**ماستر علم النفس الاجتماعي**

**محاضرات وحدة الجريمة الالكترونية**

**أ.د/ سليماني جميلة**

# مدخل إلى الجريمة الالكترونية

إن ظاهرة جرائم الكمبيوتر والانترنت، أو جرائم التقنية العالية، أو الجريمة الإلكترونية، أو السيبر كرايم– Cyber Crime أو جرائم أصحاب الياقات البيضاء White Collar/Col blanc ، ظاهرة إجرامية مستجدة نسبيا. ترتكب في دولة ما ويتحقق الفعل الإجرامي في دولة أخرى.

يرتبط حدوث الجرائم الإلكترونية، على اختلاف أنواعها، بالصدمة الثقافية التي نتجت من الانفتاح الهائل والمفاجئ الذي رافق ظهور شبكة الإنترنت، وضاعف من قدرة الأفراد على الوصول إلى خصوصيات الآخرين، وبالتالي سهولة الوصول إلى ضحاياهم، وارتكاب الجرائم في حقّهم، في شكل يعتقد هؤلاء «المجرمون» أنّه آمن وغير قابل للكشف. فالجريمة ظاهرة للعيان، إلا أن المجرم متخّفٍّ خلف أسوار الأجهزة الإلكترونية، التي يعتقد أنها تحميه أو تخفي هويته.

وفي حين تتوافر لدى الدول، إحصاءات عن الخسائر الاقتصادية الناجمة عن الجرائم الإلكترونية، من خلال سرقة الحسابات البنكية أو اختراق المواقع الرسمية، التي تقدّر عالمياً بـــ400 بليون دولار سنوياً، إلا أن جرائم كثيرة منها ذات الكلفة والطابع الاجتماعي، لا تزال مجهولة ولا تتوافر إحصاءات دقيقة عنها، وربما يكون السبب الرئيس في ذلك عدم لجوء الضحايا إلى السلطات الرسمية.

تشير الجرائم الإلكترونية ذات الطابع الاجتماعي، التي يتحدّث عنها خبراء في الأمن الإلكتروني وقانونيون أو مختصّون نفسيون واجتماعيون، إلى أنها تدور حول التشهير والتحقير وإنشاء حسابات وهمية على شبكات التواصل الاجتماعي، واستخدام صور الأشخاص الذين تُنشأ هذه الحسابات بإسمهم، أو إرسال رسائل مسيئة أو غير أخلاقية بإسمهم إلى آخرين، بهدف التشويه والإضرار بالسمعة. وتدور غالبيتها في فلك الانتقام والغيرة، والمشاجرات الاجتماعية غير اللائقة التي تُدار بطريقة غير سويّة.

**تعريف الجريمة الإلكترونية:**

يتكون مفهوم الجريمة الإلكترونية(Cyber crimes) من مقطعين هما الجريمة (crime) و (cyber) الإلكترونية. و الجريمة هي السلوكيات والأفعال الخارجة على القانون.

و قد وضع الفقهاء و الدارسون لها عدة تعريفات، تتباين تبعا لموضوع التخصص المنتمية اليه، فمنهم من عرفها من الجانب التقني و منهم من عرفها من الجانب القانوني.

و من أجل مفهوم شامل للجريمة لا بد من تعريفها من كلا الجوانب و بيان أنواعها.

**الفرع الأول : تعريـــــف الجريمة الإلكترونية من الجانب الفني.**

الجريمة الالكترونية عبارة عن نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي. كما أنها تصرف غير مشروع يؤثر في الاجهزة و المعلومات الموجودة عليها.

يعتبر هذا التعريف جامع مانع من الناحية الفنية للجريمة الالكترونية حيث انه لارتكاب الجريمة يتطلب وجود اجهزة كمبيوتر زيادة على ربطها بشبكة معلوماتية ضخمة.

**الفرع الثاني : تعريف الجريمة الالكترونية من الجانب القانوني .**

تعرف بأنها: "مجموعة من الأفعال و الأنشطة المعاقب عليها قانونا و التي تربط بين الفعل الإجرامي و الثورة التكنولوجية" و بمعني آخر هي: " نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي".

كما أن هناك من عرفها بأنها "الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني".

قسم رجال القانون العرب الجريمة المعلوماتية (الجرائم الالكترونية) في جانبها القانوني الى:

**اولا:** الجرائم التي تستعمل فيها الوسائل التكنولوجية من أجل القيام بالفعل الإجرامي مثل: تزوير أموال عن طريق الماسح الضوئي فهذا النوع له إطاره القانوني في معظم التشريعات العالمية.

**ثانيا:** الجرائم التي تستخدم التقنية الحديثة لارتكابها، حيث عن طريق شبكة الانترنيت يمكن إنشاء مواقع إباحية، أو انضمام إلى مجموعات إرهابية، أو المتاجرة بالسلاح أو المخدرات أو المتاجرة بأسرار الناس عن طريق خرق مواقعهم أو جهاز الكمبيوتر أو انتحال الشخصية باستخدام بطاقات الائتمان.

من خلال كل ما ذكر يمكن تعريف الجريمة الإلكترونية بأنها سلوك غير مشروع أو غير أخلاقي أو غير مسرح به.

## التطور التاريخي للجرائم الالكترونية:

مرت جرائم الأنترنت بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ويمكن تلخيص أهم مراحل تطورها فيما يلي:

**المرحلة الأولى:** منذ شيوع استخدام الحواسيب في الستينات و السبعينات اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر. وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شئ عابر ام ظاهرة إجرامية مستحدثة، وان الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة، ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة.

**المرحلة الثانية:** في الثمانينات، حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والانترنت ارتبطت بعمليات اقتحام نظام الكمبيوتر عن بُعد وأنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات أو البرامج. في عام 1988 ظهرت "دودة موريس" –إحدى أوائل ديدان الحواسيب المعروفة التي أثرت في البنية التحتية للإنترنت وانتشرت في الحواسيب وعلى نطاق واسع داخل الولايات المتحدة، واستغلت الدودة نقطة ضعف في نظام يونيكس "ناون 1" واستنسخت ذاتها بانتظام وتسببت بإبطاء أداء الحواسيب لدرجة عدم القدرة على استخدامها.

وعند اعتقال مطور هذه الدودة روبرت تابان موريس أصبح أول قرصان يُدان تحت قانون "احتيال الحاسوب وإساءة الاستخدام"، وهو الآن أحد القراصنة الأخلاقيين (أصحاب القبعات البيضاء –سوف نتناول هذه المفهوم فيما بعد–) حيث يعمل بروفيسورا في معهد ماساتشوستس التكنولوجي.

في صيف عام 1994 تمكن قرصان روسي يدعى فلاديمير ليفين من اختراق بنك "سيتي بنك" الأميركي وتحويل عشرة ملايين دولار من حسابات عملاء إلى حساباته الشخصية في فنلندا وإسرائيل مستخدما حاسوبه المحمول. حكم عليه بعد اعتقاله بالسجن ثلاث سنوات، واستعادت السلطات كافة المبلغ المسروق باستثناء أربعمائة ألف دولار.

شاع اصطلاح "الهاكرز" Hackers(قراصنة الانترنت) المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورا في رغبة المحترفين تجاوز امن المعلومات وإظهار تفوقهم التقني، لكن هؤلاء المغامرون أصبحوا أداة إجرام.

⇩

ظهر المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة، القادر على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية الاجتماعية والسياسية والعسكرية.

**المرحلة الثالثة:** حيث شهدت التسعينات تناميا هائلا في حقل الجرائم الالكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط جديدة: إنكار الخدمة التي تقوم عل فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامة التي يتسبب انقطاعها عن الخدمة لساعات في خسائر مالية بالملايين، ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت.

وظهرت الرسائل المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على إثارة الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المروجة لمواد غير قانونية أو غير مشروعة.

**المرحلة الرابعة:**

في أكتوبر 2012 اكتشفت شركة أمن المعلومات الروسية "كاسبرسكي" هجوما إلكترونيا عالميا حمل اسم "أكتوبر الأحمر"، وقالت إنه يجري منذ عام 2007 على الأقل ويعمل على جمع معلومات من سفارات وشركات أبحاث ومؤسسات عسكرية وشركات طاقة وغيرها، مشيرة إلى أن أهداف الهجوم الرئيسية هي دول في أوروبا الشرقية ودول الاتحاد السوفياتي السابق وآسيا الوسطى، وبعض دول أوروبا الغربية وشمال أميركا.

وفي أواخر نوفمبر 2014 تعرضت شبكة حواسيب شركة سوني بيكتشرز اليابانية في الولايات المتحدة لهجوم إلكتروني عنيف نتجت عنه سرقة عدد من الأفلام السينمائية الحديثة التي لم يكن بعضها قد عرض بعد، وتسريب مئات آلاف رسائل البريد الإلكتروني والبيانات الشخصية لحسابات معروفة، ووصفت بعض تلك الرسائل بالمحرجة، وبشكل عام تكبدت الشركة نتيجة هذا الهجوم –الذي نسب إلى كوريا الشمالية أو متعاطفين معها– خسائر قدرت بنحو مائة مليون دولار.

رغم تزايد الأبحاث و محاولات ابتكار أنظمة تكفل لأي كمبيوتر الحماية اللازمة إلاّ أنه في المقابل يتم تطوير الإجراءات المضادة لهذه الحصون الأمنية، ومعنى ذلك أن خطر إنتهاك أمن و سلامة الكمبيوتر مستمرة مدى استمرارية هذه التحصينات.

وقد يكون الكمبيوتر في مجال ارتكاب الجرائم هدفا للجرائم للجريمة أو أداة لارتكابها أو مسرحا لها. وقد يكون الكمبيوتر دورا رئيسيا في حقل اكتشاف الجريمة، و سنعرض فيما يلي لأدوار الكمبيوتر و الانترنت في مجال ارتكاب الجريمة و اكتشافها و ذلك فيما يلي:

**أ–قد يكون الكمبيوتر هدفا للجريمة:** ويتحقق ذلك في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات و الملفات المخزنة أو تعديلها، وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم. وتوجه هجمات إلى معلومات كمبيوتر أو خدماته قصد المساس بالسرية أو سلامة المحتوى و تكامليته أو تعطيل القدرة و الكفاءة للأنظمة للقيام بعملها. وهدفه هو المعلومات المخزنة بهدف السيطرة على النظام دون التصريح و دون دفع و تتضمن بعض طوائف هذا النمط أي كمبيوتر كهدف أنشطة للسرقة و الاعتداء على الملكية الفكرية.

**ب–قد يكون الكمبيوتر مكان للجريمة:** كما في حالة استغلال الكمبيوتر للإستلاء على الأموال بإجراء تحويلات غير شرعية استخدام التقنية في عمليات التزوير و التزييف، و الاستلاء على أرقام بطاقات الائتمان و إعادة استخدامها للاستيلاء على الأموال بواسطة ذلك.

**ج– قد يكون الكمبيوتر أداة للجريمة:** وذلك كما في حالة تخزين البرامج المنسوخة أو في حالة استخدامه لنشر المواد الغير قانونية أو استخدامه أداة لتخزين أو اتصال بصفقات ترويج المخدرات و أنشطة الشبكات الإباحية و نحوها.

**أنواع الجرائم الإلكترونية:**

1. **الجريمة المادية:** وهي التي تسبب أضرارا مالية على الضحية أو المستهدف من عملية النصب وتأخذ واحدة من الأشكال الثلاثة: عملية السرقة الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك كتلك التي منتشرة الآن في الكثير من الدول وفيها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية. إنشاء صفحة انترنت مماثلة جدا لموقع احد البنوك الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد على الحصول بياناته المصرفية وسرقته.

رسائل البريد الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج مع الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد

الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي.

2. **الجريمة الثقافية:** هي استيلاء المجرم على الحقوق الفكرية ونسبها له من دون موافقة الضحية فمن الممكن أن تكون إحدى الصور التالية: قرصنة البرمجيات: هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات وبيعها للناس بسعر أقل.

التعدي على القنوات الفضائية المشفرة وإتاحتها عن طريق الانترنت عن طريق تقنية. (soft copy) جريمة نسخ المؤلفات العلمية و الأدبية بالطرق الالكترونية المستحدثة.

3. **الجريمة السياسية والاقتصادية:** تستخدم المجموعات الإرهابية حالياً تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية. وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق، وبث الأخبار المغلوطة، وتوظيف بعض صغار السن، وتحويل بعض الأموال في سبيل تحقيق أهدافهم • وفي بعض البلدان يقوم الإرهابيون باستخدام الإنترنت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية • والاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجانا .
•وتساعد أيضا فى نشر الأفكار الخاطئة بين الشباب كالإرهاب والإدمان والزنا لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى.

4. **الجريمة الجنسية:** هذا النوع من الجريمة يمكن أن يتمثل بإحدى الصور التالية
•:الابتزاز: من أشهر حوادث الابتزاز عندما يقوم احد الشباب باختراق جهاز احد الفتيات أو الاستيلاء عليه و به مجموعة من صورها، وإجبارها على الخروج معه وإلا سيفضحها بما يملكه من صور مثلا •. وانتشار الصور و مقاطع الفيديو المخلة بالآداب على مواقع الانترنت.

**مميزات وخصائص الجرائم الالكترونية:**

**1-عالمية الجريمة "جرائم عابرة للقارات:** بمعنى انها لا تعترف بالحدود الجغرافية للدول وحتى بين القارات، لأنه مع إنتشار شبكة الاتصالات العالمية "الانترنت أمكن ربط أعداد هائلة منم لا حصر لها من الحواسيب عبر العالم لهذه الشبكة، حيث يمكن ان يكون الجاني في بلد والمجنى عليه في بلد آخر وهكذا فالجرائم الالكترونية تقع في أغلب الاحيان عبر حدود دولية كثيرة.

**2-جرائم صعبة الاثبات:** صعوبة متابعتها واكتشافها فهي لا تترك اثرا، هي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الالكترونية تم إكتشافها بالصدفة وبعد وقت طويل من ارتكابها، تفتقر إلى الدليل المادي التقليدي كالبصمات مثلا. وتعود أسباب صعوبة إثباتها إلى أن متابعتها و اكتشافها من الصعوبة بمكان، حيث أنها لا تترك أثرا فما هي إلا أرقام تدور في السجلات، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها، وتعود الصعوبة لأسباب:

- أنها كجريمة لا تترك أثرا بعد ارتكابها.
- صعوبة الاحتفاظ الفني بآثارها أن وجدت.
- أنها تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها.
- أنها تعتمد على الخداع في ارتكابها و التضليل في التعرف على مرتكبيها.
- أنها تعتمد على قمة الذكاء في ارتكابها.

**3-جرائم ناعمة:** إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل /، السرقة، الاغتصاب، فالجرائم الالكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد عل الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية بالحاسب الآلي.

## سمات الشخصية لمجرمي الجرائم الالكترونية

في بداية ظهور هذه الجرائم شاع الحديث عن المجرمين الصغار الذين يرتكبون مختلف أنواع الاعتداءات على نظم الكمبيوتر وتحديدا الاختراقات التي كانت بدافع التحدي واثبات المقدرة العلمية والتقنية.

**الجوانب السيكولوجية:**

إن الدراسات الحالية للجوانب السيكولوجية لمجرمي الحاسوب أظهرت شيوع عدم الشعور بلا مشروعية الطبيعة الإجرامية و بلا مشروعية الأفعال التي يقترفونها، وكذلك الشعور بعدم استحقاقهم للعقاب عن هذه الأفعال.

أي حدود الشر والخير متداخلة لدى هذه الفئة وتغيب في أنفسهم مشاعر الإحساس بالذنب، ليس هذا فقط فبعض المجرمين "هواة الإجرام" يعتبرون عملهم هذا هواية ولا يمكنهم الاستقلال منها أبداً و هذه المشاعر في الحقيقة تبدو متعارضة مع ما تظهره الدراسات من خشية مرتكبي جرائم الحاسوب من اكتشافهم وافتضاح أمرهم ولكن هذا الخوف والخشية تفسر بانتمائهم في الأغلب إلى فئة اجتماعية متعلمة ومثقفة.

يصف المختصين في علم النفس، دوافع المجرمين الإلكترونيين بالفضول الشديد، والانتقام، وأنهم يعانون من فراغ يسمح لهم بتمضية أوقات طويلة على شبكة الإنترنت. كما أنهم يتّصفون وفقاً لما جاء في كتابThe psychology of cybercrime، أو سيكولوجية الجرائم الإلكترونية (تم عرضه على الطلبة أثناء حصة المحاضرة)، بأنهم يعانون من الوساوس القهرية، فلا يمكنهم السيطرة على رغبتهم في ملاحقة الآخرين وإيذائهم. كما أنهم مصابون باضطراب الشخصية النرجسية، ويعانون من تقدير ذات متدنٍّ، ولا يملكون القدرة على المواجهة أو التعامل مع المشكلات وإدارة العلاقات جيداً. ويفشلون في بناء علاقات صحّية، ويقلل اضطراب الشخصية النرجسية من قدرتهم على تقدير نتائج أفعالهم، ويرتكبون أفعالاً تخدم شهوتهم إلى الانتقام، أو فضول التجسّس لديهم، بغض النظر عن عواقب هذه الأفعال.

كما أنّ استخدام الوسائل الإلكترونية في إيذاء الآخرين وملاحقتهم، متستّرين خلف هوية غير حقيقية، يشعرهم بمزيد من القوة والسيطرة اللتين تتطلّبهما نرجسيّتهم، وهوسهم المرضي بملاحقة ضحاياهم، وهو ما يوفره بسهولة الاتصال الدائم لهم ولضحاياهم على

الشبكة العنكبوتية، من خلال أجهزة الهواتف والأجهزة المحمولة الأخرى، المرتبطة دائماً بالإنترنت، حيث ترتكز استراتيجيتهم في إيذاء الآخرين على الإصرار والمطاردة، وتتبع أصدقائهم ومن يتفاعلون معهم على شبكات التواصل الاجتماعي، ليروّجوا إشاعاتهم عن ضحاياهم وتشويههم أمامهم.

وتفيد دراسات أخرى بأن مجرمي الإنترنت هم أفراد لديهم ميل مرتفع إلى القلق الخارج عن السيطرة، الذي يؤدّي إلى التهور في استخدام الوسائل الإلكترونية في شكل غير مدروس، في تصفية الحسابات والإساءة إلى الخصوم. كما أنّ لديهم اعتقاداً بأن الوسائل الإلكترونية أسرع في نشر الفضائح أو التشهير بالآخرين. وهم كذلك عرضة للاكتئاب أكثر وأسرع من غيرهم، ويشعرون بأن الإساءة الإلكترونية أكثر أماناً لهم، واهمين أن من الصعب الوصول إليهم أو تحديد هويتهم الحقيقية.

وفي أمثلة كثيرة لم يخطر في بال مرتكبي هذه الجرائم، أن ضحاياهم سيلجؤون إلى القضاء بسبب حساب وهمي أنشئ بإسمهم على «فايسبوك» أو «تويتر»، أو أنهم لن يتمكّنوا من معرفة هوية من نشر صورهم أو روّج الإشاعات عنهم. كما أنهم كانوا يقللون من قيمة الأمر ولا يعتبرونه جريمة، إلا أنهم فوجئوا بمداهمة منازلهم أو أماكن عملهم من جانب الأجهزة الأمنية، والتحفّظ على الأجهزة الإلكترونية والهواتف الموجودة لدى ساكني المنزل، وتحويلها إلى التحقيق الجنائي، بعد تحديد إسم صاحب حساب الإنترنت ( IP Address) الذي استُخدم لإنشاء هذه الحسابات أو إطلاق الإشاعات.

**تصنيف مجريمي الانترنت:**

من افضل التصنيفات لمجرمي التقنية التصنيف الذي اورده David Icove, Karl Seger & William Vonstorch في كتابهم جرائم الكمبيوتر الصادر عام (1995) حيث تم تقسيم مجرمي التقنية الى ثلاثة طوائف المخترقون، والمحترفون، والحاقدون.

**أولا/ القراصنة المخترقون، الهواة Hackers**

هاكر بالإنجليزية Hacker أو قرصان إن كان مخرب، عموما كلمة توصف المختص المتمكن من مهارات في مجال الحاسوب وأمن المعلوماتية. وأطلقت كلمة هاكر أساسا

على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدوا الأنظمة المختلفة ويحاولوا اقتحامها، وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة أو حتى جنحة، ولكن نجاحهم في الاختراق يعتبر نجاحا لقدراتهم ومهارتهم. إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان افتراضي لا يجب أن يكونوا فيه. والقيام بهذا عملية اختيارية يمتحن فيها المبرمج قدراته دون أن يعرف باسمه الحقيقي أو أن يعلن عن نفسه. ولكن بعضهم استغلها بصورة إجرامية تخريبية لمسح المعلومات والبعض الآخر استغلها تجاريا لأغراض التجسس والبعض لسرقة الأموال.

هنا وجدت الكثير من الشركات مثل مايكروسوفت ضرورة حماية أنظمتها ووجدت أن أفضل أسلوب هو تعيين هؤلاء الهاكرز بمرتبات عالية مهمتهم محاولة اختراق أنظمتها المختلفة والعثور على أماكن الضعف فيها، واقتراح سبل للوقاية اللازمة من الأضرار التي يتسبب فيها قراصنة الحاسوب. في هذه الحالة بدأت صورة الهاكر في كسب الكثير من الإيجابيات. إلا أن المسمى الأساسي واحد. وقد أصبحت كلمة هاكر تعرف مبرمجا ذا قدرات خاصة يستخدمها في الصواب كما يمكن استخدامها في الخطأ.

**الخلاف حول تعريف الهاكر:**

ينظر كثيرون للهاكر على أنه شخص مدمر وسلبي، ويقرن البعض كلمة هاكر مع قرصان الحاسوب. وذلك بتأثير من بعض ما ورد في الإعلام، حيث يرجع السبب لقلة فهمهم حقيقة الهاكر، وخلطهم لها بكلمة القرصنة بالإنجليزيةPiracy : التعبير الذي يصف البيع غير المشروع لنسخ من أعمال إبداعية. وهي مستخدمة في انتهاك حقوق الملكية الفكرية وحقوق النشر خصوصا بالنسبة للأفلام والمسلسلات التلفزيونية والأغاني وبرامج الحاسوب. والتي أصبحت الشبكة العنكبوتية إحدى وسائل تسويقها.

أصل الخلاف أطلقه بعض الأكاديميون لعدم فهمم لطبيعة الهاكر وأسلوب عمله بالرغم من أنه أساسا مطور مبدع. ولكنهم رأوا دوره سلبيا ومفسدا، متناسين أن الإنترنت يزدحم بمشاريع تم تطويرها من نشاط جماعي للهاكرز، من أمثلة تلك مشاريع: لينكس، ويكيبيديا، ومعظم المشاريع ذات المصدر المفتوح.

## ثانيا/ القراصنة المحترفين Crackers

تعرف هذه الطائفة بالمجرمين البالغين او المخربين المهنيين، تتراوح اعمارهم ما بين 25 و 45 سنة و يتميزون بمكانة اجتماعية بارزة في المجتمع. الكراكر Cracker مصطلح أطلق فيما بعد للتمييز بين الهاكر الصالح والهاكر المفسد، وبالرغم من تميز الإثنين بالذكاء وروح التحدي وعدم خوفهم من مواجهة المجهول. إلا أن الكراكر يقوم دائما بأعمال التخريب والاقتحام لأسباب غير ايجابية وهذا الشخص هو الذي يستحق تسمية قرصان الحاسوب. بينما الهاكر يبتكر الحلول للمشاكل ويحاول أن يبدع في عمله.

**تصنيف الهاكر أخلاقيا:**

- الهاكر ذو القبعة البيضاء(White hat hacker) ، ويطلق على الهاكر المصلح.
- الهاكر ذو القبعة السوداء(Black hat hacker) ، يطلق على الهاكر المفسد، وهو يسمى بالإنجليزيةCracker
- الهاكر ذو القبعة الرمادية(Grey hat hacker) ، المترنح بين الإصلاح والعبث.

أما اصطلاح القبعات فأصله مرتبط بتاريخ السينما وخصوصا أفلام رعاة البقر حيث كان الرجل الطيب يرتدي دائما قبعة بيضاء بينما يرتدي الرجل الشرير قبعة سوداء والرمادية لمن يقع دوره بين هاتين الحالتين.

- **القرصان الأبيض القبعة** يمارس ما يعرف بـــ**القـــرصنة الأخلاقية** هو مصطلح يُطلق في عالم تقنية المعلومات على شخص تعارض قِيَمه انتهاك أنظمة الحواسيب الأخرى. يركز القرصان ذو القبعة البيضاء على حماية الأنظمة، على عكس القرصان ذو القبعة السوداء الذي يحاول اختراقها.
- بتعريف آخر، **القرصان ذو القبعة البيضاء** هو شخص مصرّح له باستخدام الوسائل الممنوعة لمعالجة أخطار أمن الحواسيب والشبكات.
- **قبعة سوداء** (بالإنجليزية**Black hat** ) هو الشرير أو **الرجل السيء**، خصيصاً في أفلام الغرب الأمريكي (Western) مثل هذه الشخصية التي ترتدي قبعة سوداء على النقيض من الأبطال ذوي القبعة البيضاء وغالبا ما تُستخدم

هذه العبارة مجازيا في الحوسبة حيث تعود إلى المخترق الذي يقتحم الشبكات أو الحواسيب أو يصنع فيروسات الحاسوب للتخريب أو الحصول على المال.

- **القرصان رمادي القبعة** هو مصطلح يُطلق في مجتمع أمن الحواسيب على القرصان الذي يقوم بأعمال قانونية أحياناً، أو بمساعدة أمنية كما يملي عليه ضميره أحياناً، أو باختراق مؤذ في أحيان أخرى. إنه باختصار عبارة عن مزيج من القرصان ذي القبعة البيضاء والقرصان أسود القبعة، لذا اختير له اللون الرمادي كلون وسط بين الأبيض والأسود. في العادة، لا يقوم هذا النوع من القراصنة بالاختراق لأغراض خبيثة أو لمصلحة شخصية، بل لزيادة خبرته في الاختراق واكتشاف الثغرات الأمنية.

**انواع البرامج التي تشكل تهديد لنظم المعلومات:**

- **الفيروسات الحاسوبية:** هي عبارة عن برامج حاسوبية والتي ترتبط مع برامج حاسوبية اخرى أو ملفات بيانات من اجل تنفيذها بطريقة خاطئة.
- **البرامج الدودية:** هي برامج حاسوبية مستقلة تقوم بنسخ نفسها من كمبيوتر الى اخر عبر الشبكة.
- **برنامج حصان طرواده:** هو برنامج يبدو في ظاهره انه سينفذ شيء معين ولكن عند البدء يقوم بعمل اخر مضر بنظم المعلومات.
- **برامج التجسس Spyware:** هي برامج حاسوبية تقوم بالنزول بشكل سري عبر الشبكة وتقوم بتسجيل الكبسات التي استخدمت من اجل معرفة الكلمات السرية والارقام المتسلسلة.

**الجرائم الالكترونية التي يسعى الهاكرز للقيام بها:**

- الخداع الالكتروني Spoofing : والمتمثل بإرسال ايميل مزيف او التمثيل بانه ايميل لشخص اخر وتوجيه شبكة الانترنت لإرسال معلومات الى جهات اخرى غير المخصصة.

- استخدام برامج التجسس Sniffer: هي برامح حاسوبية خاصة بالتجسس ومراقبة المعلومات والمرسلة عبر الشبكة.

- انكار الخدمة: يقوم بإرسال كم هائل من الرسائل الالكترونية الى كمبيوتر معين عبر الشبكة والذي لا يستطيع التعامل معها وبالتالي تعطيل النظام.

حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية و يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة و تتمثل هذه الطوائف فيما يأتي:

**Pranksters**

الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية و المزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث). سبب التسمية: لتشابه عمله مع أسطورة حصان طروادة الخشبي الذي اختبأ به عدد من الجنود اليونانيون وكانوا سببا في فتح مدينة طروادة.

ينبغي أن نفهم أن الحاسوب تقريبا يشبه المدينة في القصة فله حائط (جدار ناري firewall/pare-feu) وله حاكم أو مستخدم هو أنت وله منافذ و أبواب والحصان هنا يشير الى البرامج والاشياء التي تقوم بتحميلها من الانترنت وتدخلها الى حاسوبك و الجيش الذي يختبئ في الحصان هو الفيروس.

**ما هو فيروس حصان طروادة Cheval de Troie :**

بالإنجليزيةTrojan Horse: هي شفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته.
حصان طروادة (اسم) برنامج كمبيوتر يبدو أنه مفيد ولكنه في الحقيقة يسبب الأضرار .
تنتشر أحصنة طروادة عندما ينخدع الأشخاص بفتحهم برنامجاً يعتقدون بأنه من مصدر شرعي. لحماية المستخدمين بشكل أفضل، تقوم Microsoft في كثير من الأحيان بإرسال نشرات متعلقة بالأمان بواسطة البريد الإلكتروني، ولكنها لا تتضمن مرفقات أبداً. كما يمكن تضمين أحصنة طروادة في البرامج التي تقوم بتحميلها مجاناً.

**طائفة الجرائم التي تستهدف الأفراد:**

**وتضم طائفتين رئيستين هما:**

**1- الجرائم غير الجنسية التي تستهدف الأفراد** Non-Sexual Crimes Against Persons وتشمل القتل بالكمبيوتر Computer Murder ، جرائم الاهمال المرتبط بالكمبيوتر Negligent Computer Homicide ، والتحريض على الانتحار Soliciting or Encouraging Suicide ، والتحريض القصدي للقتل عبر الانترنت Intentional Internet Homicide Solicitation والتحرش والمضايقة عبر وسائل الاتصال المؤتمتة Harassment via Computerized Communication والتهديد عبر وسائل الاتصال المؤتمتة Intimidation via Computerized Communication والاحداث المتعمد للضرر العاطفي او التسبب بضرر عاطفي عبر وسائل التقنية Malicious Infliction of Emotional Distress utilizing

Reckless Infliction of Emotional Distress و Computer Communication utilizing Computer Communication والملاحقة عبر الوسائل التقنية Stalking وانشطة اخلاس النظر او الاطلاع على البيانات الشخصية Online Voyeurism and Online Voyeurism Disclosure وقنابل البريد الالكتروني E-mail Bombing وانشطة ضخ البريد الالكتروني غير المطلوب او غير المرغوب به Spamming utilizing Computerized Communication وبث المعلومات المضللة او الزائفة Transmission of False Statements والانتهاك الشخصي لحرمة كمبيوتر ( الدخول غير المصرح به ) Personal trespass by computer

2- **طائفة الجرائم الجنسية Sexual Crimes :-** وتشمل حض وتحريض القاصرين على انشطة جنسية غير مشروعة Soliciting a Minor with a Computer for Unlawful Sexual Purposes وافساد القاصرين بأنشطة جنسية عبر الوسائل الالكترونية Corrupting a Minor with the use of a Computer for Unlawful Sexual Purposes. واغواء او محاولة اغواء القاصرين لارتكاب انشطة جنسية غير مشروعة Luring or Attempted Luring of a Minor by Computer for Unlawful Sexual Purposes وتلقي او نشر المعلومات عن القاصرين عبر الكمبيوتر من اجل انشطة جنسية غير مشروعة Receiving or Disseminating Information about a Minor by Computer for Unlawful Sexual Purposes والتحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية Sexually Harassing a minor by use of a Computer for Unlawful Sexual Purposes ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الانترنت بوجه عام وللقاصرين تحديدا .Posting Obscene Material On The Internet و Posting Or Receiving Obscene Material On The Internet و Trafficking In Obscene Material On The Internet و Sending Obscene Material To Minors Over The Internet ونشر الفحش والمساس بالحياء (هتك العرض بالنظر) عبر الانترنت Indecent Exposure On The Internet وتصوير او اظهار القاصرين

ضمن انشطة جنسية Depicting Minors Engaged In Sexually Explicit Conduct--Pandering Obscenity Involving A Minor واستخدام الانترنت لترويج الدعارة بصورة قسرية او للاغواء او لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم Using the Internet for Compelling Prostitution و Using the Internet for Pimping و Using the Internet for Soliciting و Using the Internet for Promoting Prostitution و الحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في انشطة جنسية Unauthorized Appropriation of Identity, Image, or Likeness for Unlawful Sexual Purposes .

بالنظر في هذه الاوصاف نجد انها تجتمع جميعا تحت صورة واحدة هي استغلال الانترنت والكمبيوتر لترويج الدعارة او اثارة الفحش واستغلال الاطفال والقصر في انشطة جنسية غير مشروعة.