الفصل الأول

الجريمة الإلكترونية

الفصل الأول

الجريمة الإلكترونية

مُقَدِّمَة:

الإنترنت بوابة بلا حراس. بل ساحة إجرام تتحدى الأجهزة الأمنية بثغرات قانونية ضخمة مما أتاح الفرصة لمافيا الجرائم الإلكترونية التجول خلالها دون رقيب أو حسيب وتمكن السرية أو الخصوصية التي تنطوي عليها لغة الكمبيوتر اللصوص من نقل المعلومات الخطرة أو المحظورة سواء معلومات مخابراتية أو خطط تخريبية أو صور سرية بمجرد الضغط على زر لوحة المفاتيح دون أدنى مجهود ودون الخوف من العقاب ويؤكد الخبراء أن الجرائم الإلكترونية تزداد كلما توغل العالم في استخدام الإنترنت وقد حققت هذه الجرائم خسائر فادحة بالاقتصاد الأمريكي قدرت بـ 250مليار سنويا ولم ينج العالم العربي من الجرائم الإلكترونية وان كانت الخسائر ليست على المستوى نفسه[1].

٢ـ المقصود بجرائم الكمبيوتر والإنترنت:

تعريف الجرمية عموما في نطاق القانون ن الجنائي "فعل غير مشروع صادر عن أداة جنائية يقرر لها القانون عقوبة أو تبرير" وعلى الرغم من تعدد الفقهاء في تعريف الجريمة وعناصرها فعناصر الجريمة السلوك والسلوك غير المشروع وفق القانون. الإرادة الجنائية ـ وإثرها ـ العقوبة أو التدبير الذي يفرضه القانون وفقا لتعريف الجريمة السابقة.

---

(١) موقع جريدة الرياض السعودية العدد ١٢٧٥٠ السنة ٣٩ موضوع " مافيا الإنترنت والجريمة الإلكترونية في الوطن العربي تزوير معلومات وإتلاف بيانات و احتيال وقريبا غسيل للأموال علي الإنترنت " من موقع الجريدة WWW.alriuadh.com .

إما جرائم الكمبيوتر ، فقد صك لها الفقهاء والدارسون عددا ليس بالقليل من التعريفات تتمايز وتتعدد تبعا لموضع العلم المنتمى إليها وتبعا لمعيار التعريف ذاته فهذه التعريفات تختلف بحسب ما إذا كانت منتمية للقانون الجنائي أم متصلة بالحياة الخاصة أم متعلقة بحقوق الملكية الفكرية أي حق التأليف البرمجي . وقد خلت المؤلفات الفقيه من تعريف اتجاهات جرائم الكمبيوتر إلا قليل منها ما يقوم على معيار واحد ، وهذه تشمل تعريفات قائمة على معيار قانوني ، كتعريفها بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة ، وتشمل أيضا تعريفات قائمة على معيار شخصي ، وتحديدا متطلب توفير المعرفة والدراية التقنية لدى شخص مرتكبها . وطائفة التعريفات القائمة على تعدد المعايير ، تشمل التعريفات التي تبرز موضوع الجريمة وأنماطها وبعض العناصر المتصلة بالبيانات[1].

ويعرف خبراء منظمون التعاون الاقتصادي والتنمية ، جريمة الكمبيوتر بأنها: " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها " .

وقد وضع هذا التعريف من قبل مجموعة الخبراء المشار إليهم للنقاش في اجتماع باريس الذي عقد عام 1983 ضمن حلقة " الإجرام المرتبط بتقنية المعلومات " ، ويتبنى هذا التعريف الفقيه الألماني Ulrich Sieher ، ويعتمد هذا التعريف على معيارين :

أولهما : " وصف السلوك " .

ثانيهم : " اتصال السلوك بالمعالجة الآلية بالبيانات أو نقلها " .

٣- تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة :

عرضنا فيها تقدم لدور الكمبيوتر في الجريمة ، فقد يكون هدف الاعتداء ، بمعنى أن يستهدف الفعل المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الكمبيوتر

(١) د سعيد عبد اللطيف حسن " الجرائم الواقعة في تكنولوجيا المعلومات " كلية الشريعة والقانون .

والشبكات، وهذا ما يعبر عنه بالمفهوم الضيق (لجرائم الكمبيوتر) وقد يكون وسيلة ارتكاب جريمة أخرى في إطار مفهوم (الجرائم المرتبطة بالكمبيوتر)، وقد يكون الكمبيوتر أخيرا بيئة الجريمة أو وسطها مخزنا للمادة الإجرامية، وفى هذا النطاق هناك مفهومان يجرى الخلط بينهما يعبران عن هذا الدور الأول جرائم التخزين، ويقصد بها تخزين المواد الإجرامية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها، والثاني: جرائم المحتوى أو ما يعبر عنه بالمحتوى غير المشروع أو غير القانوني والاصطلاح الأخير استخدم في ضوء تطور أشكال الجريمة مع استخدام الإنترنت، وأصبح المحتوى غير القانوني يرمز إلى جرائم المقامرة ونشر المواد الإباحية والغسيل الإلكتروني وغيرها باعتبار أن مواقع الإنترنت تتصل بشكل رئيسي بهذه الأنشطة، والحقيقة أن كلا المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفى نفس الوقت كوسيلة لارتكابها، وهذا التقسيم شائع بجزء منه وهو تقسيم الجرائم إلى جرائم هدف ووسيلة لدى الفقه المصري[1]. وتبعا له تنقسم جرائم الكمبيوتر إلى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات وإتلافها، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر. أما تقسيمها كجرائم هدف ووسيلة ومحتوى فانه الاتجاه العالمي الجديد في ضوء تطور التدابير التشريعية في أوروبا تحديدا، وأفضل ما يعكس هذا التقسيم الاتفاقية الأوروبية لجرائم الكمبيوتر والإنترنت لعام 2001 ذلك إن العمل منذ مطلع عام 2000 يتجه إلى وضع إطار عام لتصنيف جرائم الكمبيوتر والإنترنت وعلى الأقل وضع قائمة الحد الأدنى محل التعاون الدولي في حقل مكافحة هذه الجرائم، وهو جهد تقوده دول أوروبا لكن وبنفس الوقت بتدخل ومساهمة من قبل استراليا وكندا وأمريكا، وضمن هذه المفهوم نجد الاتفاقية المشار إليها تقسم جرائم الكمبيوتر والإنترنت إلى الطوائف التالية ـ مع ملاحظة أنها تخرج من بينها طائفة جرائم الخصوصية لوجود اتفاقية أوروبية مستقلة تعالج حماية البيانات الاسمية من مخاطر

(١) د جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، ١٩٩٢.

المعالجة الآلية للبيانات ـ اتفاقية 1981 .

لقد أوجدت الاتفاقية الأوربية تقسيما جديدا نسبيا ، فقد تضمنت أربع طوائف رئيسية لجرائم الكمبيوتر والإنترنت .

الأولى : الجرائم التي تستهدف عناصر (السرية والسلامة وموفورية) المعطيات والنظم وتضم :

- (الدخول غير قانوني)غير المصرح به .
- الاعتراض غير القانوني .
- تدمير المعطيات .
- اعتراض النظم .

الثانية : الجرائم المرتبطة بالكمبيوتر وتضم :

- التزوير المرتبط بالكمبيوتر .
- الاحتيال المرتبط بالكمبيوتر .

الثالثة : الجرائم المرتبطة بالمحتوى وتضم طائفة وفق هذه الاتفاقية وهى الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية[1] .

٤- تصنيف الجرائم تبعا لمساسها بالأشخاص والأموال:

نجد هذا التصنيف شائعا في الدراسات والأبحاث الأمريكية ـ مع فوارق بينها من حيث مشتملان التقسيم ومدى انضباطيته ، كما نجد المعيار لتقسيم جرائم الكمبيوتر والإنترنت في مشروعات القوانين النموذجية التي وضعت من جهات بحثية بقصد محاولة إيجاد الانسجام بين قوانين الولايات المتحدة المتصلة بهذا الموضوع ويعكس هذا الاتجاه التقسيم الذي تضمنه مشروع القانون النموذجي لجرائم الكمبيوتر والإنترنت

(١) المحامى يونس عرب تونس المرجع السابق في نفس الموضوع للدراسة تعريف جرائم الكمبيوتر .

الموضوع عام 1998الذي تم وضعه من قبل فريق بحثي أكاديمي والمسمى Model State Computer Crimes Code، وفى نطاقه تم تقسيم جرائم الكمبيوتر والإنترنت إلى الجرائم الواقعة على الأشخاص، والجرائم الواقعة على الأموال عدا السرقة، وجرائم السرقة والاحتيال والتزوير، وجرائم المقامرة والجرائم ضد الآداب ـ عدا الجرائم الجنسية، والجرائم ضد المصالح الحكومية ويلاحظ أن التقسيم يقوم على فكرة الغرض النهائي أو المحل نهائي الذي يستهدفه الاعتداء، لكنه ليس تقسيما منضبطا ولا هو تقسيم محدد الأطر، فالجرائم التي تستهدف الأموال تضم من حيث مفهومها السرقة والاحتيال، أما الجرائم التي تستهدف التزوير فتمس الثقة والاعتبار والجرائم الواقعة ضد الآداب قد تتصل بالشخص وقد تتصل بالنظام والأخلاق العامة، وعلى العموم فانه وتبعا لهذا التقسيم ـ الوارد ضمن مشروع القانون النموذجي الأمريكي ـ تصنيف جرائم الكمبيوتر على النحو التالي :

٥- طائفة الجرائم التي تستهدف الأشخاص:

وتضم طائفتين رئيسيتين هما :

الجرائم غير الجنسية التي تستهدف الأشخاص Non ــ Sexual Crimes Against Person وتشمل القتل بالكمبيوتر Computer Murder، والتسبب بالوفاة جرائم الإهمال المرتبط بالكمبيوتر Negligent Computer Homicide، والتحريض القصدي للقتل عبر الإنترنت International Internet Suicide Solicitation Homicideوالتحرش والمضايقة عبر وسائل الاتصال المؤتمنة Harassment via Computerized Communicationوالتهديد عبر وسائل الاتصال المؤتمنة Communication International via Computerized والأحداث المتعمد للضر العاطفي أو التسبب بضرر عاطفي عبر وسائل التقنية Malicious Infliction of Emotional Distress utilizing Computer Communicationو Reckless Infliction of Emotional Distress utilizing Computer والملاحقة عبر الوسائل التقنية Stalking وأنشطة اختلاس النظر أو الإطلاع على البيانات الشخصية Online Voyeurism and Online

Voyeurism Disclosure وقنابل البريد الإلكتروني E- mail Bombing وأنشطة ضخ البريد الإلكتروني غير المطلوب أو غير المرغوب به Spamming utilizing Computerized Communication وبث المعلومات المضللة أو الزائفة Transmission of False Statements والانتهاك الشخصي لحرمة الكمبيوتر (الدخول غير المصرح به Personal trespass by computer)

١ـ **طائفة الجرائم الجنسية** :Sexual Crimes وتشمل حض وتحريض القاصرين على أنشطة جنسية غير مشروعة Soliciting a Minor with a computer for Unlawful Sexual Purposes وإفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية Corrupting amino with the use of a computer for Unlawful Sexual Purposes وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة Luring or Attempted Luring Of Minor By computer for unlawful sexual purposes وتلقى أو نشر المعلومات عن القاصرين عبر الكمبيوتر من اجل أنشطة 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 الإنترنت بوجه عام وللقاصرين تحديدا Posting Obscene Material On The Internet Trafficking In obscene material on the internet و posting or receiving sending obscene material to و minors over obscene material on rhea internet indecent ونشر الفحش والمساس بالحياء)هتك العرض بالنظر (عبر الإنترنت the internet depicting وتصوير أو إظهار القاصرين ضمن أنشطة جنسية exposure on the inert minors engaged in sexually explicit conduct – pandering obscenity involving aminor using the internet for using the internt.

٢ ـ **طائفة جرائم الأموال** ـ عدا السرقة ـ أو الملكية المتضمنة أنشطة الاختراق

والإتلاف Property Damge and Crimes Involving Intrusions (Other than Theft).

وتشمل أنشطة اقتحام أو الدخول أو التوصل غير المصرح به مع نظام الكمبيوتر أو الشبكة إما مجردا أو لجهة ارتكاب فعل أخر ضد البيانات والبرامج والمخرجات Aggravated Computer Trespass و Disorderly Persons Offense و Computer Trespass وتخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب الكمبيوتر Computer Vandalism وإيذاء الكمبيوتر Computer Mischief واغتصاب الملكية Extortion وخلق البرمجيات الخبيثة والضارة Creation of Harmful Programs ونقلها عبر النظم والشبكات Transmission of Harmful Programs واستخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص Cyber squatting وزر إدخال معطيات خاطئة أو مزورة إلى نظام كمبيوتر Introduction False Into a Computer or Computer system ولا لتعديل غير المصرح به لأجهزة ومعدات الكمبيوتر Unlawful Modification of Computer Equipment or Supplies والإتلاف غير المصرح به لنظم الكمبيوتر (مهام نظم الكمبيوتر الأدائية Unlawful Modification of Computer) Equipment or Supplies و Unlawful Denial ، Interruption ، or Duration of Access to Computer Services وأنشطة الاعتداء على الخصوصية Computer Invasion of Privacy وهذه تخرج عن مفهوم الجرائم التي تستهدف الأموال لكنها تتصل بجرائم الاختراق (وإفشاء كلمة سر الغير Disclosure of Another's Password والحيازة غير المشروعة للمعلومات Unauthorized Possession of Computer Information وإساءة استخدام المعلومات Misuse of Computer Information ونقل معلومات خاطئة Transmission of False Data

٣ـ جرائم الاحتيال والسرقة Fraud and Theft Crimes :

وتشمل جرائم الاحتيال بالتلاعب بالمعطيات والنظم Fraud by Computer Manipulation واستخدام الكمبيوتر للحصول على أو استخدام البطاقات المالية للغير دون ترخيص Using a Computer to Fraudulently Obtain and Use Credit Card Information والاختلاس Damaging or Enhancing Another's Credit Rating عبر الكمبيوتر أو بواسطته Computer Embezzlement وسرقة معلومات الكمبيوتر Computer Information Theft وقرصنة البرامج Piracy (Software وسرقة خدمات الكمبيوتر)وقت الكمبيوتر Theft of Computer Services وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر .Computer Impersonation

٤ـ جرائم التزوير Forgery :

وتشمل تزويرا البريد الإلكتروني "E_ mail" Electronic Mail Forgery (Forgery) الوثائق والسجلات Document / Record Forgery وتزوير الهوية .Identity Forgery

٥ـ جرائم المقامرة وجرائم الأخرى ضد الأخلاق والآداب Gambling and Other Offenses Against Morality

وتشمل تملك وإدارة مشروع مقامرة على الإنترنت Owning and Operation an Internet Gambling business وتسهيل مشاريع القمار على الإنترنت Face-lifting the operation of an Internet gambling business وتشجيع مشروع مقامرة على الإنترنت Patronizing an Internet Gambling business واستخدام الإنترنت لترويج الكحول ومواد الإدمان للقصر Using the internet to provide liquor to minors و Using the internet to provide cigarettes to minors و Using the internet to provide prescription drugs.

٦ـ جرائم الكمبيوتر ضد الحكومة Crimes Against the Government

وتشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون obstruction enforcement of law or other government function والإخفاق في الإبلاغ عن جرائم الكمبيوتر Failure to report a cyber crimeوالحصول على معلومات سرية obtaining confident ional governmentوالأخبار الخاطئ عن جرائم الكمبيوتر False Reborts of Cybercrimesوالعبث بالأدلة القضائية أو التأثير فيها Tampering with evidenc و Tampering with a Computer Source Documentوتهديد السلامة العامة Endangering Public Safetyوبث البيانات من مصادر مجهولة Anonymityكما تشمل الإرهاب الإلكتروني Cyber – Terrorismوالأنشطة الثأرية الإلكترونية أو أنشطة تطبيق القانون بالذات .Cyber – Vigilantism [1].

تصنيف الجرائم كجرائم الكمبيوتر وجرائم الإنترنت:

ومن الطبيعي أن يكون ثمة مفهوم لجرائم ترتكب على الكمبيوتر وبواسطته قبل أن يشيع استخدام شبكات المعلومات وتحديدا الإنترنت، ومن الطبيعي أن تخلق الإنترنت أنماطا إجرامية مستجدة أو تأثر بالآلية التي ترتكب فيها جرائم الكمبيوتر ذاتها بعد أن تحقق تشبيك الكمبيوترات معا في نطاق شبكات محلية وإقليمية وعالمية، أو على الأقل تطرح أنماطا فرعية من الصور القائمة تختص بالإنترنت ذاتها، ومن هنا جاء هذا التقسيم، وسنجد انه كان مبررا من حيث المنطق فانه غير صحيح في الوقت الحاضر بسبب سيادة مفهوم نظام الكمبيوتر المتكامل الذي لا تتوفر حدود وفواصل في نطاقه بين وسائل الحواسب (ووسائل الاتصال)الشبكات.

وفى نطاق هذا المعيار يجرى التمييز بين الأفعال التي تستهدف المعلومات في نطاق الكمبيوتر ذاته ـ خلال مراحل المعالجة والتخزين والاسترجاع ـ وبين الأنشطة التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عبرها، وطبعا الأنشطة التي تستهدف مواقع الإنترنت وخادمها من نظم الكمبيوتر الكبيرة والعملاقة أو تستهدف تطبيقات

(١) المحامى يونس عرب تونس دراسة له عن جرائم الإنترنت من نفس المرجع السابق

واستخدامات وحلول الإنترنت وما نشا في بيئتها من إعمال إلكترونية وخدمات إلكترونية .

وفى إطار هذه الرؤية، (نجد البعض يحصر أنشطة جرائم الإنترنت بتلك المتعلقة بالاعتداء على المواقع وتعطيلها أو تشويهها أو تعطيل تقديم الخدمة) أنشطة إنكار الخدمة السابق بيانها وأنشطة تعديل وتحوير محتوى الموقع أو المساس بعنصري الموفورة والتكاملية أو سلامة المحتوى . وكذلك أنشطة المحتوى الضار، كترويج المواد الإباحية والمقامرة، وأنشطة إثارة الأحقاد والتحرش والإزعاج ومختلف صور الأنشطة التي تستخدم البريد الإلكتروني والمراسلات الإلكترونية، وأنشطة الاستيلاء على كلمات سر المستخدمين والهوية ووسائل التعريف، وأنشطة الاعتداء على الخصوصية عبر جمع المعلومات من خلال الإنترنت، وأنشطة احتيال الإنترنت كاحتيال المزادات وعدم التسليم الفعلي للمنتجات والخدمات، وأنشطة نشر الفيروسات والبرامج الخبيثة عبر الإنترنت، وأنشطة الاعتداء على الملكية الفكرية التي تشمل الاستيلاء على المواد والمصنفات المحمية وإساءة استخدام أسماء البطاقات أو الاستيلاء عليها أو استخدامها خلافا لحماية العلامة التجارية وأنشطة الاعتداء على محتوى المواقع والتصميم، (وأنشطة الروابط غير المشروعة وأنشطة الأطر غير المشروعة وهى أنشطة من خلالها أحد المواقع بإجراء مدخل لربط مواقع أخرى أو وضعها ضمن نطاق الإطار النموذجية لموقعه هو، وغيرها من الجرائم التي يجمعها مفهوم) جرائم الملكية الفكرية عبر الإنترنت .

أما جرائم الكمبيوتر فإنها وفق هذا التقسيم تعاد إلى الأنشطة التي تستهدف المعلومات والبرامج المخزنة داخل نظم الكمبيوتر وتحديدا أنشطة التزوير واحتيال الكمبيوتر وسرقة المعطيات وسرقة وقت الحواسب واعتراض المعطيات خلال النقل مع انه مفهوم يتصل بالشبكات أكثر من الكمبيوتر طبعا إضافة للتدخل غير المصرح به والذي يتوزع ضمن هذا التقسيم يسن دخول غير مصرح به لنظام الكمبيوتر ودخول غير مصرح به للشبكات فيتبع لمفهوم جرائم الإنترنت .

ولو وقفنا على هذا التقسيم فإننا بالضرورة ودون عناء سنجده غير دقيق وغير

منبط على الإطلاق، بل ومخالف للمفاهيم التقنية وللمرحلة التي وصل إليها تطور وسائل تقينة المعلومات وعمليات التكامل والدمج بين وسائل الحوسبة والاتصال، ففي هذه المرحلة، ثمة مفهوم عام لنظام الكمبيوتر يستوعب كافة مكوناته المادية والمعنوية المتصلة بعمليات الإدخال والمعالجة والتخزين والتبادل، مما يجعل الشبكات وارتباط الكمبيوتر بالإنترنت جزء من فكرة تكاملية النظام، هذا من جهة، ومن جهة أخرى، فان أنشطة الإنترنت تتطلب أجهزة الكمبيوتر تقارب بواسطتها، وهى تستهدف أيضا معلومات مخزنة ومعالجة ضمن أجهزة كمبيوتر أيضا هي الخادم التي تستضيف مواقع الإنترنت أو تديرها، وإذا أردنا إن نتحكم في فصل وسائل تقنية المعلومات، فان هذا لن يتحقق لان الشبكات ذاتها عبارة عن حلول وبرمجيات وبروتوكولات مدمجة في نظام الحوسبة ذاته إلا إذا أردنا أن نحصر فكرة الشبكات بالأسلاك وأجهزة التوجيه (الموجهات) وهذا يخرجنا من نطاق جرائم الكمبيوتر والإنترنت إلى جرائم الاتصالات التي تستهدف ماديات الشبكة، مشيرين هنا أن الموجهات التي قد يراها البعض تجهيزات تتصل بالشبكة ما هي في الحقيقة إلا برامج تتحكم بحركة تبادل المعطيات عبر الشبكة.

ويعدو المعيار غير صحيح البتة إذا ما عمدنا إلى تحليل كل نمط من أنماط الجرائم المتقدمة في ضوء هذا المعيار، فعلى سبيل المثال، تعد جريمة الدخول غير المصرح به لنظام الكمبيوتر وفق هذا المعيار جريمة كمبيوتر إما الدخول غير المصرح به إلى موقع إنترنت فإنها جريمة إنترنت، مع أن الحقيقة التقنية أن الدخول في الحالتين هو دخول إلى نظام الكمبيوتر عبر الشبكة، ولو أخذنا مثلا جريمة إنكار الخدمة وتعطيل عمل النظام، فسواء وجهت إلى نظام كمبيوتر أم موقع إنترنت فهي تستهدف نظام الكمبيوتر الذي هو في الحالة الأولى كمبيوتر مغلق وفى الثانية يدير موقع إنترنت.

حالات عملية شهيرة من واقع الملفات القضائية.

والأحداث الشهيرة في هذا الحقل كثيرة ومتعددة لكننا نكتفي في هذا المقام بإيراد ابرز الحوادث التي حصلت خلال السنوات الماضية بحيث نعرض لحوادث قديمة نسبيا وحديثة كأمثلة على تنامي خطر هذه الجرائم وتحديدا في بيئة الإنترنت.

قضية مورس:

هذه الحادثة هي أحد أول الهجمات الكبيرة والخطرة في بيئة الشبكات ففي تشرين الثاني عام 1988تمكن طالب يبلغ من العمر 23عاما ويدعى ROBER MORRIS من إطلاق فيروس عرف باسم (دورة مورس)عبر الإنترنت، أدى إلى إصابة 6 آلاف جهاز يرتبط معها حوالي 60000نظام عبر الإنترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار إضافة إلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم على مورس بالسجن لمدة 3 أعوام وعشرة آلاف غرامة.

قضية الجحيم العالمي:

تعامل مكتب التحقيقات الفدرالية مع قضية أطلق عليها اسم مجموعة الجحيم العالمي GLOBAL HELLفقد تمكنت هذه المجموعة من اختراق مواقع البيت الأبيض والشركة الفيدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية، وقد أدين اثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة، وقد ظهر من التحقيقات أن هذه المجموعة تهدف إلى مجرد الاختراق أكثر من التدمير أو التقاط المعلومات الحساسة، وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة.

فيروس ميلسا:

وفى حادثة هامة أخرى، انخرطت جهات تطبيق القانون وتنفيذه في العديد من الدول في تحقيق واسع حول إطلاق فيروس شرير عبر الإنترنت عرف باسم فيروس MELISSAحيث تم التمكن من اعتقال مبرمج الكمبيوتر من ولاية نيوجرسي في شهر نيسان عام 1999واتهم باختراق اتصالات عامة والتآمر لسرقة خدمات

الكمبيوتر ، وتصل العقوبات في الاتهامات الموجهة له إلى السجن لمدة 40 عام والغرامة التي تقدر بحوالي 500 ألف دولار وقد صدر في هذه القضية مذكرات اعتقال وتفتيش بلغ عددها 19 مذكرة .

حادثة المواقع الاستراتيجية:

وفى 19تشرين الثاني 1999تم إدانة Eric burnsمن قبل محكمة فيرجينيا الغربية بالحبس لمدة 15شهراً والبقاء تحت المراقبة السلوكية لمدة 3سنوات بعد أن اقر بذنبه وانه قام وبشكل متعمد باختراق كمبيوترات محمية الحق فيها ضررا بالغا في كل من ولايات فيرجينيا واشنطن وإضافة إلى لندن في بريطانيا ، وقد تضمن هجومه الاعتداء على مواقع لحلف الأطلسي إضافة إلى الاعتداء على موقع نائب رئيس الولايات المتحدة كما اعترف بأنه قد اطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق كمبيوترات البيت الأبيض ، وقد قام Ericبتصميم برنامج أطلق عليه web banditليقوم بعملية تحديد الكمبيوترات المرتبطة بشبكة الإنترنت التي تتوفر فيها نقاط ضعف تساعد على اختراقها ، وباستخدام هذا البرنامج اكتشف أن الخادم الموجود في فيرجينيا والذي يستضيف مواقع حكومية واستراتيجية منها موقع نائب الرئيس يتوفر فيه نقاط ضعف تمكن من الاختراق ، فقام في الفترة ما بين آب 1998وحتى كانون الثاني 1999باختراق هذا النظام 4مرات ، واثر نشاطه على العديد من المواقع الحكومية التي تعتمد على نظام وموقع USIAللمعلومات ، وفى إحدى المرات تمكن من جعل آلاف الصفحات من المعلومات غير متوفرة مما أدى إلى إغلاق هذا الموقع لثمانية أيام ، كما قام بالهجوم على مواقع لثمانين مؤسسة إعمال يستضيفها خادم شبكة LASER.NETفي منطقة فيرجينيا والعديد من مؤسسات الأعمال في واشنطن إضافة إلى جامعة واشنطن والمجلس الأعلى للتعليم في فيرجينيا رتشموند ومزود خدمات إنترنت في لندن ، كان عادة يستبدل صفحات المواقع بصفحات خاصة به تحت سام ZYKLONأو باسم لامرأة التي يحبها تحت اسم CRYSTAL .

الأصدقاء الأعداء:

وفى حادثة أخرى تمكن أحد الهاكرز (الإسرائيليين) من اختراق أنظمة معلومات حساسة في كل من الولايات المتحدة الأمريكية والكيان الصهيوني، فقد تمكن أحد المبرمجين في الولايات المتحدة وإسرائيل، وتم متابعة نشاطه من قبل عدد من المحققين في الولايات المتحدة الأمريكية حيث أظهرت التحقيقات أن مصدر الاختراقات هي كمبيوتر موجود في الكيان الصهيوني فانتقل المحققون إلى الكيان الصهيوني وتعاونت معهم جهات تحقيق إسرائيلية حيث تم التوصل للفاعل وضبطت كافة الأجهزة المستخدمة في عملية الاختراق، وبالرغم من أن المحققين أكدوا أن المخترق لم يتوصل إلى معلومات حساسة إلا أن وسائل الأعلام الأمريكية حملت أيضا أخبارا عن أن هذا الشخص كان في الأساس يقوم بهذه الأنشطة بوصفه عميلا لإسرائيل (ضد الولايات المتحدة الأمريكية).

حادثة شركة اوميغا:

مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لشركة (omega من مدينة Delawareويدعى Timothy (35عاما (تم اعتقاله في 17/2/1998)بسبب إطلاقه قنبلة إلكترونية في عام bomb 1996بعد 20يوما من فصله من العمل استطاعت أن تلغى كافة التصميم وبرامج الإنتاج لأحد كبرى مصانع التقنية العالية في نيوجرسي والمرتبطة والمؤثرة على نظم تحكم مستخدمة في nasalوالبحرية الأمريكية، ملحقا خسائر بلغت 10مليون دولار وتعتبر هذه المحادثة مثالا حيا على مخاطر جرائم التخريب في بيئة الكمبيوتر بل اعتبرت أنها أكثر جرائم تخريب الكمبيوتر خطورة على هذه الظاهرة.

وإلى جانب ما تم عرضه مقدماً فقد عرف المؤتمر المصري لجرائم المعلومات لعام ٢٠٠٦ الجريمة المعلوماتية تعريفات تستند إلى موضوع الجريمة :

ـ هي نشاط غير مشروع وجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات

المخزنة داخل الحاسب أو التي تحول عن طريقه .

ـ هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات .

ومن هذه التعريفات السابقة التي وضحها المؤتمر المصري لجرائم المعلومات يتضح أن تلك الجرائم هي المرتبطة بالنسخ أو التغيير للوصول إلى المعلومات المخزنة على الحاسب كاللص الذي يقوم بتغيير مفاتيح الخزينة ويبدلها للوصول إلى ما هو موجود بداخلها من مال أو مستندات تفيده فهي في التعريف الأول أشبه بالمثال السابق إما التعريف الثاني فهي ناتجة عن إدخال بيانات غير مملوكة لمن قام بإدخالها في أنظمة أجهزة الحاسبات للوصول للغرض المنشود وإساءة استخدام المخرجات .

تقسيم المجرم الإلكتروني:

يمكن تقسيم المجرم الإلكتروني إلى 3مجموعات :

أولاً : الموظفون العاملون بمراكز الكمبيوتر وهم يمثلون الغالبية العظمى من مرتكبي تلك الجرائم .

ثانيًا : الموظفون الساخطون على مؤسساتهم وهم يقومون باستخدام الكمبيوتر لمسح بعض المعلومات الخاصة بالشركة أو المؤسسة .

ثالثًا : الهاكرز **Hackers** أو كراكرز **Crackers** الذين يستغلون الكمبيوتر من اجل التسلية لاستخدام شبكة الإنترنت لتحقيق المزيد من الأرباح المشروعة . نجد جماعة الجريمة المنظمة يسعون لاستخدامها لتنفيذ عمليات غير مشروعة ولعل التطور المستمر للإنترنت وتوفر السرية جعل من الإنترنت جهازا مثاليا لتنفيذ الجرائم بعيداً عن أعين الأجهزة الأمنية[1] .

دور الإنترنت في حقل الجريمة

(١) موقع جريدة الرياض السعودية العدد ١٢٧٥٠ السنة ٣٩ موضوع " مافيا الإنترنت والجريمة الإلكترونية في الوطن العربي تزوير معلومات وإتلاف بيانات و احتيال وقريبا غسيل للأموال علي الإنترنت " من موقع الجريدة WWW.alriuadh.com المرجع السابق.

لعب الإنترنت أدوار ثلاثة في حقل الجريمة : فهو إما وسيلة متطورة لارتكاب الجرائم التقليدية بفعالية وسرعة اكبر من الطريق التقليدية كما في التزوير أو الاحتيال .

- أو هو الهدف الذي تتوجه إليه الأنماط الحديثة من السلوك الإجرامي التي تستهدف المعلومات ذاتها كما في اختراق النظم والدخول إليها دون تحويل وغيرها .
- أو هي البيئة بما تتضمنه من محتوى غير قانوني كالمواقع الخاصة بأنشطة ترويج المخدرات والأنشطة الإباحية وهو البيئة التخزينية والتبادلية التي تسهل ارتكاب الجرائم ، خاصة العابرة للحدود .

أضف إلى ذلك أن كشف الجرائم استلزم استخدام التقنيات الحديثة في عمليات التحري والتحقيق والكشف عن الأدلة الإجرامية ، من الطبيعي في ظل نشوء أنماط إجرامية تستهدف مصالح معترف بجمايتها إما لم تحظ بعد الاعتراف المطلوب ، وتستهدف محلا ذا طبيعة مغايرة لمحل الجريمة فيما عرفته قوانين العقوبات القائمة أن يتدخل المشرع الجنائي أو الجزائي لتوفير الحماية من هذه الأنماط الخطرة من الجرائم لضمان فاعلية مكافحتها)[1] .

(١) موقع جريدة الرياض المرجع السابق .