الموجهة ضد المكونات المنطقية والبيانات ، وبالتالي يجب أن يكون المجرم على دراية كافية بأنماط الجريمة ، فهناك أنماط مختلفة يمكن استخدامها في التلاعب في هذه البيانات مثل "القنابل المنطقية" والتي بمقتضاها يتم زرع تعليمات في برنامج مزود بعداد ، وعندما يصل إلى بداية معينة تنطلق هذه التعليمات لكي تمحو البرنامج ، كما أن هناك أنماط أخرى تعرف بالفيروسات المعلوماتية ، وهي عبارة عن برنامج من الحجم الصغير الذي يصعب اكتشافه ، ويوضع في اسطوانة ثم يقوم بنسخ نفسه بداخل النظام لتدميره في فترة وجيزة.

- المجرم المعلوماتي إنسان اجتماعي:

هناك أشخاص يرتكبون الجرائم المعلوماتية ليس بدافع الحصول على مال ، بل يكون الدافع اجتماعي ، كدافع اللهو أو لمجرد إظهار تفوقهم على النظام المعلوماتي ، أو على البرامج المخصصة لأمن النظام ، وهم لا يحصلون على أي منفعة مادية من جرائمهم ، ولكن يكتفون بالتفاخر بأنفسهم أو أن يُظهروا لضحاياهم ضعف أنظمتهم ، وفي الغالب ما يتسبب هذا التصرف في أضرار جسيمة للنظام ، ولو لم يكشف عن أي عداء للمجتمع، مستفيدين من الامكانيات المتاحة لعملية التصحيح والتعديل والمحو والتخزين والاسترجاع والطباعة ، وهي بذلك علاقة وثيقة بارتكاب الجريمة. [1]

ثانيا: خصائص المجرم المعلوماتي:

قد اختلف الباحثون في تحديد سمات المجرم المعلوماتي، كما ثبت عدم جدوى النظرة التقليدية للمجرم المعلوماتي التي سادت في كتابات الباحثين لفترة من الزمن فمجرمي المعلومات ليسوا دائما مجموعة من النوابغ الذين لا يمكن

[1] العريان، محمد على، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، ٢٠٠٤ ، ص٣٧ .

التنبــؤ بهــم أو معرفتهــم، ويتميز المجرم في جرائم الاحتيال المعلوماتية بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ، ويرمز إلى هذه الخصائص بكلمة: SKRAM ، وهي تعني المهارة Skills ، المعرفة Knowledge ، الوسيلة Resources ، السلطة Authority ، وأخيراً الباعث Motives .

- المهارة **Skills**:

الجريمة المتعلقة بالحاسب الآلي هي جريمة من الصعب أن يرتكبها شخص دون أن تكون لديه المقدرة على اختراق برامج وشبكات الحاسب ، وهذا التعدي يحدث نتيجة الإلمام بالتقنيات الحديثة ، وأدوات الحاسب ، والقدرة على المهارة في مراوغة التحصينات وبرامج أمن المعلومات التي تقف ورائها شركات البرمجة ، والمهارة والخبرة هما اللذان يحددان الأسلــوب الذي تتم به جريمة التعدي ، فإذا كان الجاني على قدر ضئيل من الخبرة والمهارة ، فإن الجريمة لا تتعدى أن تكون إتلافاً معلوماتياً ، أو محو للبرامج أو نسخها ، أما إذا كان الشخص على درجة كبيرة من المهارة والخبرة فإنه يعتبر في مقدمة المحترفين الذين يهددون نظام الحاسب الآلي ، لاستطاعته الوصول إلى الأنظمة المحصنة ضد الاختراق ، وارتكاب جرائم السرقة ، والاحتيال ، والتجسس ، وزرع الفيروسات ، والتي يصعب على الهواة فعلها.[1]

وتنفيذ الجريمة المعلوماتية بصفة عامة يتطلب قدراً من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين ، إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال أو أن تكون لديه خبرة كبيرة فيه ، بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

- المعرفة **Knowledge**:

---

(1) Cornwall (Hugo), Datatheft, Computer Fraud, Industrial Espionage and Information Crime, Heinemann: London 1987, p 134

وهي التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها ، وإمكانيات نجاحها واحتمالات فشلها ، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على المحيط الذي تدور فيه ، حتى لا يواجهون بأشياء غير متوقعة من شأنها إفشال أفعالهم أو الكشف عنهم ، وتميز المعرفة بمفهومها السابق مجرمي المعلوماتية ، حيث يستطيع المجرم المعلوماتي أن يكون تصوراً كاملاً لجريمته ، ويرجع ذلك إلى أن المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي ، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.[2]

- الوسيلة **Resources**:

وهي الإمكانيات التي يتزود بها المحتال لإتمام جريمته ، والوسائل المتطلبة للتلاعب بأنظمـــة الحاسبات الآلية هي في أغلب الحالات تتميز نسبياً بالبساطة وبسهولة الحصول عليها ، فالمجرم المعلوماتي يتميز بقدرته على الحصول على ما يحتاج إليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الإجرامي ، والحقيقة أنه كلما كان نظام الحاسب الآلي الذي يحتوي على المعلومات المستهدفة غير مألوف ، كانت الوسائل أكثر صعوبة في الحصول عليها ، لاقتصارها على عدد قليل من الأفراد هم عادة القائمون على تشغيل النظام ، وذلك على عكس الأنظمة الشائعة الاستعمال (برامج مايكرو سوفت على سبيل المثال).[1]

- السلطة **Authority**:

ويقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته ، فكثير من مجرمي المعلومات لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة ، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات ، والتي تعطي الفاعل مزايا متعددة ، كفتح الملفات وقراءتها وكتابتها ومحو أو تعديل المعلومات التي تحتوي عليها ، وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن

---

[2] الزهراني، شيخة حسين، الطبيعة القانونية للهجوم السبراني وخصائصه، مجلة جامعة الشارقة للعلوم القانونية، كلية القانون، جامعة الشارقة، المجلد ١٧، العدد ١، ٢٠٢٠، ص ٧٨٢.

[1] قورة نائلة ، المرجع السابق، ص ٥٨ .

التي تحتوي على أنظمة الحاسبات الآلية ، وقد تكون السلطة التي يتمتع بها الجاني غير حقيقية كما في حالة استخدام شفرة الدخول بشخص آخر.[2]

- الباعث **Motives:**

الباعث وراء ارتكاب الجريمة المعلوماتية لا يختلف عن الباعث في ارتكاب أي جريمة أخرى ، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمـــة المعلوماتية ، ثم يأتي بعـــد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله ، وأخيراً الانتقام من رب العمل أو أحد الزملاء.

المطلب الثاني

أنماط المجرم المعلوماتي ودوافع ارتكاب الجريمة

أولا: أنماط المجرم المعلوماتي

يتسم المجرم المعلوماتي وخاصة في مجال التجارة الإلكترونية بعدة صفات تميزه عن غيره من الجناة أو المتورطين في أشكال الإنحراف أو الإجرام الأخرى، ويعتبر الشخص الذي يقوم بارتكاب جرائم الاعتداء على برامج وشبكات الحاسب الآلي ، بقصد تحقيق هدف غير مشروع ، من الأشخاص الذين يتوافر فيهم مستوى فني وتقني عالٍ للتعامل مع هذه المعطيات ، لذا فإن الفعل الإجرامي المرتبط بالحاسب الآلي يتوقف على شخصية المجرم ودوافعه،[1] لذلك تتعدد أنماط الأشخاص الذين يحاولون اختراق شبكات وبرامج الحاسب الآلي إلى عدة تصنيفات ، وجميعها تعتمد على مدى إلمام الشخص بمهارات وفن التعامل مع الحاسب الآلي ، ولا يعني ذلك بطبيعة الحال أن كل مجرم يندرج تحت تصنيف محدد دون غيره ، بل يمكن أن يكون المجرم الواحد مزيجاً من أكثر من تصنيف:

- المحترفون **Hackers:**

---

[2] الزهراني، شيخة حسين، المرجع السابق، ص٧٨٣.

[1] الصلاحي، مفيد عبدالجليل، صفات المجرم المعلوماتي في الجرائم الالكترونية، ٢٠١٨، ص١ .

(الهاكرز) هو مصطلح في اللغة الإنجليزية يطلق على الشخص المتخصص في نظم المعلومات والبرمجيات ، والقادر على ابتكار البرامج والتعامل مع شبكات الحاسب الآلي ، وحل جميع المشاكل المتعلقة به ، وإتقان لغات البرمجة المعروفة. وقد بدأ ظهور الهاكرز أثناء الحرب العالمية الثانية ، عندما كانوا يعملون مع الجيوش لفك شفرات إشارات الأجهزة اللاسلكية للجيوش الأخرى ، ثم انتشروا بعد اختراع الحاسب الآلي لتطوير وابتكار برامج التشغيل.

ومع بداية الثمانينات وانتشار الشبكات وارتباطها بأجهزة الحاسب الآلي ، تحول عدد من المبرمجين إلى مجرمين متمكنين باستغلال إمكانياتهم وخبراتهم في مجال تقنية المعلومات ، لأغراض شخصية مخالفة للقانون ، كالتسلل إلى الأنظمة المعنية والحصول على المعلومات السرية منها ، أو تخريب نظام معين وإلحاق خسائر به بقصد الانتقام أو الايتزاز ، ومنذ ذلك الحين والقوانين والأجهزة الأمنية تلاحق من يطلق عليهم الهاكرز ، وبرغم أن وصف الهاكرز يطلق على كل من يقوم بأداء غير مشروع على برامج وشبكات الحاسب الآلي ، فإن هناك أنواعاً تختلف عن الهاكرز ولكنها تتدرج تحت وصفها ، وهو ما يسمى جميعهاً بالمجتمع السفلي للحاسب الآلي Underground Community.

- المخترقون **Crackers:**

(كراكرز) كلمة مستمدة من الفعل الإنجليزي Crack وتعني الكسر أو التحطيم ، وهي الصفة التي يتميز بها هذا النوع ، فهم يستخدمون برامج التقنية ، في محاولات لاختراق الأنظمة والأجهزة للحصول على المعلومات السرية ، أو القيام بعمليات تخريبية معينة ، كاختراق مزودات الشركات لحذف وإضافة المعلومات أو لمجرد الاطلاع عليها ، أو للدخول إلى مزود خدمة الانترنت والتلاعب بمحتويات الصفحة في موقع ما ، أو الاستيلاء على أرقام البطاقات الائتمانية واستخدامها ، وكذا القيام بمحاولة إزالة أو فك الحماية التي تصنعها شركات إنتاج البرمجيات على برامجها لمنع عمليات النسخ غير القانوني ، ومن يتميز من هذه الفئة يطلق عليهم القراصنة Pirates.

ويدخل في هذا النوع من التصنيف نوعان من المجرمين:

- **الأول: المحترفون Hackers:** وهم من يحملون درجات جامعية عليا في تخصص الحاسب والمعلوماتية ، ويعملون في مجال نظم المعلومات والبرمجة ، ويكونون على دراية ببرامج التشغيل والثغرات الموجودة بها.

- **الثاني: الهواة Pranksters:** وهم الهواة الذين لديهم هواية قوية في تعلم البرمجة ونظم التشغيل ، فيظل مستخدماً للبرامج والتطبيقات الجاهزة ولكنه يطورها حسبما تقتضيه حاجته ، وساعد على دخولهم في مجال الاختراق انتشار البرامج المساعدة الجاهزة ، وسهولة التعامل معها ، ومن الهواة من هو خبير بالأجهزة فلا يسبب ضرراً عشوائياً بالجهاز ، ومنهم المبتدئ الذي يعتبر أخطر أنواع الكراكرز ، لأنه يستخدم برامج الهجوم دون أن يفقه تطبيقها ، وتكون النتيجة دماراً واسعاً دون أن يدرك نتيجة فعله.

- المتسللون **Phreaks**:

وهم الذين يحاولون التسلل عبر الشبكات الهاتفية اعتماداً على أساليب تقنية غير قانونية ، والتحكم بها ، مستخدماً أدوات خاصة مثل مولدات النغمات الهاتفية ، ومع استخدام شركات التليفون البدالات الرقمية الديجيتال ، تحول هذا النوع إلى استخدام الأساليب البرمجية ذاتها التي يستخدمها الكراكرز ، وقد تمكن محتال من الدخول إلى جهاز شخصي لإحدى الفتيات أثناء اتصالها بشبكة الانترنت ، وأخذ يشاهد ما يحتويه من صور وملفات ، ثم لفت نظرة أن الكاميرا موصلة بالجهاز فأصدر أمر التصوير للجهاز ، وأخذ يشاهدها وهي تستخدم الجهاز ، ثم أرسل إليها رسالة واصفاً إياها بأنه يشاهدها ، كنوع من التحدي وإثبات المهارة في تعامله مع هذه التقنيات.

- العابثون بالشفرات **Cypherpunks**:

يقــوم بعض المجرمين بمحاولة الحصول على أدوات وقواعد التشفير المعقدة والقوية ، وفك الشفرات وبيعها أو توزيعها مجاناً لمن يرغب ، وقد تستخدم هذه القواعد بصورة غير قانونية ، كتبادل المعلومات بين شبكات الإجرام المنظم.

- مؤلفو الفيروسات **Malicious Hackers**:

ويعتبر هذا النوع من مجرمي المعلوماتية من أخطر الأنواع المنتمية إلى "المجتمع السفلي" للحاسب الآلي ، لأنه يقوم بتصميم برامج لها أضرار جسيمة في أجهزة الحاسب الآلي ، لا لشيء إلا الرغبة في التخريب ، مما يعتبره المحللون النفسيون أنهم مصابون بمرض عقلي أو نفسي ، لأنه لا يجني أي فائدة شخصية نتيجة فعله.

- الفوضويون **Anarchists**:

وهم الأشخاص الذين يقومون بنشر معلومات على شبكة الانترنت بهدف الترويج لمعلومات مخالفة للقانون ، مثل طرق توزيع وصناعة المخدرات ، أو كيفية صنع المواد المتفجرة ، أو تعليم القواعد الخاصة بالقرصنة ، حتى يستطيع اختراق أجهزة وشبكات الحاسب ، وغيرها من المعلومات الإجرامية ، كذلك ما يقوم به البعض من نشر معتقدات وأفكار اجتماعية أو سياسية أو دينية ، ويرغبون في فرضها باللجوء إلى التهديد والوعيد عبر شبكة الانترنت.

ثانيا: دوافع ارتكاب الجرائم المعلوماتية:

تختلف الأغراض والدوافع التي تحث المجرم المعلوماتي على ارتكابه الجريمة المعلوماتية ، وهذا يتوقف على مدى ثقافته وخبرته في مجال الحاسب الآلي ، ولكنها قد تتفق مع الدوافع الخاصة بالجريمة التقليدية ومنها السرقة والنصب والتزوير ، وجميعها تهدف إلى تحقيق مكاسب غير شرعية ، ومن أهم هذه الدوافع:

- تحقيق مكاسب مادية:

يقوم بعض مرتكبي هذه النوعية من الجرائم ، بارتكاب فعلتهم بهدف تحقيق مكاسب مادية ، ولكن يلزم في ذلك أن يكون لديهم المهارة في التعامل واختراق أنظمة المواقع المراد اختراقها ، فقد تمكن أحد القراصنة من سرقة معلومات عن بطاقات الائتمان الخاصة ب ١٥٧٠٠ عميل من على موقع Western Union عام ٢٠٠٠ واستخدمها في شراء السلع والخدمات من خلال شبكة الانترنت.

- إثبات المهارة الفنية:

قد يقوم بعض الأشخاص بمحاولات ارتكاب جرائمهم ، بهدف إثبات قدرتهم على اختراق أنظمة الحاسب ، وتفوقهم العلمي والمعرفي في تقنيات هذه التكنولوجيا ، وأنهم أصبحوا أكثر ذكاء من مبرمجيها ومخترعيها. وغالباً ما يكون هذا الدافع عند الصبية والشباب ، والمعروفين بنوابغ المعلوماتية ، فهم لا يهتمون بما قد يحدث بسبب أفعالهم ، وإنما هدفهم تخطي حواجز الحماية الخاصة بأنظمة الحاسبات ، وقد يكتشف أحدهم نقطة ضعف أمنية في أحد الأنظمة ، فيتم تناقلها بين أصدقائه بهدف الدعاية.

- ارتكاب الجريمة بهدف الترفيه والتسلية:

قد يقوم مرتكب الجريمة بارتكاب فعل إجرامي ، بهدف الترفيه عن نفسه ، أو التسلية بمحاولة الدخول في منافسة مع الآخرين ، كمن يستولي على أرقام بطاقات الائتمان ثم يقوم بلعب القمار على مواقع الانترنت ويقوم بالدفع من حساب الآخرين ، أو الدخول إلى مواقع ترفيهية يُشترط دفع اشتراكات فيها ، فيقوم بتحويل أموال إليها من حسابات الغير.

- الرغبة في الإضرار:

قد يرغب البعض في الإضرار ببعض الشركات والمؤسسات التي تتنافس معها في نفس المجال ، بهدف إضعافها ومنع سيطرتها على السوق ، وقد يلجأ البعض إلى الانتقام من المؤسسة أو الشركة التي كان يعمل بها لطرده من العمل ، كما قد يرغب بعض محترفي برمجة الحاسب إلى الإضرار بالآخرين ، مثل ما قام به أحد الأشخاص من الاستيلاء على البريد الإلكتروني لإحدى الفتيات من خلال شبكة الانترنت ، منتحلاً شخصيتها في إرسال رسائل بريد الكتروني لكل قائمة مراسلاتها ، تحتوي على عبارات وألفاظ جنسية خارجة ، الأمر الذي ترتب علية أضرار أدبية ومادية جسيمة لها ، وتم ضبطه الجاني عن طريق جهاز ADSL المرتبط بالخط التليفوني لمنزله.

الخاتمة

يتضح من خلال مجريات الدراسة أن جرائم الاحتيال الالكتروني من أكثر الجرائم تطوراً ، فهي تساير التقدم الحضاري ، وتستفيد من التقدم العلمي والتقني ، وتعتمد على ذكاء المجرم ، وجشع المجني عليه كما تغيرت جريمة الاحتيال ، من الاحتيال على البسطاء لسلب أموالهم القليلة ، وباستعمال مظاهر خادعة بسيطة ، إلى الإدعاء بامتلاك مشروعات وهمية تدار من خلال مظاهر خارجية يحرص المحتالون على إكسابها صورة المظهر المشروع بوجود وثائق ومقار وغيرها من الأمور التي تُكسب الثقة، ويربط بين جرائم الاحتيال الحديثة استغلالها التقدم العلمي والتقني في ارتكابها ، فكان الاحتيال الالكتروني هو الأداة المساعدة في ارتكاب هذه الجرائم ، عن طريق استخدام الحاسبات الآلية ، والانترنت ، وآلات الدفع الالكتروني ، والهاتف المتحرك ، إما باستعمالهم كأداة أساسية في ارتكاب الجريمة ، أو باستخدام برامج خبيثة تعطل أو تُتلف شبكات المعلومات.

ومن خلال الدراسة برزت عدة نتائج وتوصيات توصل لها الباحث

النتائج:

١. نتيجة للتطور الكبير في تقنية الاتصالات وعلى الأخص شبكة الانترنت ثارت تحديات كبيرة في أنشطة المكافحة والتحقيق والمحاكمة في جرائم الاحتيال الالكتروني والوصول إلى مرتكبيها ومعاقبتهم، كما

ثارت تحديات كبيرة من الناحيتين القانونية والفنية بشأن التفتيش والضبط وكيفية التعامل مع الأدلة غير المادية المتعلقة بهذه الجرائم، فجهات التحقيق اعتادت على أن يكون الإثبات ماديا وملموسا، ولكن في مجال شبكة الانترنت لا يستطيع المحقق تطبيق إجراءات الإثبات التقليدية على المعلومات والصور ذات الطبيعة المعنوية على شبكة الانترنت، فهذه الجرائم لا تترك آثارا مادية على مسرح الجريمة كالجرائم التقليدية، كما أن مرتكبيها يملكون القدرة على إتلاف الأدلة بشكل يسير.

٢. عدم فاعلية قوانين العقوبات التقليدية وضعفها في مواجهة تلك الجرائم عبر شبكة الانترنت والحاجة إلى إصدار قوانين فعالة لمواجهة الجرائم المعلوماتية بشكل عام والجرائم الاحتيالية عبر شبكة الانترنت بوجه خاص.

٣. وجود ضعف ونقص تشريعي في مكافحة تلك الجرائم عبر الانترنت في غالبية الدول العربية.

٤. الطبيعة العابرة للحدود لتلك النوعية من الجرائم عبر شبكة الانترنت مما يترتب عليه ارتكاب الفعل الجرمي في دولة معينة بينما تتحقق آثار هذا الفعل في دولة أو دول أخرى مما يثير مشكلة تحديد الاختصاص القضائي والقانون الواجب التطبيق.

التوصيات:

١. دعوة الجهات المعنية إلى إحكام الرقابة على الانترنت للحد من جرائم الاحتيال الالكتروني التي باتت سريعة الإيقاع في المجتمع وتشكل بؤرة إجرامية كبيرة.

٢. ضرورة فرض نوع من الرقابة على تعامل الأبناء مع وسائل التواصل الاجتماعي، لأن هناك جرائم ترتكب بسبب غياب الرقابة وتوعية الأطفال، بعدم التورط في علاقات مع غرباء عبر الإنترنت، والإفصاح عن معلومات تخصهم.

٣. ضرورة إصدار تشريعات جديدة في كل فترة لمكافحة هذه الجرائم الدخيلة بما يواكب الزيادة الكبيرة في ارتكاب مثل هذا النوع من الجرائم وقصور التشريعات العقابية التقليدية في هذا المجال، وأن تجرم تلك التشريعات كافة أفعال الجرائم الالكترونية.

٤. أهمية إنشاء خطوط ساخنة لتمكين مستخدمي الانترنت من الإبلاغ عن الجرائم التي يتعرضون لها بالاحتيال والابتزاز على الشبكة.

٥. إلزام مزودي خدمة الانترنت بالتحقق من هوية مستخدمي شبكة الانترنت، ومنع مخالفة القوانين واللوائح في حالة وجود مخالفات من قبل بعض أصحاب المواقع.

٦. ضرورة تدريب وتأهيل العاملين في الجهات الأمنية والرقابية والعدلية في تلك النوعية من الجرائم وتخصيص وحدات أمنية لديها المعرفة الكافية بتقنية الحاسب الآلي وشبكة الانترنت، لتكون بمثابة شرطة متخصصة في تعقب مرتكبي مثل هذه الجرائم والوصول إليهم.

المراجع

أولا: المراجع العربية

١. (Ulrich Seiber) – جرائم الحاسب الآلي والجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال، ترجمة الدكتور سامي الشوا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، ٢٥-٢٨، تشرين أول/أكتوبر ١٩٩٣ – والورقة المذكورة بذاتها من أوراق التحضير للمؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات – (البرازيل ٤ – ٩ أيلول ١٩٩٤).

٢. آل علي، فيصل محمود، ٢٠١٩، أثر التقنيات الحديثة على العلاقات الاسرية في مجتمع دولة الامارات العربية المتحدة، جـــــامعـــــة الملك محمد الخامس، كليـــــة الآداب والعلوم الإنسانيـــــة، قســـم علم الاجتماع، بحث مقدم لدرجة الدكتوراه في علم الاجتماع، المغرب.

٣. حجازي، عبدالفتاح بيومي، الأحداث والانترنت، دراسة متعمقة عن أثر الانترنت في انحراف الأحداث، دار الكتب القانونية، القاهرة، ٢٠٠٧م.

٤. حجازي، عبدالفتاح بيومي، مبادىء الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى ، ٢٠٠٦م .

٥. الزهراني، شيخة حسين، الطبيعة القانونية للهجوم السبراني وخصائصه، مجلة جامعة الشارقة للعلوم القانونية، كلية القانون، جامعة الشارقة، المجلد ١٧، العدد ١، ٢٠٢٠.
٦. الصغير، جميل عبد الباقي، الانترنت و القانون الجنائي ، دار النهضة العربية ، القاهرة ، ٢٠٠١ .
٧. الصلاحي، مفيد عبدالجليل، صفات المجرم المعلوماتي في الجرائم الالكترونية، ٢٠١٨.
٨. العريان، محمد على، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، ٢٠٠٤.
٩. قشوش، هدى، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،١٩٩٢.
١٠. قورة، نائلـــة عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، بيروت ، الطبعة الأولى ، ٢٠٠٥.
١١. محمد، نجاح فوزي ، "وعي المواطن العربي تجاه جرائم الاحتيال ، "بطاقات الدفع الالكتروني نموذجاً" ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، ١٤٢٨ هـــ ، ٢٠٠٧ م.
١٢. مليكة، جرجس يوسف ، مكانة الركن المعنوي في الجرائم الاقتصادية ، دراسة مقارنة ، المؤسسة الحديثة للكتاب ، لبنان ، ٢٠٠٥.

ثانيا: المراجع الاجنبية

1. Cornwall (Hugo), Datatheft, Computer Fraud, Industrial Espionage and Information Crime, Heinemann: London 1987, p 134
2. غودين، شارون، (سبتمبر ١٨, ٢٠٠٧ ."Storm Worm Botnet Attacks Anti-Spam Firms". InformationWeek مجلة إنفورمايشون وكذلك راجع ، دنيس فيشر. (٢٢-١٠-٢٠٠٧) "Experts predict Storm Trojan's reign to continue ."(يتنباء الإختصاصيون باستمرار الستورم سيكيوريتي .سيرتش) Search Security (مجلة
3. ٢٠٠٧ "Storm Worm Botnet Attacks Anti-Spam Firms". InformationWeek

4. ٢٢-١٠-٢٠٠٧)"Experts predict Storm Trojan's reign to continue)". Search Security (
5. http://www.albayan.ae/science-today/education-com/2014-01-03-1.2032994
6. Computer Hackers : Tomorrows Torrortsts , Dgnamics , News For And Aboutmembers Of the American Society For Industrial Security, Varyl Febrauary , 1990

ثالثا: المواقع الالكترونية

1. الاحتيال الالكتروني بواسطة البريد الالكتروني، موقع سامبا: على الرابط:https://dxb.samba.com/ar/security-center/security-center/phishing-faqs.aspx
2. http://www.albayan.ae/science-today/education-com/2014-01-03-1.2032994
3. الصاعدي، سلطان مسفر مبارك ، الشبكات الاجتماعية خطر أم فرصة، الألوكة، ٢٣ أبريل ٢٠١٢، متاحة على الرابط التالي: http://www.alukah.net/publications_competitions/0/4040