طبيعة الخطورة الإجرامية للمجرم المعلوماتي

The nature of the criminal risk of the information criminal

تاريخ الارسال: 2019/08/30	تاريخ القبول: 2019/12/15	تاريخ النشر: 2020/06/30

*ط.د. لحرش أيوب التومي
عضو بمخبر الحقوق والعلوم السياسية
جامعة عمار ثليجي - الأغواط
lahrecheayoubtoumi@gmail.com

أ.د. النحوي سليمان
جامعة عمار ثليجي - الأغواط
Simon.taha123@gmail.com

ملخص :

نهدف من خلال هذه الدراسة إلى محاولة تسليط الضوء على نوع خاص من المجرمين لم يعهدهم علم الإجرام كانوا نتاج ظاهرة إجرامية مستحدثة عرفت بإسم الجريمة المعلوماتية, صنعوا فارق كبير بإختلافهم الجذري عن المجرمين العاديين أو التقليديين سواء من حيث المواصفات أو التصنيف أو الدوافع وحتى الأساليب والتقنيات التي يلجؤون إليها لتنفيذ مخططاتهم الإجرامية عبر الشبكات والأنظمة المعلوماتية, غايتنا من ذلك كله وبما أنهم فكرة جديدة على الفقه الجنائي هو إبراز مدى خطورتهم الإجرامية على أمن وسلامة النظم المعلوماتية ومستخدميها خاصة في ظل الإعتماد شبه المطلق على هذه التقنية في كافة مجالات الحياة اليومية للدول والشعوب والمجتمعات.

الكلمات المفتاحية : المجرم المعلوماتي ؛ المواصفات الخاصة ؛ النشاط الإجرامي ؛ الخطورة الإجرامية.

Abstract:

Our goal through this study is to try to shed light on a particular type of criminals that criminology has not known. They ar the product of arecent criminal phenomenon known as computer crime. They are radically different from normal and traditional criminals because of the specificities,

***المؤلف المرسل :** لحرش أيوب التومي

the classification or the motives, even the styles and techniques they use to implement their criminal plans, through networks and information systems. Since this type of crime is a new phenomenon in the criminal field, we will try to highlight the criminal danger on the security of computer systems and its users, including relying almost entirely on this technique in all areas of daily life of the peoples and societies.

Keywords: Informatics criminal ; Special specificities ; Criminal activity ; Criminal danger.

مقدمة :

إن من أهم إنجازات العلم الحديث في هذا العصر وأعظمها جدوى للانسان, ظهور الحاسب الآلي والأنترنت وما حققته تكنولوجيا المعلومات والإتصالات من فوائد عديدة في مجال الرقي والتقدم الإنساني في أغلب مناحي الحياة الإقتصادية والتعليمية والطبية والعديد من المجالات الأخرى.

إلا انه وبالرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات, فإن هذه الثورة التكنولوجية المتنامية حملت في طياتها وكغيرها من الظواهر المستحدثة جملة من الانعكاسات السلبية الخطيرة جراء إساءة إستخدامها والإنحراف عن الغرض المرجو منها, مما أدى الى تفشي ظاهرة إجرامية مستحدثة عرفت بإسم الجريمة المعلوماتية.

رافق هذه الظاهرة الإجرامية المستحدثة بروز طائفة جديدة من المجرمين لم تعهدهم البشرية من قبل عرفوا بإسم مجرمي المعلوماتية وجدوا ضالتهم في العالم الرقمي واتخذوه ملجا لهم, يتمتع هؤلاء المجرمين بالخبرة والحرفية في تطويع هذه التقنية للقيام بأعمال إجرامية أفرزت إلى جانب الجريمة التقليدية جرائم معاصرة بل حولت هذه الجريمة من صفتها العادية وأبعادها المحدودة إلى أبعاد وآفاق جديدة, تعتمد التقنية في تنفيذ الفعل المجرم وبأساليب مبتكرة وطرق جديدة لم تكن معروفة من قبل جرائمهم, وذلك كله بواسطة نقرات بسيطة على لوحة مفاتيح الكمبيوتر ومن على مسافات تتعدى عشرات الآلاف من الاميال, بدون أي عناء او خسائر ودون أن يتركوا وراءهم أثرا ملموسا لملاحقتهم ومعرفة مصدرهم, كل هذا وغيره يدفعنا لطرح الإشكالية التالية: **فيما تتمثل الخطورة**

الإجرامية لهذه الطائفة الجديدة من المجرمين؟ وهو ما سنحاول الإجابة عليه من خلال المباحث التالية:

المبحث الأول : المجرم المعلوماتي مجرم بمواصفات خاصة.

المبحث الثاني : الأساليب والتقنيات الخاصة بالإجرام المعلوماتي.

المبحث الأول : المجرم المعلوماتي مجرم بمواصفات خاصة

لم يكن لإرتباط الجريمة المعلوماتية بالحاسوب والأنترنت أثر على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب, وإنما كان له أثر أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين العاديين سواء من حيث المفهوم أو من حيث سماته الخاصة وأصنافه ودوافعه, كل هذا وغيره جعل منه محلا للعديد من الأبحاث والدراسات في مجال علم الإجرام.

المطلب الأول : سمات المجرم المعلوماتي

يستفرد المجرم المعلوماتي عن غيره من المجرمين العاديين بشخصية إجرامية خاصة سمتها الذكاء والمهارة والمعرفة العلمية والتقنية المتطورة بمجال النظم المعلوماتية,[1] بالإضافة إلى الهدوء والثقة في النفس والبعد عن كل مظاهر العنف المادي,[2] كل هذه السمات وغيرها تنطوي على أفعاله وتترجم في جرائمه.

الفرع الأول : المجرم المعلوماتي مجرم يتسم بالذكاء والكفاءة والسلطة

يعتبر الذكاء أو الذكاء الغير عادي من أهم صفات مرتكبي الجريمة المعلوماتية, ولذلك غالبا ما يقال بأن الإجرام المعلوماتي هو إجرام الأذكياء مقارنة بالإجرام التقليدي, حيث يتطلب نوعا ما مقدرة عقلية عميقة وذهنية عالية في مجال التعامل مع التقنية المعلوماتية.[3]

وبما أن إرتكاب الجريمة المعلوماتية يقتضي الكثير من الدقة, فإن أغلب مجرمي المعلوماتية يتمتعون بقدرة لا يستهان بها من الإحترافية والمهارة والمعرفة بتقنيات الحاسوب وشبكة الأنترنت, والمكتسبة عن طريق الدراسة المتخصصة أو عن طريق الخبرة العلمية في مجال تكنولوجيا المعلومات الحديثة أو بمجرد التفاعل الإجتماعي مع الآخرين,[4] والتي ينبثق عليها مجموعة من الحقوق والمزايا تجعلهم مسيطرين ومتحكمين إلى حد ما إما بطريقة مباشرة أو غير مباشرة في النظم المعلوماتية, بما يوفر لديهم نظرة واسعة وإلمام كامل بمسرح الجريمة وإحتمال الفشل والنجاح وتجنب المواقف غير المتوقعة والمفاجئة التي قد

تؤدي الى إفشال مخططاتهم وضبط أفعالهم والكشف عنها, وبالتالي فإن إرتكاب الجريمة المعلوماتية لا يحتاج أي جهد عضلي بل يعتمد على الدراسة الذهنية والتفكير العلمي القائم على معرفة تقنيات الحاسوب.[5]

الفرع الثاني : المجرم المعلوماتي مجرم متكيف إجتماعيا

المجرم المعلوماتي في الغالب الأعم هو إنسان إجتماعي قادر على التكيف في بيئة إجتماعية, حتى أن بعضهم يتمتع بثقة كبيرة في الوسط الإجتماعي, فهو لا يقحم نفسه في حالة عداء مع المجتمع الذي يحيط به بل على العكس من ذلك هو إنسان قادر على التوافق والتصالح مع الاخرين والتفاعل معهم,[6] الأمر الذي يزيد من درجة خطورته الإجرامية كلما زاد تكيفه الإجتماعي مع توافر الشخصية الإجرامية لديه.

إن شعور المجرم المعلوماتي أنه محل ثقة في مجتمعه يولد لديه شعور بأنه خارج إطار الشبهات, مما يدفعه الى التمادي أكثر في إرتكاب جرائمه التي قد لا تكشف عادة وحتى وإن أكتشفت فإنها تواجه صعوبة كبيرة جدا في الإثبات.[7]

الفرع الثالث : المجرم المعلوماتي مجرم عائد للإجرام

تتكون لدى معظم مجرمي المعلوماتية نزعة إجرامية تتأثر بعوامل عضوية ونفسية تزيد من إستثارة الحالة الاجرامية وقدرة ضغوط عوامل الإجرام لديهم بشكل تتفوق فيه حتى على موانع الإقدام, الأمر الذي يكسب المجرم مهارة علمية وتكنولوجية تضاعف من رغبته في سد الثغرات التي سبق التعرف عليها وأدت إلى تقديمه للمحاكمة في المرة الأولى, مما يؤدي به الى العودة للإجرام وقد ينتهي به الأمر بتقديمه للمحاكمة مرة ثانية.[8]

الفرع الرابع : المجرم المعلوماتي مجرم حذر جدا

بالرغم من أن جل الدراسات أكدت بأن للمجرم المعلوماتي شخصية تتسم بالهدوء والمثابرة والصبر والتكيف الإجتماعي والثقة الزائدة بالنفس ونبذ العنف المادي والرغبة في التواجد داخل مجموعات إجرامية لتبادل الخبرات وتطوير الملكة الإجرامية, إلا أن ذلك لا يمنع من وجود حذر شديد وخشية وخوف كبيرين لديهم من إكتشاف أفعالهم وإفتضاح أمرهم,[9] وخير دليل على ذلك ما قاله الفقيه بيسموث" بأن للمجرم المعلوماتي شخصية مندمجة في الحياة الإجتماعية ولكنها بالمقابل شخصية حذرة جدا ", وبالتالي فبقدر تكيفه في المجتمع الحقيقي, قادر كذلك على التكيف وبشكل متوازي مع عالم الجريمة المعلوماتية

الذي يعتبره مجالا خصبا له يبنيه ويرسم حدوده معتمدا في ذلك على مبدأ العيش داخل ما يعرف بالمنطقة الذاتية المؤقتة.[10]

يجدر الإشارة في الأخير إلى أن هذه السمات ليست ثابة, وإنما هناك تباين في شخصية كل مجرم عن الآخر سواء من حيث ذكائه أو خبرته أو مركزه الإجتماعي أو إمكانياته.

المطلب الثاني: أصناف المجرم المعلوماتي

إن دراسات علم الإجرام الحديثة تسعى في الوقت الراهن إلى محاولة إيجاد تصنيف ثابت لطوائف مجرمي المعلوماتية, لكنها تجد صعوبة كبيرة في تحقيق ذلك بسبب التغير السريع الحاصل في نطاق هذه الظاهرة والمرتبط أساسا بالتسارع الرهيب في ميدان الكمبيوتر والأنترنت, فالمزيد من الوسائل والمخترعات التقنية يساهم في تغيير أنماط الجريمة وتطور وسائل الإعتداء,[11] ولذلك سنقتصر في تصنيفنا هذا لطوائف مجرمي المعلوماتية على أساس معيار مدى درجة الخطورة الإجرامية الكامنة في شخصية المجرم المعلوماتي.

الفرع الأول : طائفة الأحداث

في بداية الظاهرة شاع الحديث كثيرا عن هذه الفئة, أصطلح عليهم إسم صغار نوابغ المعلوماتية أو المبتدئين أو المراهقين العابثين, إنبهرت هذه الفئة وأغريت كثيرا بالمعلوماتية وأنظمتها حتى أن الأستاذ توم فوستر لقبهم بالمتحمسين للحاسوب.[12]

تعد هذه المرحلة مرحلة إنطلاق حيث يعمل هؤلاء العابثين سواء فرديا أو مع مجموعة على تجميع بعض المعلومات البسيطة تقنيا والمتوفرة على شبكة الأنترنت لإستخدامها ضد مستخدمين آخرين, لكن بمظهر بريئ هدفه اللهو والتسلية دون قصد إلحاق أي ضرر بهم, أي أن دافعهم من ذلك عادة يكون المغامرة والتحدي والرغبة في الإكتشاف والشهرة وجلب الأنظار,[13] ودليل ذلك أنهم لا يعملون على إبقاء مايقومون به سرا.

تظل الخطورة الاجرامية التي تشكلها هذه الفئة محدودة جدا, وذلك لأنه نادرا ما يترتب على أفعالها أضرار جسيمة, ضف إلى ذلك توافر حسن النية في تصرفاتهم التي يعتقدون بأنها غير معاقب عليها قانونا, ولكن لا يجوز الإستهانة بها أبدا خاصة إذا ما تم إحتضانها من طرف منظمات إجرامية خطيرة وتم إستغلال مهاراتهم وروح التحدي والإثارة لديهم في أغراض وغايات إجرامية.[14]

الفرع الثاني : طائفة المخترقين "الهاكرز"

تضم هذه الطائفة أشخاص يمتلكون مهارات ومؤهلات تقنية عالية جدا تصل إلى درجة الإبداع, يعملون بصفة فردية أو داخل مجموعات, يستهدفون بنشاطهم الدخول إلى أنظمة الحاسبات الآلية الغير مصرح لهم بالدخول إليها وكسر الحواجز الأمنية المخصصة لها,[15] لكن يجدر الإشارة هنا إلى أن طائفة المخترقين تنقسم إلى أربع فئات:

أولا : فئة ذوي القبعات البيضاء

وهم أشخاص متخصصون في نظم المعلوماتية والبرمجيات وعلى دراية واسعة جدا بالثغرات الأمنية, في الغالب الأعم هم هواة ومهموسون بالمعلوماتية حيث يرون في إختراقهم للأنظمة المعلوماتية تحديا وإبرازا لقدراتهم الذاتية على الإقتحام, في الحقيقة هذه الفئة لا تشكل خطورة إجرامية كبيرة وذلك لأنه لا يتوافر في تصرفاتهم دافع الحقد أو التخريب والإضرار, زد الى ذلك أنه يرجع لهم الفضل في تحسين الشبكات وتطوير خدمة الأنترنت وكشف الفجوات الأمنية وتطوير آداء أنظمة وبرامج الأمن والحماية المعلوماتية ضد الإختراقات.

ثانيا : فئة ذوي القبعات الرمادية

فئة المخترقين ذوي القبعات الرمادية تشبه الفئة السابقة لكن غايتهم أو دوافعهم مزدوجة, فهو صحيح يخترق الأنظمة المعلوماتية لإكتشاف مواطن ونقاط الضعف فيها لإبلاغ أصحابها من أجل تصحيحها لكنه وفي نفس الوقت قد يستغلها أحيانا لإرتكاب جرائم معلوماتية, أي أنه ينتقل من الإختراق السلمي إلى الإختراق التخريبي وهنا تكمن خطورتهم الإجرامية.

ثالثا : فئة ذوي القبعات السوداء

هذه الفئة من المخترقين لا تشبه الفئة الأولى ولا الثانية, هدفهم من الإختراق ليس البحث عن مواطن الضعف لإبلاغ أصحابها, وإنما هدفهم من الإختراق هو تحقيق أغراض خبيثة وإلحاق أضرار وخسائر جسيمة بالآخرين, الأمر الذي رفع من درجة خطورتهم الإجرامية إلى مستوى صنفهم في خانة الاخطر ضمن فئات المخترقين, نظرا لما يتسببون فيه من إضطرابات لأنظمة المعلوماتية وخسائر كبرى.[16]

الفرع الثالث : طائفة المحترفين

لا ترتكب هذه الطائفة الأفعال الإجرامية بدافع الشهرة وإثبات الذات وإنما بدافع تحقيق غايات إجرامية خطيرة,[17] حيث يتميز مرتكبوها بالقدرات التقنية الواسعة وسعة الخبرة الفنية في مجال أنظمة الحاسوب والشبكات, كما تتميز بالتنظيم العالي والتخطيط المحكم للأنشطة والتصرفات التي ترتكب من قبل أفرادها, الأمر الذي يعكس خطورة إجرامية كبيرة تستنتج من رغباتهم في إحداث التخريب بحيث تهدف جل اعتداءاتهم إلى تحقيق غايات خطيرة, سواء كان ذلك لصالحهم أو لصالح الجهات التي سخرتهم لإرتكاب جرائم الكمبيوتر.[18]

أولا : الكراكرز

صحيح أن الكراكرز فئة ينتمون إلى طائفة القراصنة أو المخترقين إن صح القول, لكن نظرا لخطورتهم الإجرامية الكبيرة تم تصنيفهم ضمن طائفة المحترفين, ولأن اصطلاح الكراكرز هو مرادف للهجمات الحاقدة والمؤذية فإن هذه الفئة تشكل أكبر تهديد على الأنظمة المعلوماتية, حيث يستغلون مؤهلاتهم الفنية والتقنية في تطوير أساليب إرتكاب الجريمة المعلوماتية بهدف إختراق الأنظمة لإتلافها أو تعديلها أو تخريبها, [19] وبالتالي تشكل هذه الفئة تهديدا مباشرا وخطيرا على الأنشطة والمصالح عبر الشبكة العنكبوتية.

ثانيا : الإرهابيين

تطورت أشكال الإرهاب وأساليبه بسرعة مع مر الزمن, حيث ساهمت ثورة تكنولوجيا المعلومات في بروز مصطلح الإرهاب الإلكتروني, الذي وجد ضالته التي كان يبحث عنها في تلك الموارد المعلوماتية, حيث أصبح لديه العديد من المواقع عبر الشبكة العنكبوتية وصارت تلك المواقع من أبرز مظاهره وأشكاله.[20]

ينطلق الإرهاب الإلكتروني بجميع أشكاله وشتى أصنافه من العالم المادي والإفتراضي بدوافع ومعتقدات متعددة يعمل على تجسيدها على أرض الواقع وفق تنظيم وتخطيط محكم بإستخدام الإمكانيات العلمية والتقنية, لبث أفكاره الضالة والمتطرفة والدعوة إلى مبادئه المنحرفة من خلال عبارات حماسية براقة, وإثارة الرأي العام بالتهديد والترويع الإلكتروني للأشخاص والدول.

إتخذ الإرهاب بشكله الإلكتروني أبعادا جديدة زادت من درجة خطورته الإجرامية وعقدت من طبيعة الجريمة المرتكبة, حيث سهل هذا السلاح الرقمي له الإتصال والتخفي, لتنسيق العمليات والتدريب على شن هجمات إلكترونية وتدمير المواقع بالهوية والصفة التي يرغب فيها, بعيدا عن أنظار السلطة والمجتمع.[21]

ثالثا : المنتقمين

في إطار عصرنة الإدارة إنتقلت أغلب دول العالم للأخذ بما يعرف بالإدارة الإلكترونية, إلا أنه وبالرغم من الإيجابيات العديدة التي حملتها هذه العصرنة في طياتها, لكنها أستغلت سلبا من قبل بعض الموظفين الذين أصطلح عليهم إسم الموظف الحاقد أو المنتقم.

يشكل هذا الموظف الحاقد خطر كبير على الأنظمة المعلوماتية للإدارة أو الشركة أو المنشأة التي يعمل بها, حيث يعمد إلى توظيف خبرته ومعرفته في سلوكات عدائية لإلحاق أكبر خسائر ممكنة بها, وتتعدد حالات الإنتقام حسب الميادين والجهات, مثلا كإستغلال الثغرات ونقاط الضعف في النظام لتخريبه أو إتلاف أرشيف المستخدمين, نشر وبث صور وتصميم مخططات وبرامج على مختلف المواقع في الشبكة العنكبوتية أو منحها لشركات منافسة, نسخ إحصاءات رسمية سرية ومنحها لجهات معادية.... الخ, [22] وبالتالي هنا تكمن الخطورة الإجرامية لهذا الموظف الذي يستهدف بإجرامه الإنتقام والثأر من أصحاب وأرباب العمل.

رابعا : الجواسيس

مما لا شك فيه أن التطور الكبير الذي لحق بمجال المعلومات والإتصالات أسفر عن إيجاد وسائل وطرق جديدة أكثر فعالية للتجسس, فتحت آفاق واسعة أمام الأشخاص والجهات الأخرى للتجول دون رقيب والحصول على المعلومات والوثائق السرية مهما كانت درجة خطورتها وحساسيتها والتي يعمل معظم الأشخاص والدول على إخفائها.[23]

تستخدم هذه الفئة مجموعة من الوسائل الفنية وبرامج المساعدة وأجهزة عالية الدقة تسمح بالتنصت والإختراق وفك الرموز والشفرات السرية, بغية معرفة الخطط الإستراتيجية والعسكرية وأسرار الدولة والمشروعات النووية بالإضافة إلى حالة الأسواق وتنقلات الأموال وأسرار الإنتاج والإكتشافات الصناعية المختلفة وكل ما له علاقة بالإستثمار, مستهدف بكل ذلك إستغلال تلك المعلومات للتفوق عليها أو لإفشائها لدولة

معادية أو لتحقيق مصالح شخصية والتي يأتي في مقدمتها الكسب المادي أي المتاجرة بمعلومات وأسرار الدول أو المؤسسات والشركات.[24]

خامسا : المروجين

لقد إستغل مجرمو هذه الفئة في إطار خدمة أنشطتهم الإجرامية أحدث ماتوصلت إليه التقنية المعلوماتية الحديثة, وذلك بإعتبارها الوسيلة المناسبة والبيئة الفضلى للقيام بعمليات نشر وترويج إعلانات الكترونية مخالفة للأعراف والتقاليد وماسة بالآداب العامة والقيم الإجتماعية والأخلاقية المتعارف عليها, عن طريق نوافذ دعائية ومواقع إشهارية مثيرة تستهدف السيطرة على وجدان الشباب وإستغلال طموحاتهم وإندفاعهم وقلة خبرتهم وسطحية تفكيرهم في إفساد حياتهم وتوجيههم للإنحراف.[25]

يقوم مجرمو هذه الفئة بإستغلال خبراتهم ومهاراتهم التقنية العالية بالترويج عبر العديد من المواقع للمخدرات والمؤثرات العقلية ذات الطبيعة الإلكترونية والترغيب في تجريبها بتوفير عينات مجانية عنها ومن ثم تشجيع إدمانها, بث أفكار تثير الكراهية والأحقاد لها علاقة بالعنصرية والتمييز وأفكار تثير الفتن الطائفية وتشوه أو تسيئ للشعائر والمقدسات وتدعو إلى إعتناق ديانات أخرى, الترويج لمواقع تهريب الأسلحة والأثار والمهاجرين, الترويج لمواقع الإتجار بالبشر والأعضاء البشرية,[26] نشر المواد الإباحية والثقافات الجنسية الفاحشة والدعوة لممارستها بتوفير معلومات عليها, إنشاء مواقع الكترونية تشجع وتدعو إلى القمار, الترويج لكل ما يخدش الحياء ويمس بالخصوصية والكرامة والسمعة.[27]

في الأخير يجدر الاشارة إلى أن هذه التصنيفات لا تعني أبدا بأن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات المذكورة, بل يمكن أن يكون المجرم المعلوماتي الواحد مزيجا من أكثر من طائفة, وذلك لأن له مجالات مختلفة ومفتوحة في إطار الجريمة المعلوماتية تسمح له بتقمص أي شخصية إجرامية كانت مادامت معرفته وشغفه بالنظم المعلوماتية قائمة ومستمرة, كل هذا وغيره بداية بالسمات الخاصة ووصولا لتعداد الطوائف يؤكد صحة كلامنا حول درجة الخطورة الإجرامية الكبيرة لهذا النوع الجديد من المجرمين وإختلافهم الجذري عن المجرمين العاديين.

المبحث الثاني : الأساليب والتقنيات الخاصة بالإجرام المعلوماتي

قبل الشروع في الحديث عن الأساليب الخاصة بالإجرام المعلوماتي, لابد أن نوضح أولا وقبل كل شيئ الفرق بين أسلوب تنفيذ الجريمة ونوع الجريمة, فنحن هنا لا نقصد بالأساليب أنواع الجريمة المعلوماتية وإنما نقصد بها الأساليب والتقنيات التي يتبعها المجرم المعلوماتي لتحقيق غايته الإجرامية, والتي تختلف إختلافا جذريا عن الأساليب التقليدية التي يعتمدها المجرم العادي.

يعتمد المجرم المعلوماتي على أساليب إجرامية ذات طبيعة الكترونية سمتها الحداثة والإبتكار, تمكنه من خلال خاصية عملها من التسلل داخل الأنظمة المعلوماتية وإرتكاب جريمته بعيدا عن كل ماقد يشد إليه الأنتباه ويثير حوله الريبة, مستعينا في ذلك بأي أداة تكنولوجية سواء كانت هاتف ذكي أو لوحة الكترونية أو الحاسب الآلي.

إن كثرة الهجمات الإلكترونية وكثافتها دليل على تنوع أساليبها وتعدد تقنياتها, ويمكن أن نوجز بالذكر أهم أحدث وأخطر التقنيات والبرامج المستخدمة في مجال الإجرام المعلوماتي.

المطلب الأول : أساليب إجرامية بواسطة الأدوات التقنية

ظهرت مؤخرا في العالم المعلوماتي مجموعة من الأدوات التقنية عرفت رواجا وتنوعا كبيرا خاصة في ظل الإتاحة المعلوماتية التي توفرها الشبكة العالمية الدولية وشبكة الأنترنت, وبالرغم من إيجابياتها إلا أنها أستغلت سلبا من قبل مجرمي المعلوماتية حيث سخروها للقيام بأعمال غير مشروعة تخدم مصالحهم وتحقق غاياتهم الإجرامية.

الفرع الأول : بروتوكول الشبح

أو كما يعرف بشبكات الشبح أو أسلوب التحكم عن بعد في النظام المعلوماتي, هو عبارة عن أداة تقنية إنتشرت مؤخرا عبر شبكة الأنترنت وأصبحت من أهم الوسائل التي يستخدمها مجرمو المعلوماتية في مجال إجرامهم, حيث يعمل هذا البروتوكول بصفة آلية من خلال شبكة كبيرة من أجهزة الكمبيوتر قد يصل عددها إلى مئات الاجهزة تكون منتشرة عبر كافة أنحاء العالم, يتحكم فيها المجرم المعلوماتي من خلال إستخدام بروتوكولات الشبكة للتواصل مع الأنظمة المصابة.

يستعمل المجرم المعلوماتي هذا البروتوكول من أجل توسيع دائرة نشاطه الإجرامي, فمن خلاله يمكنه نشر الفيروسات الإلكترونية, مراقبة نشاط مستخدمي الحواسيب والتجسس عليهم, شل كل أجزاء شبكة الأنترنت عبر العالم, إرسال رسائل البريد الالكتروني المزعج,[28] وبالتالي تكمن خطورة هذا البروتوكول في إمكانية إستهدافه لمئات الآلاف من أجهزة الكمبيوتر في آن واحد.

الفرع الثاني : البروكسي المجهول

أو كما يعرف بالوكيل المجهول, وهو عبارة عن أداة تقنية خطيرة تحاول جعل النشاط على شبكة الأنترنت غير مكشوف ولا يمكن تعقبه, وبالتالي تتيح للمجرم المعلوماتي تصفح شبكة الأنترنت والتنقل إلى ما وراء مرشحات الموقع خفية دون الكشف عن أي معلومات شخصية تدل عليه من خلال إخفاء"IP" الخاص به ومخلفات التصفح.[29]

تعد هذه الوسيلة التقنية من أخطر الأدوات المستخدمة في عالم الإجرام المعلوماتي, وذلك لأنها تمكن المجرم المعلوماتي من تنفيذ كل مخططاته الإجرامية دون أن يترك أي أثر يدل عليه.

الفرع الثالث : البلوتوث

هو عبارة عن تقنية تهدف لربط المعدات الإلكترونية مع بعضها البعض لتبادل البيانات والمعلومات, مثلا كالحواسيب الآلية, اللوحات الإلكترونية, الهواتف المحمولة, وبصفة عامة كل الأجهزة والمعدات الأخرى التي يمكن أن ترتبط بهذه التقنية, يستخدمه المجرم المعلوماتي من أجل تنفيذ مجموعة من الهجمات تعرف بهجمات البلوتوث, إقتصرت في بدايتها على أجهزة الكمبيوتر المحمولة المزودة بهذه التقنية ليتسع مجالها لاحقا ويشمل كل جهاز مزود بهذه التقنية.

سابقا كان نطاق هذه الهجمات لا يتعدى من 10 الى 20 متر إلا أنه ونتيجة لظهور الهوائيات الإتجاهية تم زيادة نطاقها بشكل كبير جدا, يستغلها مجرمو المعلوماتية لسحب المعلومات والملفات من الجهاز المستهدف أو للإستلاء على دليل الهاتف والرسائل والصور وأشرطة الفيديو الخاصة وحتى على رقمه التسلسلي, السيطرة على الجهاز المستهدف والمساس بأمنه, إجراء المكالمات وإرسال الرسائل وقراءة سجلات الهاتف والتنصت على المحادثات الهاتفية, تحديد مكان تواجد الجهاز, وبالتالي فالخطر الناتج عن هذه التقنية يكمن في إمكانية القيام بكل تلك الأفعال الإجرامية دون علم صاحب الجهاز هذا من جهة

ومن جهة أخرى تلك الأفعال الإجرامية ستتم حتى ولو تم إيقاف البلوتوث, وعليه لا يمكن للضحية أن تكون آمنة من هذا الإختراق.[30]

الفرع الرابع : أنظمة "PGP FONE/ PGP"

هي عبارة عن أنظمة مثيرة للقلق خاصة في الوقت الراهن نظرا لإستخدامها في التشفير العالي التردد لروابط الصوت والبيانات, من قبل مجرمي المعلوماتية خاصة فئة الإرهابيين وأعضاء عصابات الجريمة المنظمة, حيث يستخدمونها في تحويل النص من عادي الى نص مشفر, الأمر الذي يجعل من المستحيل على شخص ثالث أن يفهم تلك الأصوات والبيانات التي يتم تبادلها.[31]

هذه التقنية الخطيرة تعتبر أفضل صديق للمجرم المعلوماتي وأسوء عدو للأجهزة الأمنية, نظرا للصعوبة الكبيرة التي تتخلل عمليات فك تشفير تلك المعلومات حتى بإستخدام كل قوة التقنية وآخر ما توصلت إليه.

في مجال الإجرام المعلوماتي كانت هذه بعض الأدوات التقنية الحديثة المستعملة غالبا من قبل مجرمي المعلوماتية.

المطلب الثاني : أساليب إجرامية بواسطة البرامج الضارة

البرامج الضارة أو البرامج الخبيثة أو ملوثات جهاز الكمبيوتر, مهما كانت التسمية المستعملة فهي تنذر بخطر حقيقي يهدد أمن وسلامة النظم المعلوماتية ومستخدميها, ومما لا شك فيه أن هذه البرامج لا تظهر صدفة أي أنها لا تأتي من مصدر مجهول أو أنها تنشأ بسبب خلل بسيط في جهاز الكمبيوتر, وإنما يتم صنعها وتصميمها بشكل متقن ومتعمد من طرف مجرمي المعلوماتية من أجل تحقيق أغراضهم الإجرامية,[32] الأمر الذي يجعلها تتصدر قائمة أهم الوسائل التي يستعين بها هؤلاء لتنفيذ مخططاتهم الإجرامية.

الفرع الأول : الفيروسات

هي عبارة عن برامج خبيثة مشفرة مصممة بقدرة هائلة على التكاثر والإنتشار بشكل سرطاني أي بنسخ نفسها ذاتيا مرارا وتكرارا عدة مرات سواء داخل نفس الجهاز أو بالانتقال إلى أجهزة أخرى عبر وسائط التخزين أو عن طريق شبكة الأنترنت, تلحق هذه الفيروسات نفسها ببرامج أو ملفات أخرى كحاضنة أو تتشبه ببرامج مفيدة قصد التخفي والخداع والتمويه, مما يصعب إكتشافها من طرف الضحية وحتى برامج مضادات الفيروسات لتبدأ أعمالها التخريبية بمجرد تمكنها داخل الجهاز.[33]

تعمل هذه البرامج التطبيقية بشكل منفصل بهدف إحداث خلل في نظام الحاسوب, وتتراوح خطورتها حسب مهمتها فمنها الخطيرة ومنها غير الخطيرة وكلاهما خبيث, ومن أنواعها نذكر على سبيل المثال لا الحصر: فيروس تشرنوبل, فيروس ستاكس نات, فيروس قوس, فيروس ناسا, فيروس الشعلة, فيروس الماكرو, فيروس وير, فيروس قطاع التشغيل ... الخ, تختلف هذه الفيروسات من حيث بدأ نشاطها التخريبي, فهناك من تبدأ نشاطها بتاريخ ووقت محدد وهناك من تبدأ بالعمل بعد تنفيذ أمر معين في البرنامج المصاب وهناك من تبدأ بعد التكاثر والوصول إلى رقم معين من النسخ, بصفة عامة أغلبها يخضع لسلطة المجرم المعلوماتي فهو الذي يحدد متى وكيف تبدأ نشاطها التخريبي.[34]

تبرمج هذه الفيروسات غالبا بلغة التجميع يحملها المجرم المعلوماتي بتعليمات مختلفة حسب الأهداف التي يصبو لتحقيقها, إما التخريب بحد ذاته وإما بهدف الحصول على منافع شخصية, ومن جملة هذه الأهداف الإجرامية نذكر على سبيل المثال: تعطيل عمل الحاسوب وتدمير ملفاته وبرامجه, مسح المعلومات من القرص الصلب, إتلاف البيانات المسجلة والمخزنة داخل الحاسوب ويشمل أثره الحذف والتعديل, إجهاد الأجزاء الميكانيكية بصورة تدريجية تمهيدا لإيقاف جهاز الحاسوب عن العمل, سرقة بيانات مهمة من الحاسوب كأرقام الحسابات أو كلمات المرور أو أرقام بطاقات الائتمان, تخريب النظام المعلوماتي جزئيا أو كليا ... الخ, بعد أن تنتهي هذه الفيروسات من عملها تقوم بتدمير نفسها ذاتيا دون أن تترك أي أثر يدل عليها.[35]

الفرع الثاني : ديدان الحاسوب

هي عبارة عن برامج خبيثة ذاتية مصممة للإنتقال عبر شبكات الأتصال من جهاز إلى آخر مستغلة في ذلك الثغرات الأمنية التي تعرفها برامج وأنظمة التشغيل, تمتاز بنفس خصائص الفيروس لكنها تفوقه سرعة في الإنتشار وتعتمد على نفسها في التكاثر دون أي حاجة لإرفاق نفسها إلى برامج أوملفات أو وثائق, وبالتالي فهي لا تحتاج إلى الإستقرار في البرنامج لتكرار نفسها وإنما تنسخ نفسها بشكل مستقل من خلال النظام الخاص بك, فبمجرد أن تدخل في النظام تبدأ بمسح الشبكة الخاصة بك لكي تنتفل إلى أجهزة أخرى يكون لها ثغرات أمنية مماثلة, وبالتالي فهي تنتشر عبر الشبكات عن طريق دفتر عناوين البريد الالكتروني.

تعتبر العمليات التخريبية التي تتسبب فيها دودة الحاسوب من أشهر العمليات وأخطرها خاصة تلك التي يكون هدفها حجب الخدمة وتدعى بهجمات حجب الخدمة, حيث تنتشر الدودة فيها على عدد كبير من الأجهزة ثم توجه طلبات وهمية لجهاز خادم معين يكون المجرم المعلوماتي قد حدده مسبقا من خلال برمجته للدودة فيغرق الخادم بكثرة الطلبات الوهمية بشكل لا يستطيع معالجتها جميعا مما يتسبب في توقفه عن العمل, كما يمكن للديدان أن تسبب أضرار أخرى وفقا لكيفية تصميمها نذكر منها على سبيل المثال: إنتهاك خصوصيات أعداد كبيرة من الناس, شغل أكبر حيز ممكن من سعة الشبكة ومن ثم العمل على التقليل أو خفظ كفاءتها, تخريب الملفات والبرامج ونظم التشغيل, جعل جهاز الكمبيوتر بطيئا وغير فعال,[36] وبالتالي نجد بأن دودة الحاسوب بمختلف أنواعها تكتسي خطورة كبيرة جدا لدرجة إستحالة الحد من إنتشارها.

الفرع الثالث : حصان طروادة[37]

هو عبارة عن برنامج فيروس خبيث يمتلك قدرة كبيرة على التسلل والإختفاء في البرنامج الأصلي للمستخدم, بحيث يلحق نفسه ببرنامج آخر يكون محل ثقة وله فائدة, وبالتالي يظهر وكأنه لا يشكل أي خطر على الكمبيوتر لكنه في حقيقة الأمر يخبئ العديد من الوظائف الفتاكة حيث ينشط بمجرد تشغيل البرنامج الأصلي وينتشر ليبدأ نشاطه التدميري.[38]

ولأن عمل هذا الفيروس يعتمد على العلاقة بين العميل والخادم, فإن المجرم المعلوماتي يلحق الخادم بمجموعة ملفات وبرامج نافعة معروفة تكون محل إهتمام من قبل العامة, وبالتالي يؤدي تحميلها من طرف المستخدم وتشغيلها إلى تحميل الخادم وإستقراره في الجهاز دون علم الضحية, فاتحا المجال أمامه لإستقبال التعليمات من العميل وبمجرد إستقبالها تبدأ في العمل الإجرامي, مستهدفا من ذلك كله إما نسخ بيانات ذات قيمة أو حذف معطيات أو تزوير معلومات ومحو بعضها أو تدمير النظام المعلوماتي بأكمله, كل هذه الأغراض الخبيثة وغيرها تثير غضب وخوف الناس وتنذر بأذى كبير سيلحق أجهزة الكمبيوتر.[39]

الفرع الرابع : برنامج راصد لوحة المفاتيح

هو برنامج تجسس معلوماتي جد خطير, يعمل بدقة عالية في مجال مراقبة مضمون النشاطات الإلكترونية للمستخدم المستهدف, يمتاز بقدرة فائقة على النسخ والتخفي ويعمل بشكل هادئ جدا داخل الحاسوب, يركز على أداة مهمة جدا في التواصل مع جهاز الكمبيوتر ألا وهي لوحة المفاتيح, بعد توغله بطريقة سرية للجهاز يقوم برصد وتتبع وتسجيل كل الضربات على لوحة المفاتيح منذ لحظة بدأ تشغيل النظام إلى غاية إيقافه, يستهدف المجرم المعلوماتي من خلاله تسجيل كل ما يقوم المستخدم بكتابته من أسماء مواقع, رسائل الكترونية, عناوين أسماء مستخدمين, كلمات مرور, وذلك حتى قبل تشفيرها أوحذفها.

يستخدم هذا البرنامج بشكل كبير جدا للتجسس وجمع المعلومات على الأشخاص والحواسيب التابعة للشركات التجارية والصناعية, وكذلك الأنظمة المعلوماتية للمؤسسات العمومية التابعة للدولة, وبصفة عامة كل جهاز يحتوي معلومات سرية وحساسة وهنا تكمن خطورة هذا البرنامج.[40]

كانت هذه أهم الأساليب الإجرامية المعلوماتية التي لا يمكن للمجرم المعلوماتي وفي سبيل تحقيق أغراضه الإجرامية وإتمام نشاطه عبر الشبكات والنظم المعلوماتية الإستغناء عنها, نظرا لفعاليتها في تحقيق الأهداف المسطرة والإطاحة بأكبر قدر ممكن من الضحايا, ولعل أهم ما يميزها هو وفرتها وقابليتها للتحميل والإستعمال بسهولة كبيرة إضافة إلى ضعف الرقابة على نشاطات توزيعها وإنتاجها وإستعمالها وهو ما يساهم في إنتشارها وتفاقمها, مما يحول دون توفير الحماية لمستخدمي الأنظمة المعلوماتية وتعقب الخارجين عن القانون.

الخاتمة :

في الختام نود أن نذكر بعض النتائج التي تدعم فكرة تميز المجرم المعلوماتي بخطورة إجرامية كبيرة مقارنة بالمجرم العادي أو التقليدي, نوجزها في النقاط التالية:

- إن تحديد الخطورة الإجرامية للمجرم المعلوماتي أمر في غاية الضرورة, لاسيما مع إتساع قاعدة المجتمع الإفتراضي والإنتشار الكبير للجريمة المعلوماتية.

- المجرم المعلوماتي من أكبر السلبيات التي خلفتها الثورة الرقمية.

- للمجرم المعلوماتي شخصية إجرامية ذات طبيعة ديناميكية مستقلة وقائمة بذاتها, فهو من جهة مثال منفرد للمجرم الذكي ومن جهة أخرى إنسان إجتماعي بطبعه, الأمر الذي يزيد من درجة خطورته الإجرامية.

- المجرم المعلوماتي شخصية إجرامية تهدد بخطر إجرامي كبير, تحولت من مجرد اللهو واللعبث بالأنظمة المعلوماتية إلى أهداف أكبر وأخطر من ذلك يتصدرها تحقيق الربح المادي, الإنتقام, الإضرار بالغير, وصولا إلى الإرهاب المعلوماتي.

- إن شخصية المجرم المعلوماتي عبارة عن مزيج بين سمات خاصة ودوافع عديدة, فالمجرم المعلوماتي لا يعني بالضرورة أنه من فئة وحيدة وله دافع خاص بعينه, وإنما هو حسب شخصيته ودوافعه قد ينتمي إلى أكثر من فئة الأمر الذي يساهم بشكل مباشر في ظهور أصناف جديدة لم تكن موجودة من قبل.

- تتنوع الأساليب الإجرامية وأنماطها ولا يمكن عمليا حصرها حتى ولو أمكن ذلك في الوقت الحاضر, إلا أنه لا يمكن التنبؤ بالوسائل الفنية والتقنية التي قد تستحدث في مجال تكنولوجيا المعلومات, على إعتبار أن هذا الحقل يعرف تطورا متسارعا ومتجددا ومتشعبا حيث يزداد تعقيدا كلما طفت على السطح تقنيات جديدة.

- إن الأساليب والتقنيات المستعملة في مجال الجريمة المعلوماتية من قبل المجرم المعلوماتي أشد فتكا وخطورة من الأساليب التقليدية التي يستعملها المجرم العادي أو التقليدي في جرائمه, وذلك نظرا للأضرار والخسائر الجسيمة التي يسببها نشاط إجرامي معلوماتي مقارنة بما قد تسببه جريمة تقليدية, وعليه فالإجرام المعلوماتي قد تعدى المعنى الكلاسيكي للأساليب التقليدية.

- المجرم المعلوماتي من أصعب الشخصيات الإجرامية التي تتعامل معها الأجهزة الأمنية في العالم.

بناء على هذه النتائج توصلنا لإقتراح مفاده: أن المجرم المعلوماتي مهما تمت محاربته بقوة القانون وبقوة الحلول الفنية والتقنية, فلن نتمكن من القضاء عليه طالما أن الفجوة التكنولوجية كبيرة وقابلة للتطور يوما بعد الآخر ولسنا حتى في مستوى إستعابها تقنيا ومواجهتها جنائيا, لذلك فالحل الوحيد المتبقي هو محاولة إحتواء هذه الفئة التي تكون على درجة كبيرة من الخطورة وتحويل وجهة نشاطهم السلبي إلى وجهة إيجابية مقابل توظيفهم وتحفيزهم بمرتبات, حتى يكون هناك مواجهة فعالة بين خبير وآخر يفوقه قدرة تقنية وإمكانات فنية.

الهوامش :

[1] المضحكي حنان ريحان مبارك, الجرائم المعلوماتية, دراسة مقارنة, منشورات الحلبي الحقوقية, لبنان, 2014, ص 41.

[2] أمير فرج يوسف, الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت, مكتبة الوفاء القانونية, مصر, 2011, ص 119.

[3] *chawki Mohamed, combattre le cyber criminalité, édition, France, 2009, p57.*

[4] أمير فرج يوسف, مرجع سابق, ص 120.

[5] الدسوقي طارق إبراهيم عطية, الأمن المعلوماتي, دار الجامعة الجديدة للنشر, مصر, 2009, ص 176-177.

[6] العريان محمد علي, الجرائم المعلوماتية, دار الجامعة الجديدة, مصر, 2011, ص 77.

[7] العزيزى فؤاد حسين, الجرائم المعلوماتية, دراسة مقارنة, دار الفكر الجامعي, مصر, 2014, ص 45.

[8] نبيه نسرين عبد الحميد, الجريمة المعلوماتية والمجرم المعلوماتي, منشأة المعارف, مصر, 2008, ص 26.

[9] *chawki Mohamed, Op-cit, p60.*

[10] المنطقة الذاتية المؤقتة: هي المنطقة التي يختبئ ويعيش داخلها المجرم المعلوماتي أثناء فترة غيابه عن المجتمع الحقيقي والتي يحرص من خلال حذره الدائم على عدم السماح لأي كان من الولوج إليها, وهذا مايفسر وجود فئة شاذة من مجرمي المعلوماتية اللذين يتميزون بالعزلة على العالم الحقيقي نظرا لتواجدهم على الدوام بالمنطقة الذاتية المؤقتة, انظر المزيد في:

- Humbert Jean Philipe, les mondes du cyber délinquance et l'image sociale du pirate informatique, thèse de doctorat, sciences de l'information est de la télécommunication, centre de recherche sur les médiations, université Paul Verlaine, Metz, France, 2007, p248.

[11] الشمري غانم مرضي, الجرائم المعلوماتية, الدار العلمية الدولية للنشر والتوزيع, الاردن, 2016, ص 42.

[12] العزيزى فؤاد حسين, مرجع سابق, ص 41.

[13] العريان محمد علي, مرجع سابق, ص 79.

[14] *Quéménér Myriam, cyber menaces, entreprise et internautes, édition Economico, France, 2008, p18.*

[15] حجازي عبد الفتاح بيومي, الجريمة في عصر العولمة, دار النهضة العربية, مصر, 2010, ص 141.

[16] الزيدي وليد, القرصنة على الأنترنت والحاسوب, دار أسامة للنشر والتوزيع, الاردن, 2003, ص 32.

[17] الشمري غانم مرضي, مرجع سابق, ص 44.

[18] الدسوقي طارق إبراهيم عطية, مرجع سابق, ص 183.

[19] نبيه نسرين عبد الحميد, مرجع سابق, ص 48.

[20] أمير فرج يوسف, مرجع سابق, ص 250.

[21] المضحكي حنان ريحان مبارك, مرجع سابق, ص 282.

[22] ممدوح خالد إبراهيم, الجرائم المعلوماتية, دار الفكر الجامعي, مصر, 2009, ص 56.

[23] المضحكي حنان ريحان مبارك, مرجع سابق, ص 278.

[24] حجازي عبد الفتاح بيومي, مرجع سابق, ص 143-144.

[25] *Quéménér Myriam, Op-cit, p22-23.*

[26] المضحكي حنان ريحان مبارك, مرجع سابق, ص224-225.

[27] أمير فرج يوسف, مرجع سابق, ص 347.

[28] موسى مصطفى محمد, أساليب إجرامية بالتقنية الرقمية, دراسة مقارنة, دار الكتب القانونية, مصر, 2005, ص 122.

[29] *Arpagian Nicolas, le cyber sécurité, édition presse universitaire de France /PUF/, France, 2010, p42.*

[30] الحمداني بشرى حسين, القرصنة الإلكترونية أسلحة الحرب الحديثة, دار أسامة للنشر والتوزيع, الاردن, 2014, ص 84.

[31] عوض الحاج علي أحمد, عبد الأمير خلف حسين, أمنية المعلومات وتقنيات التشفير, دار الحامد للنشر والتوزيع, الاردن, 2004, ص 210.

[32] موسى مصطفى محمد, مرجع سابق, ص 134.

[33] حجازي عبد الفتاح بيومي, مرجع سابق, ص 145.

[34] العريان محمد علي, مرجع سابق, ص 106-107.

[35] الحمداني بشرى حسين, مرجع سابق, ص 96.

[36] المومني نهلا عبد القادر, الجرائم المعلوماتية, دار الثقافة للنشر والتوزيع, الاردن, 2008, ص 130-131.

[37] سمي هذا الفيروس بحصان طروادة نسبة للقصة اليونانية الشهيرة لحصان طروادة, حيث اختبأ الجنود اليونانيون داخله واستطاعوا إقتحام مدينة طروادة والتغلب على جيشها.

[38] الزيدي وليد, مرجع سابق, ص 113.

[39] العريان محمد علي, مرجع سابق, ص 109.

[40] المومني نهلا عبد القادر, مرجع سابق, ص 216-217.