الإنترنت تعريفه بدايته و أشهر جرائمه

إلى كل من يسعى إلى تنمية ثقافته ومعلوماته .....

إلى من سمع بمصطلح الانترنت ورغب في معرفة المزيد منه.....

إليكم جميعاً هذه العمل المتواضع جداً لعله يكون الشمعة الأولى لإنارة الطريق في عالم الانترنت.

مقدمة:

لا يخفى على احد ما تمثله الثقافة العامة من أهمية للأشخاص بشكل عام، ولرجل الأمن بشكل خاص، و نظراً لانتشار تقنية الانترنت بشكل سريع وواسع استلزم معه الإلمام بشيء بسيط عن هذه التقنية تمهيدا للأخذ بها واستغلالها في خدمة الأهداف الأمنية.

ومن هنا جاءت هذه الورقة البحثية الموجزة كمحاولة مختصرة لتبسيط مفهوم الانترنت وتعريف الفيروسات الحاسوبية والاختراقات كوتهما من أهم الجرائم التي ترتكب في شبكة الانترنت، وان كانت هناك العديد من جرائم الانترنت التي ظهرت كنمط حديث أفرزته التقنية الحديثة، والتي لا يسع المجال هنا للتطرق لها، ولعلنا نفرد لها بحث آخر إن شاء الله وسيكتفى هنا بالتعريف بالانترنت وبداياته وكيفية عمله ومستلزمات استخدامه ومن ثم التطرق إلى تعريف بأشهر جرائمه وهي جرائم الفيروسات الحاسوبية وجرائم الاختراقات.

تعريف الإنترنت وبداياته واستخداماته :

يمكن الدخول إلى الشبكة العالمية والمعروفة بالانترنت بواسطة جهاز الحاسب الآلي، فما هو تعريف الإنترنت وكيف بدأ :

أولا ما هي الشبكة : وظيفة أي شبكة هي تيسير المشاركة في المعلومات والبرامج وغيرها من موارد النظام بين عدد كبير من المستخدمين والشبكات علي نوعين :

١- الشبكات المحلية (LAN) (LOCAL AREA NETWORKS) تستخدم داخل منطقة معينة أو حيز معين.

٢- الشبكات علي نطاق واسع (WIDE AREA NETWORKS)(WAN) تربط بين عدة شبكات محلية معا في إطار واحد باستخدام التلفون أو القمر الصناعي أو الميكروويف.

ثانيا : تعريف الإنترنت : "الإنترنت هو جزء من ثورة الاتصالات ويعرف البعض الإنترنت بشبكة الشبكات في حين يعرفها البعض الآخر بأنها شبكة طرق المواصلات السريعة، ويمكن تعريف الإنترنت بشبكة الشبكات" (ابوالحجاج، ١٩٩٨م، ص ١٨)

بداية الإنترنت: بدأ الإنترنت في ١٩٦٩/١/٢ عندما شكلت وزارة الدفاع الأمريكية فريقا من العلماء للقيام بمشروع بحثي عن تشبيك الحاسبات وركّزت التجارب علي

تجزئة الرسالة المراد بعثها إلى موقع معين في الشبكة ومن ثم نقل هذه الأجزاء بشكل وطرق مستقلة حتى تصل مجّمعة إلى هدفها وكان هذا الأمر يمثل أهمية قصوى لأمريكا وقت الحرب ففي حالة نجاح العدو في تدمير بعض خطوط الاتصال في منطقة معينة فان الأجزاء الصغيرة يمكن أن تواصل سيرها من تلقاء نفسها عن أي طريق آخر بديل إلى خط النهاية. ومن ثم تطور المشروع وتحول إلى الاستعمال السلمي حيث انقسم عام ١٩٨٣ إلى شبكتين احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) كما احتفظت بغرضها الأساسي وهو خدمة الاستخدامات العسكرية . وسميت الشبكة الثانية باسم (MILNET) للاستخدامات المدنية أي تبادل المعلومات وتوصيل البريد الإلكتروني ومن ثم ظهر المصطلح " الإنترنت " حيث أمكن تبادل المعلومات بين هاتين الشبكتين. وفي عام ١٩٨٦ أمكن ربط شبكات خمس مراكز للكمبيوترات العملاقة وسميت (NSFNET) والتي أصبحت العمود الفقري وحجر الأساس لنمو وازدهار الإنترنت في أمريكا ومن ثم دول العالم الأخرى.

من يملك الإنترنت؟؟ لا أحد في الوقت الراهن يملك الإنترنت ففي البداية يمكن القول بان الحكومة الأمريكية ممثلة في وزارة الدفاع ثم المؤسسة القومية للعلوم هي المالك الوحيد للشبكة ولكن بعد تطور الشبكة ونموها لم يعد هناك مالك لها واختفي مفهوم التملك ليحل محله ما أصبح يسمي بمجتمع الإنترنت كما أن تمويل الشبكة تحول من القطاع الحكومي إلى القطاع الخاص. ومن هنا ولدت العديد من الشبكات الإقليمية ذات الصبغة التجارية حيث يمكن الاستفادة من خدماتها مقابل اشتراك. (أبو الحجاج ١٩٩٨م).

توسع الشبكة: في عام ١٩٨٥م كان هناك اقل من ألفي حاسوب آلي مرتبط بالشبكة وفي عام ١٩٩٥م وصل العدد إلى (٥) مليون حاسوب وفي عام١٩٩٧م تتجاوز حاجز الـ (٦) مليون وتستخدم ما يزيد علي (٣٠٠) ألف خادم (SERVER) أي شبكة فرعية متناثرة في أرجاء العالم,ويمكن القول بان عدد المستخدمين الجدد يبلغ (٢) مليون شهريا أي ما يعني انضمام (٤٦) مستخدم جديد للشبكة في كل دقيقة (السيد ، ١٩٩٧ م).

وفي استطلاع أجرته شبكة (NUA) الأمريكية قدر عدد مستخدمي الشبكة عالميا بحوالي (١٣٤) مليون مستخدم في العام ١٩٩٨م وتصدرت الولايات المتحدة الأمريكية وكندا الصدارة حيث من حيث عدد المستخدمين الذي بلغ (٧٠) مليون مستخدم (NUA , (1998).

وفي تقرير أخير صدر بتاريخ ٢٦ أكتوبر ٢٠٠٠ م قدّر عدد المستخدمين للشبكة عام ٢٠٠٥ بحوالي (٢٤٥) مليون مستخدم وان غالبية هذه الزيادة ستكون خارج الولايات المتحدة الأمريكية (NUA ,10. 2000)

كما أوضح مسح ميداني اجري بتاريخ ٦ نوفمبر ٢٠٠٠ على (٢٥٠٠) مستخدم للانترنت في كلا من أمريكا وبريطانيا وألمانيا واستراليا وفرنسا أن متوسط استخدام الإنترنت (٤,٢) ساعة أسبوعيا في أمريكا و (٣,٢) ساعة في أوروبا و (٣,٦) ساعة في استراليا . وان (٤٤٪) من مستخدمي الشبكة في أمريكا يتصلون

بها من منازلهم مقابل (٣٨٪) في استراليا و (٣١٪) في بريطانيا وألمانيا في حين تبلغ النسبة في فرنسا (١٦٪) (NUA ,11. 2000)
وقد أشار الرئيس الأمريكي إلى أن هناك مشروع مستقبلي لتطوير شبكة الإنترنت باسم (الإنترنت ٢) أو الجيل الثاني من الإنترنت فكان مما قاله " لا بد من أن نبني الجيل الثاني لشبكة الإنترنت لتتاح الفرصة لجامعاتنا الرائدة ومختبراتنا القومية للتواصل بسرعة تزيد ألف مرة من سرعات اليوم، وذلك لتطوير كل من العلاجات الطبية الحديثة ومصادر الطاقة الجديدة، وأساليب العمل الجماعي " (أفاق الإنترنت ، ١٩٩٧)
وقد ظهر حديثا ما يشير إلى أن هناك في هذه الأيام سباق فضاء من نوع آخر حيث استطاعت شركة ستارباند (Starband) في تجربه أجرتها في شمال أميركا من إكمال مشروع انترنت أقمار اصطناعية ذو اتجاهين وسرعته كما أوردته الشركة هي (٥٠٠) ك.ب في الثانية من الإنترنت إلى الحاسوب وسيبدأ تسويقه إلى المستهلك ويذكر انه يقف وراء هذه المشروع أكثر من شركة متخصصة في هذا المجال وهي: (Microsoft ,Echostar and Ing Furman Selz Investments)

بروتوكولات الإنترنت :

حتى تستطيع إقامة اتصال بين الحاسوبات المختلفة فان الأمر يتطلب وجود مجموعة من القواعد المتفق عليها والمعروفة باسم البروتوكولات، وقد تنوعت أسماء هذه البروتوكولات بين الأسماء الطريفة مثل جوفر (Gopher) والأسماء الطويلة المزعجة التي تم اختصارها مثل بروتوكول نقل النص المتشعب (HTTP) بدلا من(Transfer Protocol Hypertext) أو بروتوكول التحكم في النقل (TCP/IP) بدلا عن مسماه الطويل (Transmission Control Protocol/Internet Protocol)

فما هي هذه البرتوكولات وما هي وظائفها :

أولا : بروتوكول الإنترنت (IP) (Internet Protocol) أحد أهم البروتوكولات الأساسية والـ (IP) عبارة عن رقم مكون من أربعة أجزاء، يعرّف الجزء الأول من الرقم بدءاً من اليسار المنطقة الجغرافية، والجزء الثاني يحدد المنظمة أو الحاسوب المزود، أما المجموعة الثالثة من الأرقام فتحدد مجموعة الكمبيوترات التي ينتمي إليها الجهاز، والمجموعة الرابعة يحدد الجهاز المستخدم. ويمكن اعتبار الـ (IP) نوع من الخرائط الخاصة بالانترنت، حيث يمكن الاتصال بأي حاسوب أو بأي موقع من خلال نقطة معينة على هذه الخريطة.

ثانيا : لغة ترميز النص التشعبي وبروتوكول نقل النص التشعبي (Language and HTML Hypertext Markup and hypertext Transfer Protocol (HTTP)

يتحكم (HTML) و (HTTP) معا في الشبكة العنكبوتية (WWW) فـ الـ(HTML) طريقة لإضافة تنسيق إلى ملفات النصوص بحيث يمكنك رؤية أشياء مثل العناوين، والكلمات المراد تحديدها للفت الانتباه، والفقرات التي يتم توسيطها بالصفحة، والصورة المدرجة داخل النص، وذلك عند استخدامك لمستعرض ويب (HTML)أما (HTTP) فهو بروتوكول يقوم بتعريف كيفية إرسال و استقبال ملفات (HTML)

ثالثا: بروتوكول التحكم في النقل(Transmission Control Protocol) أو ما يعرف اختصارا بـ(TCP) هو البروتوكول الذي يعرِّف البناء الخاص بالبيانات وكيفية إرسالها بين الحاسوبات،وعادة يتم تقسيم هذه البيانات إلى أجزاء عند إرسالها، ومن ثم يعمد إلى إعادة تجميعها وإعادتها إلى ترتيبها الأصلي عند وصولها إلى نقطة النهاية. ونظرا لاشتراك البروتوكول (TCP) و (IP) فقد جرى العمل عادة إلى الإشارة إليهما مجتمعين بـ (TCP/IP)

رابعا: تلنت (Telnet) : هو بروتوكول يقوم يتيح لك تشغيل جهاز آخر من خلال جهازك. فعندما تستخدم برنامج (Telnet) يمكنك الدخول إلى كمبيوتر آخر وتشغيل برامج كما لو كنت تجلس أمامه.

خامسا: جوفر (Gopher) يتم عرض محتويات الجهاز الخادم الذي يستخدم بروتوكول (Gopher) على هيئة قوائم فرعية ويمكنك اختيار أي عنصر من عناصر هذه القوائم. وما يميز هذا البروتوكول هو إعطاء المستخدم إمكانية اختيار أي عنصر من عناصر هذه القوائم ولو كانت على خادم (Gopher) آخر يختلف عن الخادم الذي قدم لك القائمة الأولى.

سادسا : بروتوكول نقل أخبار الشبكة: (Network News Transfer Protocol)والمعروف اختصارا بـ(NNTP) تقوم أجهزة الخادم الخاصة بـيوزنت (UseNet) بتخزين الرسائل وتبادلها باستخدام بروتوكول (NNTP) وبهذه الطريقة يستطيع العديد من الأفراد قراءة و إرسال الرسائل إلى هذه الأجهزة الخادمة باستخدام برنامج لقراءة الأخبار.

مستلزمات الاتصال بالشبكة:

حاسب إلى ٢- مودم ٣- الاشتراك في الخدمة ٤- برامج تصفح الشبكة

خدمات الإنترنت:

١- البريد الإلكتروني :لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص له عنوان بريدي بصورة سريعة جدا لا تتعدى دقائق .

٢- قوائم العناوين البريدية : تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعات من الأشخاص لهم اهتمامات مشتركة .

٣- خدمة المجموعات الإخبارية: تشبه خدمة القوائم البريدية باختلاف أن كل عضو يستطيع التحكم في نوع المقالات التي يريد استلامها.

٤- خدمة الاستعلام الشخصي : يمكن الاستعلام عن العنوان البريدي لأي شخص أو هيئة تستخدم الإنترنت والمسجلين لديها.

٥- خدمة المحادثات الشخصية : يمكن التحدث مع طرف آخر صوتا وصورة وكتابة.
٦- خدمة الدردشة الجماعية : تشبه الخدمة السابقة إلا انه يمكن التحدث مع أكثر من شخص في نفس الوقت حيث يمكن تنظيم مؤتمر لعدد من الأفراد.
٧- خدمة تحويل أو نقل الملفات : لنقل الملفات من حاسب إلى آخر (FTP) وهي اختصار (FILE TRANSFER PROTOCOL).
٨- خدمة الأرشيف الإلكتروني :(ARCHIE) يمكن البحث عن ملفات معينة قد تكون مفقودة في برامجك المستخدمة في حاسبك .
٩- خدمة شبكة الاستعلامات الشاملة : (GOPHER) يسمح للمستخدم بتشغيل والاستفادة من خدمات الكثير من الموارد الأخرى مثل خدمة نقل الملفات وخدمة المشاركة في قوائم العناوين البريدية حيث يفهرس المعلومات الموجودة علي الشبكة
١٠- خدمة الاستعلامات واسعة النطاق : (WAIS) تسمي هذه الخدمة باسم حاسباتها الخادمة نفسها وهي أكثر ذكاء ودقة وفاعلية من الأنظمة الأخرى حيث تبحث داخل الوثائق أو المستندات ذاتها عن بعض الكلمات المحورية أو الدالة التي يحددها المستخدم ثم تقدم نتائج البحث في شكل قائمة بأسماء المواقع التي تحتوي علي المعلومات المطلوبة.
١١- خدمة الدخول عن بعد : (TELNET) تسمح باستخدام برامج وتطبيقات في الحاسب الآلي الآخر .
١٢- الصفحة الإعلامية العالمية : (WWW) (WORLD WIDE WEB) وتسمي أيضا الويب (WEB) : تجمع معا كافة الموارد المتعددة التي تحتوي عليها الإنترنت للبحث عن كل ما تريد في الشبكات المختلفة وإحضارها بالنص والصوت والصورة و الويب نظاما فرعيا من الإنترنت لكنها النظام الأعظم من الأنظمة الأخرى فهي النظام الشامل باستخدام الوسائط المتعددة

برامج التصفح المتوفرة :

هناك العديد من برامج تصفح الانترنت، أهمها:

١- NETSCAPE
٢- INTERNET EXPLORER
٣- MOSAIC

الفيروسات الحاسب آلية :

الفيروسات الحاسب آلية هي إحدى أنواع البرامج الحاسب الآلية، إلاّ أنّ الأوامر المكتوبة في هذه البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما، أو حتى مجرد فتح البرنامج الحامل للفيروس، أو الرسالة البريدية المرسل معها الفيروس، إصابة الجهاز به ومن ثَمّ قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به. وقد عرّفها أحد خبراء الفيروسات (Fred Cohen) بأنّها نوع من البرامج التي تؤثّر في البرامج الأخرى، بحيث تعدّل في تلك البرامج لتصبح نسخة منها، وهذا يعنى ببساطة أنّ

الفيروس ينسخ نفسه من حاسب آلي إلى حاسب آلي آخر، بحيث يتكاثر بأعداد كبيرة (Highley,1999).
ويمكن تقسيم الفيروسات إلى خمسة أنواع :
الأول: فيروسات الجزء التشغيلي للاسطوانة كفيروس (Brain) و(Newzeland).
الثاني: الفيروسات المتطفلة كفيروس (Cascade) وفيروس (Vienna).
الثالث: الفيروسات المتعددة الأنواع كفيروس (Spanish-Telecom) وفيروس (Flip).
الرابع:الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوس أو الوندوز.
الخامس: يعرف بحصان طروادة، وهذا النوع يصنّفه البعض كنوع مستقّل بحد ذاته، إلاّ أنّه أدرج في هذا التقسيم كأحد أنواع الفيروسات، وينسب هذا النوع إلى الحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاء سلمي إلا أنّ أثره التدميري خطير.
وتعمل الفيروسات على إخفاء نفسها عن البرامج المضادة للفيروسات باستخدام طرق تشفير لتغيّر أشكالها، لذلك وجب تحديث برامج مكافحة الفيروسات بصفة دائمة (عيد،١٤١٩هـ : ٦٣-٦٦).
ويختلف الخبراء في تقسيمهم للفيروسات، فمنهم من يقسمّها على أساس المكان المستهدف بالإصابة داخل جهاز الكمبيوتر، ويرون أنّ هناك ثلاثة أنواع رئيسة من الفيروسات هي: فيروسات قطاع الإقلاع(Boot Sector) وفيروسات الملفات(File Injectors)وفيروسات الماكرو(macro Virus).
وهناك من يقسّمها إلى: فيروسات الإصابة المباشرة (Direct action) وهي التي تقوم بتنفيذ مهمتها التخريبية فور تنشيطها، أو المقيمة (staying) وهي التي تظل كامنة في ذاكرة الكمبيوتر وتنشط بمجرد أن يقوم المستخدم بتنفيذ أمر ما، ومعظم الفيروسات المعروفة تندرج تحت هذا التقسيم، وهناك أيضاً الفيروسات المتغّيرة (Polymorphs) التي تقوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلّل برامج مكافحة الفيروسات (موقع جريدة الجزيرة ،٢٠٠٠).
ومن الجرائم المتعلقة بإرسال فيروسات حاسوبية قيام شخص أمريكي يدعى (Robert Morris) بإرسال دودة حاسوبية بتاريخ الثاني من نوفمبر عام (١٩٨٨م) عبر الإنترنت، وقد كرّر الفيروس نفسه عبر الشبكة بسرعة فاقت توقع مصمم الفيروس وأدى ذلك إلى تعطيل ما يقارب من (٦٢٠٠) ستة آلاف ومائتي حاسبٍ آلي مرتبط بالإنترنت، وقد قدرّت الأضرار التي لحقت بتلك الأجهزة بمئات الملايين من الدولارات. ولو قُدّر لمصمم الفيروس تصميمه بحيث يكون أشدّ ضرراً، للحقت أضرار أخرى لا يمكن حصرها بتلك الأجهزة، وقد حُكم على المذكور بالسجن ثلاث سنوات بالرغم من دفاع المذكور عن نفسه أنّه لم يكن يقصد إحداث مثل تلك الأضرار(Morningstar, 1998).

كيف يتم اقتحام الجهاز؟

لتتم عملية الاقتحام يجب زرع حصان طروادة في جهاز الضحية بعدة طرق منها:

١. يرسل عن طريق البريد الإلكتروني باعتباره ملفاً ملحقاً حيث يقوم الشخص باستقباله وتشغيله، وقد لا يرسل وحده حيث من الممكن أن يكون ضمن برامج، أو ملفات أخرى.

٢. عند استخدام برنامج المحادثة الشهير (ICQ) وهو برنامج محادثة أنتجته إسرائيل.

٣.عند تحميل برنامج من أحد المواقع غير الموثوق بها وهي كثيرة جدا.

٤.طريقة أخرى لتحميله، تتلخّص في مجرد كتابة كوده على الجهاز نفسه في دقائق قليلة.

٥.في حالة اتصال الجهاز بشبكة داخلية أو شبكة إنترانت.

٦.يمكن نقل الملف أيضاً بواسطة برامج (FTP) أو (Telnet) الخاصة بنقل الملفات.

٧.كما يمكن الإصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكرو الموجود في برامج معالجة النصوص (Nanoart,2000).

وبصفة عامة فإن برامج القرصنة تعتمد كلياً على بروتوكول الـ (TCP/IP) وهناك أدوات (ActiveX) مصمّمه ومجهّزة لخدمة التعامل بهذا البروتوكول، ومن أشهرها (WINSOCK.OCX) لمبرمجي لغات البرمجة الداعمة للتعامل مع هذه الأدوات. ويحتاج الأمر إلى برنامجين، خادم في جهاز الضحية، وعميل في جهاز المتسلل، فيقوم الخادم بفتح منفذ محدد مسبقاً في جهاز الضحية ، في حين يكون برنامج الخادم في حالة انتظار لحظة محاولة دخول المخترق لجهاز الضحية، حيث يتعرف برنامج الخادم (server) على إشارات البرنامج المخترق، ويتم الاتصال، ومن ثَمّ يتمّ عرض كامل محتويات جهاز الضحية عند المخترق، حيث يتمكّن من العبث بها أو الاستيلاء على ما يريد منها .

فالمنافذ (Ports) يمكن وصفها ببوابات للجهاز، وهناك ما يقارب الـ(٦٥,٠٠٠) منفذ تقريباً في كل جهاز، يميّز كلّ منفذ عن الآخر برقم خاص ولكلّ منها غرض محدد، فمثلاً المنفذ (٨٠٨٠) يخصص أحياناً لمزود الخدمة، وهذه المنافذ غير مادية مثل منفذ الطابعة، وتعدّ جزءاً من الذاكرة، لها عنوان معين يتعرف عليها الجهاز بأنّها منطقة إرسال واستقبال البيانات، وكلّ ما يقوم به المتسلل هو فتح أحد هذه المنافذ للوصول لجهاز الضحية وهو ما يسمى بطريقة الزبون/الخادم (Client\Server) حيث يتمّ إرسال ملف لجهاز الضحية، يفتح المنافذ فيصبح جهاز الضحية (server)، وجهاز المتسلل (Client)، ومن ثَمّ يقوم المتسلل بالوصول لهذه المنافذ باستخدام برامج كثيرة متخصصة كبرنامج (Net Bus) أو (Net Sphere).

ولعلّ الخطورة الإضافية تكمن في أنّه عند دخول المتسلل إلى جهاز الضحية فإنّه لن يكون الشخص الوحيد الذي يستطيع الدخول لذلك الجهاز، حيث يصبح ذلك الجهاز

مركزاً عاماً يمكن لأي شخص الدخول عليه بمجرد عمل مسح للمنافذ (Port scanning) عن طريق أحد البرامج المتخصصة في ذلك.

خطورة برامج حصان طروادة:

بداية تصميم هذه البرامج كان لأهداف نبيلة، كمعرفة ما يقوم به الأبناء، أو الموظفون، على جهاز الحاسب في غياب الوالدين، أو المدراء، وذلك من خلال ما يكتبونه على لوحة المفاتيح، إلا أنّه سرعان ما أسيء استخدامه. وتعدّ هذه البرامج من أخطر البرامج المستخدمة من قبل المتسللين، لأنّه يتيح للدخيل الحصول على كلمات المرور (passwords)، وبالتالي الهيمنة على الحاسب الآلي بالكامل. كما أنّ المتسلل لن يتمّ معرفته أو ملاحظته لأنّه يستخدم الطرق المشروعة التي يستخدمها مالك الجهاز. كما تكمن الخطورة أيضاً في أنّ معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات، إضافة إلى أنّ الطبيعة الساكنة لحصان طروادة يجعلها أخطر من الفيروسات، فهي لا تقوم بتقديم نفسها للضحية مثلما يقوم الفيروس الذي دائما ما يمكن ملاحظته من خلال الإزعاج، أو الأضرار التي يقوم بها للمستخدم، وبالتالي فإنه لا يمكن الشعور بهذه الأحصنة أثناء أدائها لمهمتها التجسسية، وبالتالي فإنّ فرص اكتشافها، والقبض عليها تكاد تكون معدومة (Nanoart,2000).

أهم المنافذ المستخدمة لاختراق الجهاز:

إذن فأهمّ مورد لهذه الأحصنة هي المنافذ (Ports) التي تقوم بفتحها في جهاز الضحية ومن ثمّ التسلل منها إلى الجهاز والعبث بمحتوياته. فما هذه المنافذ؟ سنحاول هنا التطرّق بشكل إجمالي إلى أهم المنافذ التي يمكن استخدامها من قبل المتسللين، والبرامج المستخدمة في النفاذ من هذه المنافذ :

المنفذ	اسم البرنامج
21	blade Runner , doly Trojan ,FTP Trojan , Invisible FTP , Larva ,WebEX , Win Crash
23	Tiny Telnet Server
25	Antigen , Email Password Sender , Haebu Coceda , Kauang 2 , Pro Mail trojan , Shtrilitz , Stealth , Tapirs ,Terminator , Win Pc ,Win Spy ,Kuang20.17A-0.30
31	Agent 31 , Hackers Paradise , Master Paradise
41	Deep Throat
58	DMSetup
79	Fire hotcker
80	Executor
110	Pro Mail trojan

121	Jammer Killah
421	TCP wrappers
456	Hackers Paradise
531	Rasmin
555	Ini Killer , Phase Zero , Stealth Spy
666	Attack FTP ,Satanz BackDoor
911	Dark Shadow
999	Deep Throat
1001	Silencer , WEBEX
1011 1012	Doly Trojan
1024	Net Spy
1045	Rasmin
1090	Xtreme
1095 1097 1098 1099	Rat
1170	Psyber Stream Server , Voice
1234	Ultors Trojan
1243	Back Door -G , SubSeven
1245	VooDoo Doll
1349	UPD – BO DLL
1492	FTP99CMP
1600	Shivka – Burka
1807	Spy Sender
1981	Shockrave
1999	Back Door
2001	Trojan Cow
2023	Ripper
2115	Bugs

2140	Deep Throat , The Invasor
2565	Striker
2583	Win Crash
2801	Phineas Phucker
3024	Win crash
3129	Master Paradise
3150	Deep Throat , The Invasor
3700	Portal Of Doom
4092	Win crash
4567	File Nail
4590	ICQ Trojan
5000	Bubbel , Back Door Setup , Sockets de troie
5001	Back Door Setup , Sockets de troie
5321	Fire hotcker
5400 5401 5402	Blade Runner
5555	ServeMe
5556 5557	Bo Facil
5569	Robo-Hack
5742	Win Crash
6400	The Thing
6670	Deep Throat
6711	SubSeven
6771	Deep Throat
6776	Back Door-G , SubSeven
6939	Indoctrination
6969	Gate Crasher , Priority
7300 7301	Net Monitor

7306 7307 7308	
7000	Remote Grab
7789	BacK Door Setup , ICKiller
9872 9873 9874 9875 10067 10167	Portal of Doom
9989	iNi – Killer
10520	Acid Shivers
10607	Coma
11000	Senna Spy
11223	Progenic trojan
12223	Hack 99 Key Logger
12345	Pie Bill Gates , X -billNet busGaban Bus
12346	X-billNet BusGaban Bus
12361 12362	Whack – a – mole
12631	WhackJob
13000	Senna Spy
16969	Priority
20001	Millennium
20034	NetBus 2 Pro
21544	Girl Friend
22222	Prosiak
23456	Evil Ftp , Ugly FTP
26274	UPD – Delta Source
29891	UPD - The Unexplained
30029	AOL Trojan

30100 30101 30102	NetSphere
30303	Sockets de Troie
31337	Baron Night , BO client ,Bo2 , Bo Facil UPD - BackFire , Back Orifice , DeppBo
31338 31339	NetSpy DK
31338	UPD - Back Orific , Deep BO
31666	Bo Whack
33333	Prosiak
34324	Big Gluck , TN
40412	The Spy
40421	Agent 40421 , Master Paradise
40422 40423 40426	Master Paradise
47262	UPD –Delta Source
50505	Sockets de Troie
50766	Fore
53001	Remote Windows Shutdown
54321	School Bus
60000	Deep Throat
61466	Telecommando
65000	Devil

المصدر موقع (http://www.nanoart.f2s.com/hack/ports3.htm)

أهم برامج الاختراق:

١. **برنامج** (Sub Seven) : أخطر برامج الاختراق يسمى في منطقة الخليج (الباكدور جي) ويطلق عليه البعض اسم القنبلة. تتركز خطورته في أنه يتميز بمخادعة الشخص الذي يحاول إزالته فهو يعيد تركيب نفسه تلقائيا بعد حذفه ويعتبر أقوى برنامج اختراق للأجهزة الشخصية وفي إصدارته الأخيرة يمكنه أن يخترق سيرفر لقنوات المحادثة (Mirc) كما يمكنه اختراق جهاز أي شخص بمجرد معرفة

اسمه في (ICQ) كما يمكنه اختراق مزودات البريد (smtp/pop3) يعتبر الاختراق به صعب نسبيا وذلك لعدم انتشار ملف التجسس الخاص به في أجهزة المستخدمين إلا أنه قائما حاليا على الانتشار بصورة مذهلة ويتوقع أنه بحلول منتصف عام ٢٠٠١ سوف تكون نسبة الأجهزة المصابة بملف السيرفر الخاص به (٤٠-٥٥ ٪) من مستخدمي الإنترنت حول العالم وهذه نسبة مخيفة جدا إذا تحققت فعلا وهذا البرنامج خطير للغاية فهو يمكن المخترق من السيطرة الكاملة على الجهاز وكأنه جالس على الجهاز الخاص به حيث يحتوي البرنامج على أوامر كثيرة تمكنه من السيطرة علي جهاز الضحية بل يستطيع أحيانا الحصول على أشياء لا يستطيع مستخدم الجهاز نفسه الحصول عليها مثل كلمات المرور فالمخترق من هذا البرنامج يستطيع الحصول على جميع كلمات المرور التي يستخدمها صاحب الجهاز !!! ومن أهم أعراض الإصابة بهذا البرنامج ظهور رسالة " قام هذا البرنامج بأداء عملية غير شرعية " وتظهر هذه الرسالة عند ترك الكمبيوتر بدون تحريك الماوس أو النقر على لوحة المفاتيح حيث يقوم البرنامج بعمل تغييرات في حافظة الشاشة وتظهر هذه الرسائل عادة عندما تقوم بإزالة ادخالات البرنامج في ملف (system.ini) .

٢. **برنامج** (Back Orific) : ثاني أشهر البرامج وأقدمها يعطي المستخدم قدرة كاملة على جهاز الضحية تم الإعلان عنه من قبل جهة تدعى بجمعية البقرة الميتة (Cult of Dead Cow) والإصدارة التي صدرت في عام ١٩٩٩ باسم بـ (BO2K)

٣-. **برنامج** (Hack 'a' Tack)**:** شائع في أوروبا ونادر الاستخدام في الشرق الأوسط.

٤. **برنامج** : (Net bus) **:** أشهر البرامج وأكثرها انتشارا وقد يكون سبب انتشاره أنه من أوائل البرامج التي ظهرت لهذا الغرض ، ولسهولة استخدامه لقي رواجا كبيرا وعلى الرغم من أنه أنه لم يكمل العامين من عمره إلا أنه يوجد العديد من الإصدارات التي تتحسن وتزداد خطورة في كل إصدارة عن سابقتها (Nanoart,2000).

أنواع برامج الحماية :

للحماية من الاختراق والتجسس هناك طرق تستخدمها برامج الحماية للقيام بمهماتها ومن الممكن تصنيف هذه الطرق بشكل عام إلى أربعة طرق :

وجود قاعدة بيانات مسجل فيها عدد من أحصنة طروادة المعرفة مسبقاً ، ويتم عمل مسح لكافة الملفات الموجودة في الجهاز المستخدم ومطابقتها مع الموجود في هذه القاعدة للتعرف على الملفات المتطابقة،وهذه الطريقة تحتاج إلى تحديث دوري مستمر نظراً لصدور أنواع جديدة من البرامج وظهور إصدارات أحدث للبرامج القديمة

البحث عن وجود تسلسل محدد من الرموز التي تميز كل ملف تجسسي (Signature) والتي تميز أحصنة طروادة عن غيرها من البرامج العادية وهذه الطريقة أيضاً تحتاج إلى تحديث وذلك لتجدد هذه البرامج وسلوكياتها وقد يحدث أن

تعطى البرامج التي تستخدم هذه الطريقة تنبيهات خاطئة أحياناً ولكنها نادرة وذلك لاشتباهها ببعض البرامج كما حصل مع مجلة (PCMagazine) العربية في إحدى إصداراتها السابقة ، حين أظهرت بعض برامج كشف الفيروسات عن وجود فيروس في القرص المدمج الملحق بالمجلة ثم ظهر أن ذلك خطأ من البرنامج
الكشف عن التغيرات التي تطرأ على ملف التسجيل (Registry) وتوضيح ذلك للمستخدم لمعرفة إن كان التغير حصل من برنامج معروف أو من حصان طروادة
مراقبة منافذ الاتصال (Ports) الخاصة بالجهاز لاكتشاف أي محاولة غير مسموح بها للاتصال بالجهاز الهدف وقطع الاتصال و إعطاء تنبيه لذلك .
وتختلف البرامج من حيث استخدامها للأساليب المذكورة حيث أن كل برنامج يستخدم أسلوب أو أكثر . كما أن البرامج من حيث الشمول تنقسم إلى نوعين :
(أ) - نوع خاص بالحماية من اختراق معينة خصوصاً البرامج المشهورة في هذا المجال مثل (NetBus) أو برنامج (Back Orifice) فقط. وعيب مثل هذا النوع انه لا تستطيع اكتشاف الاختراق القادم من برامج أخرى إلا أن ميزة هذه الأنواع من البرامج هي قوتها في التصدي للهجمات القادمة من البرنامج المخصص له الحماية
.(ب) - نوع عام حيث يقوم بالتصدي لكافة الأنواع دون تخصيص
(Nanoart,2000)

المراجع :

أولا المراجع العربية :

أبو الحجاج، أسامة.(١٩٩٨ م) دليلك الشخصي إلى عالم الإنترنت . القاهرة : نهضة مصر .

السيد، سمير.(١٩٩٧م). محاضرات في شبكة المعلومات العالمية . القاهرة : مكتبة عين شمس.

عيد، محمد فتحي.(١٤١٨هـ). الإجرام المعاصر. الرياض : أكاديمية نايف العربية للعلوم الأمنية .

مجلة أفاق الإنترنت. (١٩٩٧)، إنترنت ٢، المؤلف، السنة ١ (٣) ،٣٨-٤١.

موقع جريدة الجزيرة (٢٠٠٠) http://www.al-jazirah.com

ثانيا : المراجع الأجنبية :

NUA Internet Surveys. (1998,June). How Many Online? [Online].
Available:
http://www.nua.ie/surveys/howmayonline/index.html
[15.6.1998].

NUA Internet Surveys. (1998,June). How Many Online? [Online]. Available: http://www.nua.ie/surveys/howmayonline/index.html [26.10.2000].

NUA Internet Surveys. (1998,June). How Many Online? [Online]. Available: http://www.nua.ie/surveys/howmayonline/index.html [6.11.2000].

Nanoart. (2000) [Online]. http://www.nanoart.f2s.com/hack/Available: [15/11/2000]

الحرب المعلوماتية

يتعرض الإنسان في هذا العصر إلى كم هائل من المعلومات يصعب عليه في كثير من الأحيان التعامل معه. حاصرت المعلومات الإنسان ومازالت تحاصره بواسطة وسائل عدة ، ابتداء بالآلة الطابعة ، ومروراً بالتلفاز والمذياع ، وانتهاء بالحاسب الآلي والإنترنت. لقد إزداد الإعتماد على نظم المعلومات والإتصالات في آخر عقدين من القرن الماضي إزدياد مضطرد حتى أصبحت تلك النظم عاملاً رئيساً في إدارة جميع القطاعات المختلفة كالقطاع المصرفي والتجاري والأمني فضلاً عن المشاريع الحيوية والحساسة كتوليد ونقل الطاقة ووسائل المواصلات جوية كانت أو بحرية. إن مجرد تخيل تعطل تلك النظم أمراً يثير الرعب لدى الكثير ولو ليوم واحد ولعل مشكلة عام ألفين أكبر دليل على ذلك. إن تعطيل مثل هذه الخدمات يعني – في أفضل صوره وأدناها تشاؤم – تجميد للحياة المدنية. لذا فقد فتحت وسائل التقنية الحديثة مجالات أوسع وأخطر للحرب المعلوماتية.

إن "حرب المعلومات" ليست حديثة ، فقد مارستها البشرية منذ نشأتها باستخدام نظم المعلومات المتوفرة لديها. فقد قام أحد القياصرة بتشفير بعض المعلومات الحساسة والمطلوب إرسالها إلى قادته خوفاً من كشف سرية هذه المعلومات من قبل أعدائه. وبعد اختراع المذياع ، بدأ استخدامها كوسيلة في الحرب حيث يقوم أحد الأطراف بضخ معلومات موجهه إلى الطرف الآخر تهدف إلى إحداث تأثيرات نفسيه لديه كنشر معلومات سريه أو مكذوبة عنه وذلك لزعزعة الثقة فيه . ومع ظهور الحاسب الآلي واستخدام شبكات لربط أجهزة الحاسب وانتشار شبكة الإنترنت بشكل خاص واتساع استخدامها ، بدأت "حرب المعلومات" تأخذ بعداً جديد. فالتضخم الكبير في صناعة المعلومات جعل الاعتماد على نظمه الحديثة (الحاسب الآلي و الشبكات) أكبر وأكثر في إدارة أمور الحياة المختلفة ولذا فإن استخدام المعلومات كسلاح أصبح أكثر عنفاً و أشد تأثيراً. ومع ذلك فإن نظم المعلومات التقليدية كالطباعة و المذياع مازالت ضمن قائمة وسائل الحرب المعلوماتية ، ففي حرب الخليج الأخيرة تم استخدام وسائل تقليدية حيث أسقطت القوات المشتركة ما يقرب من ٣٠ مليون نشرة داخل الأراضي العراقية بالإضافة إلى بث إذاعي موجه ، كان الهدف من ذلك كله إقناع أفراد الجيش العراقي بالاستسلام و أنهم لن ينالهم أذى من ذلك. تشير تقارير منظمة الصليب الأحمر الأمريكي إلى أن حوالي ٩٠ ألف جندي عراقي قاموا بتسليم أنفسهم يحمل معظمهم بعض النشرات التي تم إسقاطها أو قصاصات منها مخفية في ملابسهم. وفي الحرب نفسها تم أيضاً استخدام وسائل حديثة في المعركة المعلوماتية حيثُ استخدمت الأقمار الصناعية و طائرات التجسس المختلفة. وقد تزامن في نفس الفترة قيام مجموعة من "الهاكرز" هولنديي الجنسية من اختراق عدد كبير من أجهزة الحاسب الآلي تابعة للدفاع الأمريكي مرتبطة بشبكة الإنترنت. كانت هذه الأجهزة تحوي معلومات هامة عن

الجيش الأمريكي . استطاع هؤلاء معرفة معلومات حساسة مثل مواقع الجيش و تفاصيل الأسلحة المختلفة الموجودة في كل موقع من هذه المواقع كان يمكن أن يستغلها النظام العراقي لصالحه. (١)
وعلاوة على استخدامها كعامل مساعد في الحروب التقليدية ، يمكن أن تكون "المعلوماتية" هي الساحة التي يتحارب فيها الأعداء ، و لعل أشهر مثال على ذلك "الحرب الهاكرية" بين مجموعات عربية و إسرائيلية التي إستمرت عدة أشهر بين عامي ٢٠٠٠م و٢٠٠١م حيث قام كل طرف بتعطيل أو تخريب مواقع للطرف الآخر، فقد تم في الشهر الأول لهذه المعركة (أكتوبر ٢٠٠٠) - وهي أعنف فترة لهذه الحرب غير المعلنة حتى الآن - تخريب ٤٠ موقع إسرائيلي مقابل ١٥ موقع عربي. (٢)

هناك ثلاثة عناصر أساسية للحرب المعلوماتية هي "المهاجم" و "المدافع" و "المعلومات وأنظمتها ". وبناءً على ذلك هناك نوعين من الحروب المعلوماتية هي "الحرب المعلوماتية الهجومية" و"الحرب المعلوماتية الدفاعية".

الحرب المعلوماتية الهجومية

تستهدف الحرب المعلوماتية الهجومية معلومات معينة أو نظم معلومات عند الطرف المراد مهاجمته "المدافع" وذلك لزيادة قيمة تلك المعلومات أو نظمها بالنسبة للمهاجم أو تقليل قيمتها بالنسبة للمدافع أو بهما جميعاً. أما قيمة المعلومات ونظمها فهي مقياس لمقدار تحكم واستحواذ المهاجم (او المدافع) بالمعلومات ونظمها. إن ما يسعى للحصول عليه المهاجم في حربه المعلوماتية من أهداف قد تكون مالية كأن يقوم بسرقة وبيع سجلات لحسابات مصرفية ، وقد تكون الحرب المعلوماتية الهجومية لأهداف سياسية أو عسكرية ، أو لمجرد الإثارة و إظهار القدرات وهذا ما يحدث عادةً في مجتمعات "الهاكرز" (١).

إن عمليات الحرب المعلوماتية المتعلقة بزيادة قيمة المعلومات ونظمها بالنسبة للمهاجم لها عدة أشكال. من أهم هذه العمليات هي التجسس على المدافع و ذلك لسرقة معلومات سرية عنه بغض النظر عن الأهداف فقد تكون هذه الأهداف تجارية بين شركات أو إستراتيجية وعسكرية بين دول. ومن تلك العمليات أيضاً التعدي على الملكية الفكرية وقرصنة المعلومات كسرقة البرامج الحاسوبية وتوزيع مواد مكتوبة أو مصورة بدون إذن المالك الشرعي لهذه المواد وهذا النوع من العمليات إنتشر بشكل كبير مع وجود الإنترنت نظراً لسهولة النشر و التوزيع على هذه الشبكة. إنتحال شخصيات آخرين ُ تصنف كذلك ضمن عمليات الحرب المعلوماتية الهجومية حيث يقوم المهاجم بإستغلال هوية الغير إما لتشويه سمعته أو لسرقته. أما بالنسبة لعمليات الحرب المعلوماتية المتعلقة بتقليل قيمة المعلومات أو أنظمتها بالنسبة للمدافع فلها صورتان وهما إما تخريب أو تعطيل نظم المعلومات

الخاصة بالمدافع (أجهزة الحاسب الآلي أو أنظمة الإتصالات) ، أو سرقة أو تشويه معلوماته (٣).

إن قيمة المعلومات ونظمها بالنسبة للمهاجم في الحرب المعلوماتية الهجومية تعتمد بشكل كبير على قدرات و إمكانيات المهاجم في الوصول إلى نظم المعلومات ، كما تعتمد قيمتها كذلك على أهمية تلك المعلومات و نظمها بالنسبة له .

إن المهاجم في الحرب المعلوماتية الهجومية قد يكون شخص يعمل بمفرده أو يكون ضمن منظومة بغض النظر عن هذه المنظومة فقد تكون تجارية أو سياسية أو عسكرية. تتعدد تصنيفات المهاجمين ، لكن من أهمها و أكثرها خطورة هو ذلك الشخص الذي يعمل داخل الجهة المراد مهاجمتها ، و تكمن خطورة هذا الشخص في قدرته على معرفة معلومات حساسة و خطيرة كونه يعمل داخل تلك الجهة. لذلك فإن حرب التجسس بين الدول التي تعتمد على عناصر يعملون داخل الجهة الأخرى تعد من أخطر أنواع التجسس حيث تفرض الدول أشد الأحكام صرامة على من يمارس ذلك و التي تصل إلى الإعدام في كثير من الدول. لا يقتصر هذا الصنف من المهاجمين على الممارسات بين الدول بل قد يكون ذلك الشخص المهاجم يعمل داخل شركة حيث يقوم بسرقة معلومات تجارية سرية من تلك الشركة و ذلك لغرض إفشاءها أو بيعها لشركات منافسة أو التلاعب بالسجلات المالية وذلك لمطامع و أهداف شخصية. إن من أشهر الجرائم المعلوماتية تلك التي أطاحت ببنك بارينجز (Barings Bank) في بريطانيا حيث قام أحد مسئولي البنك بعمل استثمارات كبيرة للبنك في سوق الأسهم اليابانية و بعد سقوط حاد لتلك الاستثمارات حاول إخفاء هذه الخسائر و التي تقدر بحوالي بليون جنيه إسترليني في حسابات خاطئة على أنظمة الحاسب الآلي للبنك (٤).

أما الصنف الثاني فهم المجرمون المحترفون الذين يسعون لسرقة معلومات حساسة من جهات تجارية أو حكومية و ذلك لغرض بيعها على جهات أخرى تهمها تلك المعلومات.

يمثل ما يسمى بـ "الهاكرز" الصنف الثالث ، والذين لا يهدفون في حربهم المعلوماتية إلا للمغامرة و إظهار القدرات أمام الأقران ، فلا توجد عادةً عند هؤلاء أطماع مالية.

الصنف الرابع من أصناف المهاجمين في الحرب المعلوماتية هو تلك الجهات المتنافسة التي يسعى بعضها للوصول إلى معلومات حساسة لدى الطرف الآخر ، و ذلك سعياً للوصول إلى موقف أفضل من الجهة المنافسة. أما الصنف الخامس فهو حكومات بعض الدول ، تسعى من خلال حروب جاسوسية إلى الحصول على معلومات إستراتيجية و عسكرية عن الدول الأخرى ، و لعل من أشهر تلك

الحروب الجاسوسية تاريخياً تلك التي كانت بين الولايات المتحدة و الاتحاد السوفييتي خلال الحرب الباردة. هذه جملة من أصناف المهاجمين و لا تعني أنها شاملة بل تبقى هناك أصناف أخرى لا يسعنا هنا التطرق إليها (١).

الحرب المعلوماتية الدفاعية

تشمل الحرب المعلوماتية الدفاعية جميع الوسائل الوقائية المتوفرة "للحد" من أعمال التخريب التي قد تتعرض لها نظم المعلومات. بالطبع فإن هذه الوسائل الوقائية هي فقط "للحد" و "التقليل" من الأخطار فليس من المتوقع عملياً أن توجد وسائل "تمنع جميع" الأخطار. إن إتخاذ قرار بشأن إستخدام وسيلة من تلك الوسائل يعتمد على تكلفة تلك الوسيلة و علاقتها بحجم الخسارة التي يمكن أن تنتج في حالة عدم إستخدامها ، فمن غير المقبول و المعقول أن تكون قيمة هذه الوسيلة الوقائية المستخدمة أعلى من قيمة الخسارة التي تقوم تلك الوسيلة بالحماية منها.

إن إزدهار صناعة تقنية المعلومات و إنتشارها في السنوات القليلة الماضية كان سبب في إزدهار وإنتشار صناعة أدوات التخريب المعلوماتية . فعن طريق مواقع كثيرة على شبكة الإنترنت ، يمكن للشخص قليل الخبرة الحصول على عدة أدوات تخريبية يمكن إستخدامها لشن هجوم على أجهزة حاسوبية مرتبطة بالشبكة و إحداث أشكال مختلفة من التخريب. و هنا يحسن بنا التنويه بأن التخريب الذي يمكن أن تتعرض له نظم المعلومات تختلف صوره و تتعدد أشكاله و الأضرار التي قد تنتج عنه ، فهناك أدوات تخريبية تقوم بحذف معلومات و أخرى تقوم بسرقة معلومات أو تغييرها ، كما تقوم أدوات تخريبية أخرى بإحداث بعض الأضرار على أجهزة نظم المعلومات. و هناك أدوات كثيرة أخرى لا تقوم بعملية تخريب و إنما يمكن إستخدامها بطريقة غير مباشرة لإحداث ضرر. لذا فإن الوسائل الدفاعية تختلف بإختلاف تلك الإدوات التخريبية و طبيعة الأضرار التي قد تحدثها.

يمكن تقسيم وسائل الدفاع إلى أربعة مجالات ، أول تلك المجالات هو المنع و الوقاية حيث تسعى الوسائل الدفاعية في هذا المجال إلى منع حدوث المخاطر من البداية و ذلك بحماية نظم المعلومات من وصول المهاجمين المحتملين إليها . تشمل هذه الوسائل إجراءات إخفاء المعلومات (Information Hiding) و تشفيرها كما تشمل كذلك إجراءات التحكم في الدخول على نظم المعلومات (Access Controls).

أما المجال الثاني من مجالات الحرب المعلوماتية الدفاعية فهو التحذير و التنبيه و الذي يسعى لتوقع حدوث هجوم قبل حصوله أو في مراحله الأولى. و يشابه هذا المجال المجال الثالث و هو كشف الإختراقات والذي يعد من أشهر و أكثر وسائل الدفاع إستخداماً. حيث يشمل ذلك وسائل تقليدية كإستخدام كاميرات مراقبة للكشف

عن دخول غير المصرح لهم للمبنى الذي يضم نظم المعلومات المطلوب حمايتها ، كما يشمل هذا المجال وسائل تقنية حاسوبية تتمثل في برامج و أجهزة تقوم بمراقبة العمليات التي تعمل نظم المعلومات على تنفيذها ، و ذلك للكشف عن عمليات غير مصرح بها تكون هذه العمليات مؤشراً لإختراقات تمت على تلك النظم. أما المجال الرابع من وسائل الدفاع في الحرب المعلوماتية الدفاعية هو ما يسمى بـ "التعامل مع الإختراقات" حيث تناقش هذه الوسائل الآليات الازمة للتعامل مع الإختراقات بعد حدوثها مثل كيفية إعادة النظم إلى وضعها الطبيعي ، و تجميع الأدلة و البراهين التي يمكن عن طريقها معرفة هوية المخترق من ثم مقاضاته ، و توثيق الحادث و ذلك لتجنب تكرار حدوثه في المستقبل.

مراجع :

(١) D. Denning, “*Information Warfare and Security*”, Addison Wesley, 1999.

(٢) http://www.wired.com/news/politics/0,1283,40030,00.html

(٣) Stephen Northcutt,``*E-Warfare*", SANS Institute, 2001.

(٤) D. Parker,``*Fighting Computer Crime*," Wiley, 1998.

(٥) D. Alberts,`` *Defensive Information Warfare*," NDU Press, 1998.

المخاطر الأمنية للانترنت :

مقدمة حول جرائم الحاسب الآلي والإنترنت:
أُشْتُقتْ كلمة الجريمة في اللغة من الجُرم وهو التعدي أو الذنب، وجمع الكلمة إجرام وجروم وهو الجريمة. وقد جَرَمَ يَجْرِمُ واجْتَرَمَ وأجْرَم فهو مجرم وجريم (ابن منظور، بدون : ٦٠٤ – ٦٠٥)، وعَرَّفت الرشيعة الاسلامية الجريمة بانها " محظورات شرعية زجر الله عنها بحد أو تعزير" (الماوردي، ١٤١٧هـ : ١٩)
تعرّف جرائم الحاسب الآلي والإنترنت بانها: " ذلك النوع من الجرائم التي تتطلب المام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها" (مندورة،١٤١٠ : ٢١)، كما يمكن تعريفها بانها " الجريمة التي يتم ارتكابها اذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني " (محمد ، ١٩٩٥ : ٧٣)
وهناك من عرفها بانها " أي عمل غير قانوني يستخدم فيه الحاسب كاداة، أو موضوع للجريمة " (البداينة، ١٤٢٠هـ : ١٠٢).
أما التعريف الإجرائي لدراسة الباحث فتُعَرَّفْ جرائم الإنترنت بأنها : جميع الأفعال المخالفة للتشريع الإسلامي ولأنظمة المملكة العربية السعودية والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الإنترنت، ويشمل ذلك الجرائم الجنسية،جرائم الاختراقات ،الجرائم التجارة الإلكترونية ، جرائم إنشاء أو ارتياد المواقع المعادية، جرائم القرصنة ،الجرائم المنظمة. وفي كل الاحوال فجريمة الحاسب الآلي " لاتعترف بالحدود بين الدول ولا حتى بين القارات فهي جريمة تقع في اغلب الاحيان عبر حدود دولية كثيرة " (عيد، ١٤١٩هـ: ٢٥٢)، وتعد جريمة الإنترنت من الجرائم الحديثة التى يُستخدم فيها شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها (Vacca , 1996)
واطلق مصطلح جرائم الإنترنت أو (Internet Crimes) في مؤتمر جرائم الإنترنت المنعقد في استراليا للفترة من ١٦ – ١٩٩٨/٢/١٧م (بحر، ١٩٩٩م : ٢)
وبالرغم من حداثة جرائم الحاسب الآلي والإنترنت نسبيا الا انها لقت اهتماما من قبل بعض الباحثين حيث اجرت العديد من الدراسات المختلفة لمحاولة فهم هذه الظاهرة ومن ثم التحكم فيها، ومنها دراسة اجرتها منظمة (Busieness Software Alliance) في الشرق الاوسط حيث أظهرت أن هناك تباين بين دول منطقة الشرق الاوسط في حجم خسائر جرائم الحاسب الآلي حيث تراوحت ما بين (٣٠) مليون دولار أمريكي في المملكة العربية السعودية والامارات العربية المتحدة و (١,٤) مليون دولار أمريكي في لبنان (موثق في البداينة، ١٤٢٠هـ : ٩٨)
كما أظهرت دراسة قامت بها الامم المتحدة حول جرائم الحاسب الآلي والإنترنت بان (٢٤ – ٤٢ ٪) من منظمات القطاع الخاص والعام على حد

سواء كانت ضحية لجرائم متعلقة بالحاسب الآلي والإنترنت (البداينة، ١٩٩٩م : ٥).

وقدرت الولايات المتحدة الامريكية خسائرها من جرائم الحاسب الآلي مابين ثلاثة وخمسة بلاين دولار سنويا، كما قدرت المباحث الفيدرالية (FBI) في نهاية الثمانينات الميلادية أن متوسط تكلفة جريمة الحاسب الآلي الواحد حوالي ستمائة الف دولار سنويا مقارنة بمبلغ ثلاثة الاف دولار سنويا متوسط الجريمة الواحدة من جرائم السرقة بالاكراه. وبينت دراسة اجراها احد مكاتب المحاسبة الامريكية أن مائتين واربعين (٢٤٠) شركة امريكية تضررت من جرائم الغش باستخدام الكمبيوتر Computer Fraud)).

كما بينت دراسة اخرى اجريت في بريطانيا انه وحتى اواخر الثمانينات ارتكب ما يقرب من (٢٦٢) مائتين واثنين وستون جريمة حاسوبية وقد كلفت هذه الجرائم حوالي (٩٢) اثنان وتسعون مليون جنيه استرليني سنويا (محمد ، ١٩٩٥م : ٢١).

وأظهر مسح اجري من قبل (the computer security institute) في عام (١٩٩٩م) ان خسائر (١٦٣) شركة من الجرائم المتعلقة بالحاسب الآلي بلغت أكثر من مائة وثلاثة وعشرون مليون دولار، في حين اظهر المسح الذي أجري في عام (٢٠٠٠م) ارتفاع عدد الشركات المتضررة حيث وصلت إلى (٢٧٣) شركة بلغ مجموع خسائرها اكثر من مائتين وستة وخمسون مليون دولار(Rapalus,2000)، كما بينت احصائيات الجمعية الامريكية للامن الصناعي ان الخسائر التى قد تسببها جرائم الحاسب الالي للصناعات الامريكية قد تصل الى (٦٣) بليون دولار امريكي وان (٢٥٪) من الشركات الامريكية تتضرر من جرائم الحاسب الالي في حين اصيب (٦٣٪) من الشركات الامريكية والكندية بفيروسات حاسوبية، وان الفقد السنوي بسبب سوء إستخدام الحاسب الالي وصل (٥٥٥) مليون دولار (Reuvid,1998, p. 14)

ومن الصعوبة بمكان تحديد أي جرائم الحاسب الآلي المرتكبة هي الاكبر من حيث الخسائر حيث لا يعلن الكثير عن مثل هذه الجرائم، ولكن من اكبر الجرائم المعلنة هي جريمة لوس انجلوس حيث تعرضت اكبر شركات التامين على الاستثمارات المالية (EFI) للافلاس وبلغت خسائرها مليارين دولار امريكي. وهناك ايضا حادثة انهيار بنك بارينجر البريطاني في لندن اثر مضاربات فاشلة في بورصة الاوراق المالية في طوكيو حيث حاول البنك اخفاء الخسائر الضخمة باستخدام حسابات وهمية ادخلها في الحسابات الخاصة بالبنك بمساعدة مختصيين في الحاسب الآلي وقد بلغت اجمالي الخسائر حوالي مليار ونصف دولار امريكي (داود، ١٤٢٠هـ: ٣١)

وتعتبر هذه الخسائر بسيطة نسبيا مع الخسائر التى تسببتها جرائم نشر الفيروسات والتي تضر بالافراد والشركات وخاصة الشركات الكبيرة حيث ينتج عنها توقف اعمال بعض تلك الشركات نتيجة إتلاف قواعد بياناتها، وتتراوح اضرار الفيروسات ما بين عديمة الضرر إلى البسيط الهين وقد تصل إلى تدمير محتويات

كامل الجهاز، وأن كان الاكثر شيوعا من هذه الفيروسات هو ما يسبب ضررا محصورا في اتلاف البيانات التي يحتويها الجهاز وبالرغم من ذلك فإن الضرر قد يصل في بعض المنشئات التجارية والصناعية إلى تكبد خسائر مادية قد تصل إلى مبالغ كبيرة، وعلى سبيل المثال وصلت خسائر فيروس كود رد إلى ملياري دولار امريكي، في حين وصلت الاضرار المادية لفيروس الحب الشهير (٨,٧) مليون دولار واستمر انتشار الفيروس لخمسة اشهر وظهر منه (٥٥) نوعا.
(Ajeebb.com,8/8/2001)

وجرائم الإنترنت كثيرة ومتنوعة ويصعب حصرها ولكنها بصفة عامة تشمل الجرائم الجنسية كإنشاء المواقع الجنسية الاباحية والتى تقوم بإيجار الأفلام الجنسية وجرائم الدعارة أو الدعاية للشواذ أو تجارة الأطفال جنسيا، كما تشمل جرائم ترويج المخدرات أو زراعتها، وتعليم الإجرام والإرهاب كتعليم صنع المتفجرات، إضافة إلى جرائم الفيروسات واقتحام المواقع. وكثيرا ما تكون الجرائم التى ترتكب بواسطة الإنترنت وثيقة الصلة بمواقع ارضية على الطبيعة كما حدث منذ حوالي سنتين عندما قام البوليس البريطاني بالتعاون مع أمريكا ودول أوروبية بمهاجمة مواقع أرضية لمؤسسات تعمل في دعارة الإنترنت ، وأن كانت متابعة جرائم الحاسب الآلي والإنترنت والكشف عنها من الصعوبة بمكان حيث أن " هذه الجرائم لا تترك اثرا، فليست هناك اموال أو مجوهرات مفقودة وأن ما هي ارقام تتغير في السجلات. ومعظم جرائم الحاسب الآلي تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أن الجرائم التى لم تكتشف هي اكثر بكثير من تلك التى كشف الستر عنها" (مندورة ، ١٤١٠هـ : ٢٢).

وتعود أسباب صعوبة إثبات جرائم الحاسب الآلي إلى خمسة امور هي :

أولا: انها كجريمة لا تترك اثر لها بعد ارتكابها.

ثانيا: صعوبة الاحتفاظ الفنى باثارها ان وجدت.

ثالثا: انها تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.

رابعا: انها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.

خامسا: انها تعتمد على قمة الذكاء في ارتكابها(موثق في شتا،٢٠٠١م : ١٠٣).

إلا ان أهم خطوة في مكافحة جرائم الإنترنت هي تحديد هذه الجرائم بداية ومن ثم تحديد الجهة التى يجب ان تتعامل مع هذه الجرائم والعمل على تاهيل منسوبيها بما يتناسب وطبيعة هذه الجرائم المستجدة وياتي بعد ذلك وضع تعليمات مكافحتها والتعامل معها والعقوبات المقترحة ومن ثم يركز على التعاون الدولي لمكافحة هذه الجرائم .

والإنترنت ليس قاصرا على السلبيات الأمنية فقط حيث يمكن أن يكون مفيدا جدا في النواحي الأمنية كأن يستخدم الإنترنت في ايصال التعاميم والتعليمات بسرعة وكذلك في امكانية الاستفادة من قواعد البيانات المختلفة والموجودة لدى القطاعات الاخرى وتبادل المعلومات مع الجهات المعنية، ويفيد ايضا في مخاطبة الإنتربول ومحاصرة المجرمين بسرعة.

ففي دراسة أمنية لشرطة دبي حول الاستخدامات الأمنية للانترنت حددت عشر خدمات امنية يمكن تقديمها للجمهور عن طريق شبكة الإنترنت وابرزت (١٥) سلبية يمكن أن تنجم عن الاستخدام السيئ لهذه التقنية أبرزها الاباحية والمعاكسات والاحتيال والتجسس والتهديد والابتزاز. وتطرقت الدراسة إلى أهمية الاستعانة بشبكة الإنترنت نظرا لدورها في نشر المعلومات بين الافراد في كافة انحاء العالم (البيان،٢٠٠٠م).

كما حددت دراسة الشهري الايجابات الأمنية لشبكة الإنترنت في تلقي البلاغات، توفير السرية للمتعاونين مع الأجهزة الأمنية، طلب مساعدة الجمهور في بعض القضايا، نشر صور المطلوبين للجمهور، نشر المعلومات التى تهم الجمهور، تكوين جماعات اصدقاء الشرطة، توعية الجمهور امنيا، استقبال طلبات التوظيف، نشر اللوائح والانظمة الجديدة، توفير الخدمة الأمنية خارج اوقات العمل الرسمي، سهولة الوصول إلى العاملين في الجهاز الامني ، اجراء استفتاءت محايدة لقياس الرأي العام، وسيط فاعل في عملية تدريب وتثقيف منسوبي القطاع واخيرا وسيط مهم للاطلاع على خبرات الدول المتقدمة ولاتصال مع الخبراء والمختصين في مختلف دول العالم (الشهرى، فايز، ١٤٢٢هـ).

وليس الامر قاصرا على ذلك بل بادرت الدول الاوروبية الى الاستخدام الفعلي لشبكة الإنترنت في البحث عن المجرمين والقبض عليهم " فقد تمكنت العديد من الدول وفي مقدمتها المانيا وبريطانيا وتأتي في المرتبة الثالثة فرنسا من إستخدام شبكة الإنترنت في السعي نحو ضبط المجرمين – بل التعرف على كل الحالات المشابهة في كل انحاء اوروبا والاتصال فورا بالانتربول عبر شبكة الإنترنت" (الشهاوي، ١٩٩٩م : ٢٥)

فئات الجناة في جرائم الحاسب الآلي :

يمكن بصفة عامة حصر انواع الجناة في جرائم الحاسب الآلي في اربعة فئات :

الفئة الاولي : العاملون على اجهزة الحاسب الآلي في منازلهم نظرا لسهولة اتصالهم باجهزة الحاسب الآلي دون تقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز.

الفئة الثانية : الموظفون الساخطون على منظماتهم التى يعملون بها فبعودون إلى مقار عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو اتلافه أو حتى سرقته، وقد يجد الموظف نفسه احيانا مرتكبا لجريمة حاسوبية بمحض الصدفة ودون تخطيط مسبق منه .

الفئة الثالثة : فئة العابثين أو ما يعرفون بمسمى المتسللين (Hackers) وينقسم المتسللين إلى قسمين فمنهم الهواة أو العابثون بقصد التسلية ، وهناك المحترفين اللذين يتسللون إلى اجهزة مختارة بعناية ويعبثون أو يتلفون أو يسرقون محتويات ذلك الجهاز. وتقع اغلب جرائم الإنترنت حاليا تحت هذه الفئة سواء الهواة منهم أو المحترفون.

الفئة الرابعة: الفئة العاملون في الجريمة المنظمة كالعصابات العاملة في مجال سرقة السيارات حيث يستخدمون الشبكة في معرفة الولايات الاعلى سعرا من حيث

قطع الغيار ومن ثم يقومون ببيع قطع غيار السيارات المسروقة في تلك الولايات(محمد،١٩٩٥م :٧٤- ٧٥)

خصائص وأنواع جرائم الحاسب الآلي والإنترنت :

بطيعة الحال فان من الصعوبة بمكان الفصل بين جرائم الحاسب الآلي وجرائم الإنترنت فلابد للاول لارتكاب الثاني ولذلك فسنبين هنا خصائص وأنواع جرائم الحاسب الآلي بصفة عامة والتى تشمل في المقابل بعض جرائم الإنترنت، ومن ثم سنتطرق إلى بعض المخاطر الأمنية للانترنت بصفة خاصة، ويمكن تصنيف جرائم الحاسب الآلي في مجموعات:

المجموعة الاولي :

تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي واستغلالها بطريقة غير مشروعة كمن يدخل إلى احدى الشبكات ويحصل على ارقام بطاقات ائتمان بنكية مخزنة في الجهاز ويستدعى الجاني رقما معينا لاحدى البطاقات ويحصل بواسطته على مبالغ من حساب مالك البطاقة ، وما يميز هذا النوع من الجرائم انه من الصعوبة بمكان اكتشافه ما لم يكن هناك تشابهه في بعض اسماء اصحاب هذه البطاقات .

المجموعة الثانية :

تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها أو تدميرها كليا أو جزئيا ويمثل هذا النوع الفيروسات المرسلة عبر البريد الالكتروني أو بواسطة برنامج مسجل في احد الوسائط المتنوعة والخاصة بتسجيل برامج الحاسب الآلي ويمكن اكتشاف مثل هذه الفيروسات في معظم الحالات بواسطة برامج حماية مخصصة للبحث عن هذه الفيروسات ولكن يشترط الامر تحديث قاعدة بيانات برامج الحماية لضمان اقصى درجة من الحماية . ومع أن وجود هذه البرامج في جهاز الحاسب الآلي لا يعنى اطلاقا الحماية التامة من أي هجوم فيروسي وأن ما هو احد سبل الوقاية والتى قد يتسلل الفيروس إلى الجهاز بالرغم من وجودها ويلحق اذى بالجهاز ومكوناته خاصة اذا كان الفيروس حديث وغير معروف من السابق .

المجموعة الثالثة :

تشمل استخدام الحاسب الآلي لارتكاب جريمة ما، وقد وقعت جريمة من هذا النوع في احدى الشركات الامريكية التى تعمل سحبا على جوائز اليانصيب حيث قام احد الموظفين بالشركة بتوجيه الحاسب الآلي لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة إلى شخص بطريقة غير مشروعة [وأن كان اليانصيب غير مشروع اصلا]

المجموعة الرابعة :

تشمل اساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الاشخاص المرخص لهم باستخدامه ومن هذا استخدام الموظف لجهازه بعد انتهاء عمله في امور لا تخص العمل .(محمد ، ١٩٩٥م) و (مندورة ، ١٤١٠ هـ)

المخاطر الأمنية للانترنت

لايمكن حصر المخاطر الأمنية بصفة دقيقة لاسباب متعددة منها ان انتشار الإنترنت يعتبر حديثا نسبيا كما انه ولطبيعة العمل الامني فان المخاطر مستجدة دوما ولا تقف عند زمن معين أو على نمط محدد، فالخير والشر في صراع دائم لايتوقف منذ قديم الزمن، الا انه

" يمكن النظر للانترنت كمهدد للامن الاجتماعي وخاصة في المجتمعات المغلقة والشرقية، حيث ان تعّرض مثل هذه المجتمعات لقيم وسلوكيات المجتمعات الاخرى قد تسبب تلوثا ثقافيا يؤدي إلى تفسخ اجتماعي وأن هيار في النظام الاجتماعي العام لهذه المجتمعات. إن الاستخدام غير الاخلاقي واللاقانوني للشبكة قد يصل إلى مئات المراهقين والهواة مما يؤثر سلبا على نمو شخصياتهم النمو السليم ويوقعهم في ازمات نمو، وازمات قيمية لا تتماشى مع النظام الاجتماعي السائد، وبخاصة عند التعامل مع المواضيع الجنسية وتقديم الصور والمواد الاباحية" (البداينة، ١٩٩٩م : ١٠١)

ولذلك سنتطرق هنا إلى أهم – وليس إلى جميع - المخاطر الأمنية للانترنت.

ومن أهم هذه المخاطر:

. التجسس الالكتروني:-

" في عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي " (البداينة، ١٩٨٨م) و العالم العربي والاسلامي كان ولا يزال مستهدف امنيا وثقافيا وفكريا وعقديا لاسباب لاتخفى على احد. وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية خاصة مع استخدام الإنترنت وأن تشاره عربيا وعالميا. ولا تكمن الخطورة في استخدام الإنترنت ولكن في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية ولايمكن حتما الاعتماد على وسائل الحماية التى تنتجها الشركات الاجنبية فهي ليست في مأمن ولا يمكن الاطمئنان لها تماما. ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الانظمة أو ما يعرفون اصطلاحا (hackers) فمخاطر هؤلاء محدودة وتقتصر غالبا على العبث أو اتلاف المحتويات والتى يمكن التغلب عليها باستعادة نسخة اخرى مخزنة في موقع امن، اما الخطر الحقيقي فيكمن في عمليات التجسس التى تقوم بها الأجهزة الاستخباراتية للحصول على اسرار ومعلومات الدولة ومن ثم افشائها لدول اخرى تكون عادة معادية، أو استغلالها بما يضر بالمصلحة الوطنية لتلك الدولة. وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف اخيرا عن مفتاح وكالة الامن القومي الامريكية (NSA) والتى قامت بزاعته في نظام التشغيل الشهير وندوز، وربما يكون هذا هو احد الاسباب الرئيسية التى دعت الحكومة الالمانية باعلانها في الاونة الاخيرة عن استبدالها لنظام التشغيل وندوز بانظمة اخرى.كما كشف اخيرا النقاب عن شبكة دولية ضخمة للتجسس الالتكروني تعمل تحت اشراف وكالة الامن القومية الامريكية بالتعاون مع اجهزة الاستخبارات والتجسس في كندا،بريطانيا، استراليا ونيوزيلندا ويطلق عليها اسم (ECHELON) لرصد المكالمات الهاتفية والرسائل بكافة انواعها سواء ماكان

منها برقيا، تلكسيا، فاكسيا أو الكترونيا. وخصص هذا النظام للتعامل مع الاهداف غير العسكرية وبطريقة تجعله يعترض كميات هائلة جدا من الاتصالات والرسائل الالكترونية عشوائيا باستخدام خاصية الكلمة المفتاح بواسطة الحاسبات المتعددة والتى تم انشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية ومنها محطة رصد الاقمار الصناعية الواقعة في منطقة واي هوباي بجوب نيوزيلندا، ومحطة جير الدتون الموجودة باستراليا، والمحطة الموجودة في منطقة موروينستو في مقاطعة كورنوول ببريطانيا، والمحطة الواقعة في الولايات المتحدة الامريكية بمنطقة شوجرجروف وتبعد(٢٥٠) كيلومترا جنوب واشنطن دي سي، وايضا المحطة الموجودة بولاية واشنطن على بعد(٢٠٠) كيلومتر جنوب غرب مدينة سياتل. ولا يقتصر الرصد على المحطات الموجهة إلى الاقمار الصناعية والشبكات الدولية الخاصة بالاتصالات الدولية، بل يشمل رصد الاتصالات التى تجرى عبر انظمة الاتصالات الارضية وكذا الشبكات الإلكترونية . أي انه يرصد جميع الاتصالات التى تتم بأي وسيلة. ويعتبر الافراد والمنظمات والحكومات اللذين لا يستخدمون انظمة الشفرة التامينية أو انظمة كودية لحماية شبكاتهم واجهزتهم، اهدافا سهلة لشبكة التجسس هذه، وأن كان هذا لا يعنى بالضرورة ان الاهداف الاخرى التى تستخدم انظمة الشفرة في مأمن تام من الغزوات الاستخباراتية لهذه الشبكة ومثيلاتها. ولا يقتصر التجسس على المعلومات العسكرية أو السياسية بل تعداه إلى المعلومات التجارية والاقتصادية بل وحتى الثقافية (عبدالمطلب، ٢٠٠١م : ٣٠-٤٥).

فمع توسع التجارة الإلكترونية عبر شبكة الإنترنت تحولت الكثير من مصادر المعلومات إلى اهداف للتجسس التجاري ففي تقرير صدر عن وزارة التجارة والصناعة البريطانية أشار إلى زيادة نسبة التجسس على الشركات من (٣٦٪) عام (١٩٩٤م) إلى (٤٥٪) عام (١٩٩٩م).كما اظهر استفتاء اجرى عام (١٩٩٦م) لمسؤلي الامن الصناعي في الشركات الامريكة حصول الكثير من الدول وبشكل غير مشرع على معلومات سرية لانشطة تجارية وصناعية في الولايات المتحدة الامريكية(داود،١٤٢٠هـ : ٦٢).

ومن الاساليب الحديثة للتجسس الالكتروني اسلوب إخفاء المعلومات داخل المعلومات وهو أسلوب شائع وأن كان ليس بالامر السهل، ويتلخص هذا الاسلوب في لجوء المجرم إلى اخفاء المعلومة الحساسة المستهدفة بداخل معلومات اخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها وبذلك لا يشك احد في ان هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبسا، كما قد يلجأ إلى وسائل غير تقليدية للحصول على المعلومات السرية(داود، ١٤٢٠هـ : ٦٧)

وبعد الاعتداءات الاخيرة على الولايات المتحدة الامريكية صدرت تعليمات جديدة لأقمار التجسس الاصطناعية الأمريكية بالتركيز على أفغانستان والبحث عن أسامة بن لادن والجماعات التابعة له، وقررت السلطات الأمريكية الاستعانة في عمليات التجسس على أفغانستان بقمرين اصطناعيين عسكريين مصممان خصيصا لالتقاط

الاتصالات التي تجرى عبر أجهزة اللاسلكي والهواتف المحمولة، بالإضافة لقمرين اصطناعيين آخرين يلتقطان صورا فائقة الدقة وفي نفس الوقت طلب الجيش الأمريكي من شركتين تجاريتين الاستعانة بقمرين تابعين لهما لرصد الاتصالات ومن ثم تحول بعد ذلك إلى الولايات المتحدة حيث تدخل في أجهزة كمبيوتر متطورة لتحليلها. وتشارك في تلك العمليات شبكة إشيلون المستخدمة في التجسس على المكالمات الهاتفية ورسائل الفاكس والبريد الإلكتروني، الأمر الذي يتيح تحليل الإشارات التي تلتقطها الأقمار الصناعية حتى إن كانت واهنة أو مشفرة (BBC,2001)

- للاستاذة يمكن الرجوع الى كتاب الجريمة عبر الانترنت للدكتور ممدوح

عبدالمطلب ص ٣٠ – ٤٥ .

-3القرصنة :

يقصد بالقرصنة هنا الاستخدام او/و النسخ غير المشروع لنظم التشغيل أو/ولبرامج الحاسب الآلي المختلفة .وقدتطورت وسائل القرصنة مع تطور التقنية، ففي عصر الإنترنت تطورت صور القرصنة واتسعت واصبح من الشائع جدا العثور على مواقع بالإنترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي رمزي. وقد ادت قرصنة البرامج إلى خسائر مادية باهضة جدا وصلت في العام (١٩٨٨م) إلى (١١) مليار دولار امريكي في مجال البرمجيات وحدها، ولذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد وأن شاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات ومن ذلك منظمة اتحاد برمجيات الاعمال Busines) (Software Alliance أو ما تعرف اختصارا بـ(BSA)، والتى اجرت دراسة تبين منها ان القرصنة على الإنترنت ستطغى على انواع القرصنة الاخرى، ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الإنترنت ومنها تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم على الإنترنت لمعرفة مدى استخدام المتصفح للموقع لبرامج مقرصنة الا ان تلك الشركات تراجعت عن هذا التهديد اثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الإنترنت . كما قامت بعض تلك الشركات بالاتفاق مع مزودي الخدمة لابلاغهم عن اي مواقع مخصصة للبرامج المقرصنة تنشأ لديهم وذلك لتقديم شكوي ضدهم ومقاضاتهم ان امكن أو اقفال تلك المواقع على اقل تقدير. والقرصنة عربيا لا تختلف كثيرا عن القرصنة عالميا ان لم تسبقها بخطوات خاصة في ظل عدم توفر حقوق الحماية الفكرية أو في عدم جدية تطبيق هذه القوأن ين ان وجدت(فادي، نوفمبر ١٩٩٩م : ٢٨-)٣٥

.الارهاب الالكتروني :

في عصر الازدهار الالكتروني وفي زمن قيام حكومات الكترونية كما في الامارات العربية المتحدة، تبدل نمط الحياة وتغيرت معه اشكال الاشياء وأن ماطها ومنها ولا شك انماط الجريمة والتي قد يحتفظ بعضها بمسماها التقليدي مع تغيير جوهري أو

بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها القديمة في اسمها جريمة الارهاب والتى اخذت منحنى حديث يتماشى مع التطور التقنى.
وقد انتبه الغرب إلى قضية الارهاب الالكتروني منذ فترة مبكرة، فقد شكل الرئيس الامريكي بيل كلنتون لجنة خاصة (www.nipc.gov) مهمتها حماية البنية التحتية الحساسة في امريكا والتى قامت في خطوة اولى بتحديد الاهداف المحتملة استهدافها من قبل الارهابين ومنها مصادر الطاقة الكهربائية والاتصالات اضافة إلى شبكات الحاسب الآلي، ومن ثم تم انشاء مراكز خاصة في كل ولاية للتعامل مع احتمالات أي هجمات ارهابية الكترونية، كما قامت وكالة الاستخبارات المركزية بانشاء مركز حروب المعلوماتية وظفت به الفا من خبراء امن المعلومات، كما شكلت قوة ضاربة لمواجهة الارهاب على مدار الساعة ولم يقتصر هذا الامر على هذه الوكالة بل تعداه إلى الأجهزة الحكومية الاخرى كالمباحث الفدرالية والقوات الجوية. وبعد الهجمات الاخيرة على الولايات المتحدة الامريكية ارتفعت اصوات البعض بممارسة الارهاب الالكتروني ضد المواقع الاسلامية والعربية التى يشتبه بانها تدعم الارهاب، واوردت شبكة (CNET) الاخبارية خبرا عن اتفاق (٦٠) خبيرا في امن الشبكات ببدء تلك الهجمات الارهابية على مواقع فلسطينية وافغانية. (مجلة انترنت العالم العربي، ٢٠٠١م (
وحذّر تقرير صدر من وزارة الدفاع الامريكية عام ١٩٩٧م من ((بيرل هاربور الكترونية)) في اشارة إلى الهجوم المفاجئ الذى شنه سلاح الجو الياباني على الاسطول الامريكي في ميناء ((بيرل هاربور)) اثناء الحرب العالمية الثانية، وتوقع التقرير ان يزداد الهجوم على نظم المعلومات في الولايات المتحدة الامريكية من قبل الجماعات الارهابية أو عصابات الاجرام المنظم أو عملاء المخابرات الاجنبية وأن يصل هذا الهجوم إلى ذروته عام2005 م ، واوضح التقرير ان شبكة الاتصالات ومصادر الطاقة الكهربائية والبنوك وصناعات النقل في الولايات المتحدة الامريكية معرضة للهجوم من قبل أي جهة تسعى لمحاربة الولايات المتحدة الامريكية دون ان تواجه قواتها المسلحة. (داود، ١٤٢٠هـ (

.4الجرائم المنظمة :
يتبادر إلى الذهن فور التحدث عن الجريمة المنظمة عصابات المافيا كون تلك العصابات من اشهر المؤسسات الاجرامية المنظمة. وقد سارعت عصابات المافيا بالاخذ بوسائل التقنية الحديثة سواء في تنظيم أو تنفيذ اعمالها، ومن ذلك انشاء مواقع خاصة بها على شبكة الإنترنت لمساعدتها في ادارة العمليات وتلقي المراسلات واصطياد الضحايا وتوسيع اعمال وغسيل الاموال، كما تستخدم تلك المواقع في انشاء مواقع افتراضية تساعد المنظمة في تجاوز قوأن ين بلد محدد بحيث تعمل في بلد اخر يسمح بتلك الانشطة. ويوجد على الشبكة (٢١٠) موقع يحتوي اسم نطاقها على كلمة مافيا، في حين يوجد (٢٤) موقعا يحتوى على كلمة

مافيا، كما وجد (4) مواقع للمافيا اليهودية. وقد خصص بعض هذه المواقع للاعضاء فقط ولم يسمح.
لغيرهم بتصفح تلك المواقع في حين سمحت بعض المواقع للعامة بتصفح الموقع وقامت مواقع اخرى بوضع استمارة تسجيل لمن يرغب في الانضمام إلى العصابة من الاعضاء الجدد) .الجنيدي(أ)، ١٩٩٩م : ٣٦(
والجريمة المنظمة ليست وليدة التقدم التقني وأن كانت استفادت كثيرا منه فا" الجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنلوجيا والعولمة أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان وأن ما أصبح إنتشارها على نطاق واسع وكبير وأصبحت لاتحدها الحدود الجغرافية"(اليوسف، ١٤٢٠هـ ، ص : ٢٠١(، كما أستغلت عصابات الجريمة المنظمة " الامكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الاجرامية وتنفيذ وتوجيه العمليات الاجرامية بيسر وسهولة " (حبوش،١٤٢٠هـ: ٢٥٣)
٥- .المواقع المشبوهة:
يكثر انتشار الكثير من المواقع غير المرغوب فيها على شبكة الإنترنت ومن هذه المواقع ما يكون موجها ضد سياسة دولة محددة أو ضد عقيدة أو مذهب معين. وهي تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد المستهدف.
ففي المواقع السياسية المعادية يتم غالبا تلفيق الاخبار والمعلومات ولو زورا وبهتانا أو حتى الاستناد إلى جزيئ بسيط جدا من الحقيقة ومن ثم نسج الاخبار الملفقة جولها، وغالبا ما يعمد اصحاب تلك المواقع إلى انشاء قاعدة بيانات بعناوين اشخاص يحصلون عليها من الشركات التى تبيع قواعد البيانات تلك أو بطرق اخرى ومن ثم يضيفون تلك العناوين قسرا إلى قائمتهم البريدية ويبدأو في اغراق تلك العناوين بمنشوراتهم، وهم عادة يلجئون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضون له ولايصال اصواتهم إلى اكبر قدر ممكن. اما المواقع المعادية للعقيدة فمنها ما يكون موجها من قبل اعداء حاقدين من اتباع الديانات الاخرى كالمواقع التى تنشئها الجاليات اليهودية أو النصرانية تحت مسميات اسلامية بقصد بث معلومات خاطئة عن الاسلام والقران، أو بهدف الدعاية للاديان الاخرى ونشر الشبهه والافتراءت حول الاسلام ومن أمثلة هذه المواقع:
موقع http://www.answering-islam.org/
وموقع http://www.aboutislam.com/
وموقع/http://www.thequran.com/
اما القسم الثاني من المواقع المعادية للعقيدة فهي المواقع التى يكون افرادها من ذات العقيدة واحدة ولكن يختلفون في المذاهب .

6.المواقع المتخصصة في القذف وتشويه سمعة الاشخاص:
المواقع الموجهة ضد اشخاص محددين فهي موجود ولكنها ليست منتشرة انتشار المواقع الاخرى وتركز هجومها غالبا على ابراز سلبيات الشخص المستهدف و نشر بعض اسراره سواء التى يتم الحصول عليها بطريقة غير مشروعة بعد الدخول

على جهازه والعبث به أو بتلفيق الاخبار عنه .وهناك حادثة مشهورة وقعت في بداية دخول الإنترنت وجرىتداولها بين مستخدمى الإنترنت حول قيام شخص في دولة خليجية بإنشاء موقع خاص بفتاة قام بنشر صورها عارية اضافة إلى صور اخرى مع صديقها وهي في اوضاع مخلة والتي حصل علي تلك الصور بعد التسلل إلى حاسبها الشخصي وسرقة تلك الصور منه ومن ثم حاول ابتزازها جنسيا وعندما رفضت هددها بنشر تلك الصور في موقع على الإنترنت فاصرت على الرفض فقام بتنفيذ تهديده ووزع الرابط لذلك الموقع على العديد من المنتديات والقوائم البريدية وادى ذلك إلى انتحار الفتاة حيث فضحها بين ذويها ومعارفها.
كما وقعت حادثة تشهير اخرى من قبل من اسموا نفسهم " الامجاد هكرز " حيث اصدروا بيان نشر على الإنترنت بواسطة البريد الالتكروني ووصل العديد من مشتركي الإنترنت واوضحوا فيه قيام شخص يكنى بحجازي نادي الفكر في احدى المنتديات (منتديات الحجاز للحوار) على التطاول بالقدح والسب السافر على شيخ الإسلام ابن تيمية والشيخ محمد بن عبدالوهاب وغيرهم من رموز الدعوة السلفية وقد استطاع (الأمجاد هكرز) اختراق الموقع المذكور واختراق البريد الإلكتروني الشخصي للمكنى حجازي نادي الفكر ومن ثم تم نشر صوره وكشف اسراره في موقعهم على الإنترنت حيث خصصوا صفحة خاصة للتشهير بالمذكور وعنوانها على الشبكة هو (http://216.169.120.174/hijazi.htm : موقع منتدى الفوائد،١٤٢١هـ(

.7المواقع والقوائم البريدية الاباحية:
"أصبح الانتشار الواسع للصور والافلام الاباحية على شبكة الإنترنت يشكل قضية ذات اهتمام عالمي في الوقت الراهن، بسبب الازدياد الهائل في اعداد مستخدمي الإنترنت حول العالم " (الزعاليل، ١٤٢٠هـ: ٧٦(، وتختلف المواقع والقوائم البريدية الاباحية عن المواقع المشبوهة والمصنفة في البند السابق في كون ان هذه المواقع والقوائم البريدية مخصصة لنشر الصور الجنسية بكافة انواعها واشكالها، وتختلف المواقع الاباحية عن القوائم البريدية - التى تخصص لتبادل الصور والافلام الجنسية - في ان المواقع الاباحية غالبا ما يكون الهدف منها الربح المادي حيث يستوجب على متصفح هذه المواقع دفع مبلغ مقطوع مقابل مشاهدة فيلم لوقت محدد أو دفع اشتراك شهري أو سنوي مقابل الاستفادة من خدمات هذه المواقع، وأن كانت بعض هذه المواقع تحاول استدراج مرتاديها بتقديم خدمة ارسال صور جنسية مجانية يومية على عناويهم البريدية.
اما القوائم البريدية فهي غالبا مجانية ويقوم اعضائها من المشتركين بتبادل الصور والافلام على عناوينهم البريدية وربما تكون القوائم البريدية ابعد عن امكانية المتابعة الأمنية حيث يركز نشاطها على الرسائل البريدية والتى تكون من الصعوبة بمكان منعها عن اعضاء اي مجموعة، حتى وأن تم الانتباه إلى تلك القائمة لاحقا وتم حجبها، فان الحجب يكون قاصرا على المشتركين الجدد واللذين لا يتوفر لديهم وسائل تجاوز المرشحات، اما الاعضاء السابقين فلا حاجة لهم إلى الدخول إلى

موقع القائمة حيث يصل إلى بريديهم ما يحتاونه دون ان تستطيع وسائل الحجب التدخل.
واستفادت هذه المواقع والقوائم من الانتشار الواسع للشبكة والمزايا الاخرى التى تقدمها حيث " تتيح شبكة الإنترنت أفضل الوسائل لتوزيع الصور الفاضحة والافلام الخليعة بشكل علنى فاضح يقتحم على الجميع بيوتهم ومكاتبهم، فهناك على الشبكة طوفان هائل من هذه الصور والمقالات والافلام الفاضحة بشكل لم يسبق له مثيل في التاريخ" (داود،١٤٢٠هـ : ٩٣)، فكل مستخدم للانترنت معرض للتأثر بما يتم عرضه على الإنترنت الذي لا يعترف باي حدود دولية أو جغرافية فهو يشكل خطرا حقيقيا للاطفال فضلا عن الكبار نتيجة تاثيراته المؤذية وغير المرغوبة(موثق في الزغاليل، ١٤٢٠هـ .(78 : ويوجد على الإنترنت الاف المواقع الاباحية وعدد كبير جدا من القوائم الجنسية والتى اصبحت اكثر تخصصا فهناك قوائم خاصة للشواذ من الجنسين وهناك قوائم اخرى تصنف تحت دول محددة ومن المؤسف انه وجدت بعض المواقع الشاذة بمسميات عربية بل وسعودية والادهى والامر ان يربط بين بعض القوائم الاباحية والاسلام كموقع اسمى نفسه " السحاقيات المسلمات " وهكذا.
وكشفت احدى الدراسات ان معدل التدفق على الواقع الاباحية في اوقات العمل التى تبدأ من الساعة التاسعة صباحا إلى الخامسة عصرا تمثل (٪70) من اجمالي نسبة التدفق على تلك المواقع.(بي بي سي، ٢٠٠١/٦/١٢م.(
كما كشفت دراسة قام بها الدكتور مشعل القدهي بان هناك اقبال كبير جدا على المواقع الاباحية حيث تزعم شركة (Playboy) الاباحية بأن (٤,٧) مليون زائر يزور صفحاتهم على الشبكة اسبوعيا، وبان بعض الصفحات الاباحية يزورها (٢٨٠٠٣٤) زائر يوميا وأن هناك مائة صفحة مشابهة تستقبل اكثر من (٢٠٠٠٠) الف زائر يوميا واكثر من الفين صفحة مشابهة تستقبل اكثر من (١٤٠٠) زائر يوميا، وأن صفحة واحدة من هذه الصفحات استقبلت خلال عامين عدد (٤٣٦١٣٥٠٨) مليون زائر ، كما وجد ان (٨٣,٥٪) من الصور المتداولة في المجموعات الاخبارية هي صور اباحية، وبان اكثر من (٢٠٪) من سكان امريكا يزورون الصفحات الاباحية حيث تبدأ الزيارة غالبا بفضول وتتطور إلى ادمان، وغالبا لا يتردد زوار هذه المواقع من دفع رسوم مالية لقاء تصفح المواد الاباحية بها أو شراء مواد خليعة منها وقد بلغت مجموعة مشتروات مواد الدعرة في الإنترنت في عام (١٩٩٩م) ما نسبته (٨٪) من دخل التجارة الإلكترونية البالغ (١٨) مليار دولار امريكي في حين بلغت مجموعة الاموال المنفقة للدخول على المواقع الاباحية (٩٧٠) مليون دولار ويتوقع ارتفاع المبلغ ليصل إلى (٣) مليار دولار في عام (٢٠٠٣م)، وقد اتضح ان اكثر مستخدمى المواد الاباحية تتراوح اعمارهم ما بين (١٢) و (١٥) عام في حين تمثل الصفحات الاباحية اكثر صفحات الإنترنت بحثا وطلبا(القدهي،١٤٢٢هـ .(
كما وضحت دراسة أدست (Adsit) عن إدمان المواقع الاباحية ان المواقع الاباحية اصبحت مشكلة حقيقية وأن الاثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون

الاخر، ويمكن ان يلمس اثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة وإغتصاب الاطفال بصفة خاصة، العنف الجنسي، فقد العائلة لقيمها ومبادئها وتغيير الشعور نحو النساء إلى الابتذال بدل الاحترام. ويبدوا ان لكثرة المواقع الاباحية على الإنترنت والتى يقدر عددها بحوالي (70.000) ألف موقع دور كبير في ادمان مستخدمي الإنترنت عليها حيث اتضح ان نسبة ٪15 من مستخدمي الإنترنت البالغ عددهم(٩,٦٠٠,٠٠٠) مليون شخص تصفحوا المواقع الاباحية في شهر ابريل عام ١٩٩٨م(Adsit, 1999)(
وقد جرت محاولة حصر القوائم العربية الاباحية في بعض المواقع على شبكة الإنترنت ومنها موقع الياهو (YAHOO) فوجد انها تصل إلى (١٧١) قائمة، بلغ عدد اعضاء اقل تلك القوائم (٣) في حين وصل عدد اكثرها أعضاء إلى (٨٦٨٣). اما موقع قلوب لست (GLOBELIST) فقد احتوى على (٦ (قوائم اباحية عربية ، في حين وجد عدد (٥) قوائم عربية اباحية على موقع توبيكا (TOPICA)وقد قامت مدينة الملك عبدالعزيز للعلوم والتقنية مشكورة باغلاق تلك المواقع .

.8تزوير البيانات:
تعتبر من اكثر جرائم نظم المعلومات انتشارا فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من اشكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها أو اضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك. وقد وقعت حادثة في ولاية كاليفورنيا الامريكية حيث عمدت مدخلة البيانات بنادي السيارات وبناء لاتفاقية مسبقة بتغيير ملكية السيارات المسجلة في الحاسب الآلي بحث تصبح باسم احد لصوص السيارات والذي يعمد إلى سرقة السيارة وبيعها وعندما يتقدم مالك السيارة للابلاغ يتضح عدم وجود سجلات للسيارة باسمه وبعد بيع السيارة تقوم تلك الفتاة باعادة تسجيل السيارة باسم مالكها وكانت تتقاضي مقابل ذلك مبلغ مائة دولار واستمرت في عملها هذا إلى ان قبض عليها، وفي حادثة الخرى قام مشرف تشغيل الحاسب باحد البنوك الامريكية بعملية تزوير حسابات اصدقائه في البنك بحيث تزيد ارصدتهم ومن ثم يتم سحب تلك المبالغ من قبل اصدقائه وقد نجح في ذلك وكان ينوى التوقف قبل موعد المراجعة الدورية لحسابات البنك الا ان طمع اصدقاءه اجبره على الاستمرار إلى ان قبض عليه)داود، ١٤٢٠هـ : ٤٥- ٤٧). ومما لاشك فيه ان البدء التدريجي في التحول إلى الحكومات الإلكترونية سيزيد من فرص ارتكاب مثل هذه الجرائم حيث سترتبط الكثير من الشركات والبنوك بالإنترنت مما يسهل الدخول على تلك الانظمة من قبل محترفي اختراق الانظمة وتزوير البيانات لخدمة اهدافهم الاجرامية .

.9غسيل الاموال:
مصطلح حديث نسبيا ولم يكن معروفا لرجال الشرطة فضلا عن العامة وقد بدأ استخدام المصطلح في امريكا نسبة إلى مؤسسات الغسيل التى تملكها المافيا، وكان

اول استعمال قانوني لها في عام ١٩٣١م إثر محاكمة لاحد زعماء المافيا تمت في امريكا واشتملت مصادرة اموال قيل انها متأتية من الاتجار غير المشروع بالمخدرات. واختلف الكثير في تعريف غسيل الاموال وقد يكون التعريف الاشمل هو " أي عملية من شأنها اخفاء المصدر غير المشروع الذي اكتسبت منه الاموال"(عيد، ١٤٢٢هـ: ١٢٤-١٢٥(

ومن البديهي ان ياخذ المجرمون باحدث ما توصلت اليه التقنية لخدمة أنشطتهم الاجرامية ويشمل ذلك بالطبع طرق غسيل الاموال التى استفادت من عصر التقنية فلجأت إلى الإنترنت لتوسعة وتسريع اعمالها في غسيل اموالها غير المشروعة، ويجد المتصفح للانترنت مواقع متعددة تتحدث عن غسيل اموال ومنها الموقع http://www.laundryman.u.net.com:كما يجد ولا شك ايضا المواقع التى تستخدم كساتر لعمليات غسيل الاموال ومنها المواقع الافتراضية لنوادي القمار والتى قام مكتب المباحث الفدرالية (FBI)الامريكي بمراقبة بعض هذه المواقع واتضح انها تتواجد في كاراكاو، جزر الانتيل، جزيرة أنتيجوا وجمهورية الدومينكان وقد اسفرت التحريات التى استمرت خمسة اشهر عن اعتقالات واتهامات للعديد من مدراء تلك المواقع.ومن المميزات التى يعطيها الإنترنت لعملية غسيل الاموال السرعة، اغفال التوقيع وأن عدام الحواجز الحدودية بين الدول، كما تسأهم البطاقات الذكية، والتى تشبه في عملها بطاقات البنوك المستخدمة في مكائن الصرف الآلية، في تحويل الاموال بواسطة المودم أو الإنترنت مع ضمان تشفير وتأمين العملية. كل هذا جعل عمليات غسيل الاموال عبر الإنترنت تتم بسرعة اكبر وبدون ترك اي اثار في الغالب. ويقدر المتخصصون المبالغ التى يتم تنظيفها سنويا بـحوالي (٤٠٠) مليار دولار (عبدالمطلب،٢٠٠١م : ٦٨(72 -

.10القمار عبر الإنترنت:

كثيرا ما تتداخل عملية غسيل الامول مع اندية القمار المنتشرة، الامر الذي جعل مواقع الكازيهونات الافتراضية على الإنترنت محل اشتباه ومراقبة من قبل السلطات الامريكية. وبالرغم من ان سوق القمار في امريكا يعتبر الاسرع نموا على الاطلاق الا ان المشكلة القانونية التى تواجه اصحاب مواقع القمار الافتراضية على الإنترنت انها غير مصرح لها حتى الان في امريكا بعكس نوادي القمار الحقيقية كالمنتشرة في لاس فيجاس وغيرها، ولذلك يلجأ بعض اصحاب تلك المواقع الافتراضية على الإنترنت إلى انشائها وادارتها من اماكن مجاورة لامريكا وخاصة في جزيرة انتيجوا على الكاريبي .

ويوجد على الإنترنت اكثر من الف موقع للقمار يسمح لمرتاديه من مستخدمى الإنترنت ممارسة جميع انواع القمار التى توفرها المواقع الحقيقية، ومن المتوقع ان ينفق الامريكيون ما يزيد عن (٦٠٠) مليار دولار سنويا في اندية القمار وسيكون نصيب مواقع الإنترنت منها حوالي مليار دولار.

وقد حاول المشرعون الامريكيون تحريك مشروع قانون يمنع المقامرة عبر الإنترنت ويسمح بملاحقة اللذين يستخدمون المقامرة السلكية أو اللذين يروجون لها

سواء كانت هذه المواقع في امريكا أو خارجها (عبدالمطلب، ٢٠٠١م : ٧٨ – ٨٢)

.11تجارة المخدرات عبر الإنترنت :
كثيرا ما يحدّر اولياء الامور ابنائهم من رفقاء السوء خشية من تأثيرهم السلبي عليهم وخاصة في تعريفهم على المخدرات فالصاحب ساحب كما يقول المثل وهذا صحيح ولا غبار عليه ولكن وفي عصر الإنترنت اضيف إلى اولياء الامور مخاوف جديدة لا تقتصر على رفقاء السوء فقط بل يمكن ان يضاف اليها مواقع السوء - ان صح التعبير -ومن تلك المواقع طبعا المواقع المنتشرة في الإنترنت والتى لاتتعلق بالترويج للمخدرات وتشويق النشئ لاستخدانها بل تتعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافة اصنافها وأن واعها وبأبسط الوسائل المتاحة. والامر هنا لايحتاج إلى رفاق سوء بل يمكن للمراهق الانزواء في غرفته والدخول إلى اي من هذه المواقع ومن ثم تطبيق ما يقرأه ويؤكد هذه المخاوف أحد الخبراء التربوين في بتسبيرج بالولايات المتحدة والذي أكد إن ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات وأن ترنت. ولا تقتصر ثقافة المخدرات على تلك المواقع فقط بل تسأهم المنتديات وغرف الدردشة في ذلك ايضا .وبالرغم من انتشار المواقع الخاصة بالترويج للمخدرات وتعليم كيفية صنعها الا ان هذه المواقع لم تدق جرس الانذار بعد ولم يهتم باثارها السلبية وخاصة على النشئ كما فعلته المواقع الاباحية وخاصة في الدول التى تعرف باسم الدول المتقدمة، وقد اعترف الناطق الرسمي للتحالف المناهض للمخدرات بانهم خسروا الجولة الاولي في ساحة الإنترنت حيث لم يطلق موقعهم الخاص على الشبكة http://www.cadca.org الا منذ عامين فقط. وبالاضافة إلى هذا الموقع توجد مواقع اخرى تحارب المخدرات وتساعد المدمنين على تجاوز محنتهم ومن ذلك الموقع الخاص بجماعة-Join) Together)وعنوانهم على النت هو http://192.12.191.21 إلا أن هذه المواقع قليلة العدد والفائدة مقارنة بكثرة وقوة المواقع المضادة(الجنيدي(ب)، ١٩٩٩م : ٣٩-٤٠ .(

.12تهديدات التجارة الإلكترونية:
بدأ مفهموم التجارة الإلكترونية ينتشر في السبعينات الميلادية وذلك لسهولة الاتصال بين الطرفين ولامكانية اختزال العمليات الورقية والبشرية فضلا عن السرعة في ارسال البيانات وتخفيض تكلفة التشغيل والأهم هو ايجاد اسواق اكثر اتساعا.
ونتيجة لذلك فقد تحول العديد من شركات الاعمال إلى استخدام الإنترنت والاستفادة من مزايا التجارة الإلكترونية ، كما نحول تبعا لذلك الخطر الذي كان يهدد التجارة السابقة ليصبح خطرا متوافقا مع التجارة الإلكترونية . فالاستيلاء على بطاقات الائتمان عبر الإنترنت امر ليس بالصعوبة بمكان اطلاقا، فـ" لصوص بطاقات الائتمان مثلا يستطيعون الان سرقة مئات الالوف من ارقام البطاقات في يوم واحد من خلال شبكة الإنترنت ، ومن ثم بيع هذه المعلومات للاخرين " (داود،

١٤٢٠هـ: ٧٣) وقد وقع بالفعل بعض الحوادث التى قام اصحابها باستخدام الإنترنت لتنفيذ عملياتهم الاجرامية ومن ذلك حادثة شخص الماني قام بالدخول غير المشروع إلى احد مزود الخدمات واستولى على ارقام بطاقات ائتمانية الخاصة بالمشتركين ومن ثم هدد مزود الخدمة بافشاء ارقام تلك البطاقات ما لم يستلم فدية وقد تمكنت الشرطة الالمانية من القبض عليه. كما قام شخصان في عام (١٩٩٤م) بانشاء موقع على الإنترنت مخصص لشراء طلبات يتم بعثها فور تسديد قيمتها الكترونيا، ولم تكن الطلبات لتصل اطلاقا حيث كان الموقع وهمي قصد منه النصب والاحتيال وقد قبض على مؤسسيه لاحقا.(موثق في عبدالمطلب، ٢٠٠١م (85 : واثبت شبكة (MSNBC) عمليا سهولة الحصول على ارقام بطاقات الائتمان من الإنترنت ، حيث قامت بعرض قوائم تحتوي على اكثر من (٢٥٠٠) رقم بطاقة ائتمان حصلت عليها من سبعة مواقع للتجارة الإلكترونية باستخدام قواعد بيانات متوفرة تجاريا، ولم يكن يصعب على اي متطفل استخدام ذات الوسيلة البدائية للاستيلاء على ارقام تلك البطاقات واستخدامها في عمليات شراء يدفع قيمتها اصحابها الحقيقين. ويقترح بعض الخبراء باستخدام بطاقة ائتمان خاصة بالإنترنت يكون حدها الائتماني معقول بحيث يقلل من مخاطر فقدانها والاستيلاء غير المشروع عليها، وهو الامر الذي بدأت بعض البنوك الدولية والمحلية في تطبيقه اخيرا. (عبدالمطلب،٢٠٠١م : ٨٦ – ٩٠(

ويتعدى الامر المخاطر الأمنية التى تتعرض لها بطاقات الائتمان فنحن في بداية ثورة نقدية تعرف باسم النقود الإلكترونية (Electronic Cach) أو (Cyber Cash)والتى يتنبأ لها ان تكون مكملة للنقود الورقية والبلاستيكية (بطاقات الائتمان) وأن يزداد الاعتماد عليها والثقة بها، كما ان هناك الاسهم والسندات الإلكترونية المعمول بها في دول الاتحاد الاوروبي والتى اقر الكونجرس الامريكي التعامل بها في عام ١٩٩٠م، وبالتالي فان التعامل معها من خلال الإنترنت سيواجه مخاطر امنية ولا شك. ولذلك لجأت بعض الشركات والبنوك إلى العمل سويا لتجاوز هذه المخاطر كالاتفاق الذي وقع بين مؤسسة هونج كونج وشنغهاي البنكية (HSBC)وهي من اكبر المؤسسات المصرفية في هونج كونج وشركة كومباك للحاسب الآلي وذلك لتطوير اول نظام الي آمن للتجارة الالتكرونية والذي يمنح التجار خدمة نظام دفع امن لتمرير عمليات الشراء عبر الإنترنت . (داود، ١٤٢٠هـ (124 – 123 :

.13جرائم ذوي الياقات البيضاء :

لم يظهر هذا المصطلح من الجرائم الا حديثا ويرجع الفضل في ذلك إلى عالم الاجتماع سذرلاند (Sutherland) وترتكب هذه الجرائم من قبل الطبقة الراقية في المجتمع ذوي المناصب الادارية الكبيرة، وتشمل انواعا مختلفة من الجرائم كالرشوة والتلاعب بالشيكات والاختلاس والسرقة وتزوير العلامات التجارية للشركات العالمية ووضعها على منتجات محلية أو عالمية غير مشهورة وشراء المعلبات قبل انتهاء صلاحيتها واستبدال تاريخ صلاحيتها .وهذا النوع من المشاكل يصعب

ارتكابها أو كشفها والتحقيق فيها دون المام جيد بظروف الانتاج والحسابات الجارية والعمل التجاري ومبادي التقنية الحسابية الالتكرونية .وقدرت خسائر المجتمع الامريكي بمبلغ (١٢– ٤٢) مليون دولار سنويا نتيجة خداع المستهلكين باستخدام جميع وسائل التكنلوجيا المتقدمة(اليوسف،١٤٢٠هـ.(211-209 :واستفاد مرتكبوا هذه الجرائم من انتشار الإنترنت في تطوير جرائمهم وطرق ارتكابها وتوسعة الرقعة الجغرافية لها بحيث اصبحت عالمية بعد ان كانت محلية.

.14الجرائم الاقتصادية :

تتنوع الجرائم الاقتصادية بتنوع النظام السائد في الدولة فعلى سبيل المثال في الدول الراسمالية نجد ان اغلب الجرائم الاقتصادية تتمحور حول الاحتكارات والتهرب الضريبي والجمركي والسطو على المصارف وتجارة الرقيق الابيض والاطفال، في حين تتمحور تلك الجرائم في النظام الاشتراكي على الرشوة والاختلاس والسوق السوداء. وهذا لا يعنى بالضرورة انه لايمكن ارتكاب كل انواع هذه الجرائم في مجتمع واحد حيث يمكن ان تجد في المجتمع الراسمالي مثلا جرائم رشوة واختلاسات والعكس صحيح. وكما في الجرائم الاخرى فان الإنترنت سأهم في تطوير طرق واساليب ارتكاب هذه الجرائم ووسع منطقة عملها خاصة مع توجه الكثير من الدول في التحول إلى الحكومات اللالكترونية كما في دولة الامارات العربية المتحدة مثلا،حيث استفاد المجرمون من التقدم التقني في اختلاس الاموال وتحويل الارصدة النقدية وكذلك في سرقة التيار الكهربائي والمياه وخطوط الهاتف والعبث بها واتلافها) .اليوسف،١٤٢٠هـ : ٢١١-٢١٤)، ويندرج تحت هذا البند حادثة اقتحام متسللين لنظام الحاسب الآلي الذي يتحكم في تدفق اغلب الكهرباء في مختلف انحاء ولاية كاليفورنيا الامريكية، وبالرغم من ان الهجوم كان محدودا الا انه كشف عن ثغرات امنية في نظام الحاسب الآلي لشركة الكهرباء وقد اوضح هذا الخبر موقع ارابيا على شبكة الإنترنت بتاريخ ٢٠٠١/٦/١٠م واستند فيه إلى خبر نشر في صحيفة لوس انجلوس تايمز الامريكية في اليوم السابق. (موقع ارابيا،٢٠٠١/٦/١٠م(

.15انتهاك الخصوصية:

تتفق الشتريعات السماوية والانظمة الوضعية على ضرورة احترام خصوية الفرد ويعتبر مجرد التطفل على تلك المعلومات سواء كانت مخزنة في الحاسب الآلي أو في بريده الالتكروني أو في أي مكان اخر انتهاكاً لخصوصيته الفردية. وأدى انتشار الإنترنت إلى تعرض الكثير من مستخدمي الإنترنت لانتهاك خصوصياتهم الفردية سواء عمدا أو مصادفة، فبكل بساطة ما أن يزور مستخدم الإنترنت أي موقع على شبكة الإنترنت حتى يقوم ذلك الموقع باصدار نسختين من الكعكة الخاصة باجهزتهم (Cookies)وهي نصوص صغيرة يرسلها العديد من مواقع الويب لتخزينها في جهاز من يزور تلك المواقع لعدة اسباب لعل منها التعرف على من

يكرر الزيارة للموقع أولاسباب اخرى، وتبقى واحدة من الكعكات في الخادم (السيرفر) الخاص بهم والأخرى يتم تخزينها على القرص الصلب لجهاز الزائر للموقع في أحد الملفات التي قامت الموقع الأخرى بتخزينها من قبل دون أن يشعر صاحب الجهاز بذلك أو حتى الاستئذان منه! وفورا يتم اصدار رقم خاص ليميز ذلك الزائر عن غيره من الزوار وتبدأ الكعكة بأداء مهمتها بجمع المعلومات وارسالها إلى مصدرها أو احدى شركات الجمع والتحليل للمعلومات وهي عادة ما تكون شركات دعاية وإعلان وكلما قام ذلك الشخص بزيارة الموقع يتم ارسال المعلومات وتجديد النسخة الموجودة لديهم ويقوم المتصفح لديه بعمل المهمة المطلوبة منه مالم يقم صاحب الجهاز بتعديل وضعها، وقد تستغل بعض المواقع المشبوهة هذه الكعكات بنسخ تلك الملفات والاستفادة منها بطريقة أو باخرى. كما قد يحصل اصحاب المواقع على معلومات شخصية لصاحب الجهاز طوعا حيث يكون الشخص عادة اقل ترددا عندما يفشى معلوماته الشخصية من خلال تعامله مع جهاز الحاسب الآلي بعكس لو كان الذي يتعامل معه انسان اخر(داود،١٤٢٠هـ: ٥٠-٥٢) و (موقع صافولا ، ١٤٢١هـ.(

و هناك وسائل لحماية الخصوصية اثناء تصفح الإنترنت ، ولكن " من الصعب جدا السيطرة على ما يحدث للمعلومة بمجرد خروجها من جهاز الحاسب (الآلي (وعلى ذلك فان حماية الخصوصية يجب ان تبدأ من البداية بتحديد نوعية البيانات التى لاينبغي ان تصبح عامة ومشاعة ثم بتقييد الوصول إلى تلك المعلومات" (داود، ١٤٢٠هـ (53 :

16.إنتحال شخصية الفرد :

تعتبر جرائم انتحال الشخصية من الجرائم القديمة الا ان التنامي المتزايد لشبكة الإنترنت اعطى المجرمين قدرة اكبر على جمع المعلومات الشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم. فتنتشر في شبكة الإنترنت الكثير من الاعلانات المشبوهة والتى تداعب عادة عريزة الطمع الانساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك مثلا اعلان عن جائزة فخمة يكسبها من يسأهم بمبلغ رمزي لجهة خيرية والذي يتطلب بطبيعة الحال الافصاح عن بعض المعلومات الشخصية كالاسم والعنوأن والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، وبالرغم من ان مثل هذا الاعلان من الوضوح بمكان انه عملية نصب واحتيال الا انه ليس من المستبعد ان يقع ضحيته الكثير من مستخدمي الإنترنت . ويمكن ان تؤدي جريمة انتحال الشخصية إلى الاستيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو حتى الاساءة إلى سمعة الضحية. (داود، ١٤٢٠هـ: ٨٤-٨٩ (

17.انتحال شخصية المواقع:

مع ان هذا الاسوب يعتبر حديث نسبيا الا انه اشد خطورة واكثر صعوبة في اكتشافه من انتحال شخصية الافراد، حيث يمكن تنفيذ هذا الاسلوب حتى مع المواقع

التى يتم الاتصال بها من خلال نظم الاتصال الامن (Secured Server) حيث يمكن وبسهولة اختراق مثل هذا الحاجز الامني، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني، أو يحاول المجرم اختراق موقع لاحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور. ويتوقع ان يكثر استخدام اسلوب انتحال شخصية المواقع في المستقبل نظرا لصعوبة اكتشافها(داود، ١٤٢٠هـ:٨٩-٩٣.(

18.الاغراق بالرسائل :

يلجأ بعض الاشخاص إلى ارسال مئات الرسائل إلى البريد الالكتروني لشخص ما بقصد الاضرار به حيث يؤدى ذلك إلى تعطل الشبكة وعدم امكانية استقبال أي رسائل فضلا عن امكانية انقطاع الخدمة وخاصة اذا كانت الجهة المضررة من ذلك هي مقدمة خدمة الإنترنت مثلا حيث يتم ملء منافذ الاتصال (Communication-Ports)وكذلك قوائم الانتظار (Queues) مما ينتج عنه انقطاع الخدمة وبالتالي تكبد خسائر مادية ومعنوية غير محدودة، ولذلك لجأت بعض الشركات إلى تطوير برامج تسمح باستقبال جزء محدود من الرسائل في حالة تدفق اعداد كبيرة منها(داود،١٤٢٠هـ:٩٣ (

واذا كان هذا هو حال الشركات الكبيرة فلنا ان نتصور حال الشخص العادي اذا تعرض لمحاولة الاغراق بالرسائل حيث لن يصمد بريده طويلا امام هذا السيل المنهمر من الرسائل عديمة الفائدة أو التى قد يصاحبها فيروسات أو صور أو ملفات كبيرة الحجم، خاصة اذا علمنا ان مزود الخدمة عادة يعطي مساحة محددة للبريد لا تتجاوز عشرة ميقا كحد اعلى.

19.الفيروسات الحاسب الآلية:

الفيروسات الحاسب الآلية هي احدى انواع البرامج الحاسب الآلية الا أن الاوامر المكتوبة في هذه البرنامج تقتصر على اوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو امر ما أو حتى مجرد فتح البرنامج الحامل لفيروس أو الرسالة البريدية المرسل معها الفيروس اصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به. وقد عرفها احد خبراء الفيروسات (Fred Cohen) بانها نوع من البرامج التى تؤثر في البرامج الاخرى بحيث تعدل في تلك البرامج لتصبح نسخة منها، وهذا يعنى ببساطة أن الفيروس ينسخ نفسه من حاسب الي إلى حاسب الي اخر بحيث يتكاثر باعداد كبيرة .(Highley,1999)ويمكن تقسيم الفيروسات إلى خمسة انواع:

الاول:فيروسات الجزء التشغيلي للاسطوأن ة كفيروس ((Brain و (Newzeland)

الثاني : الفيروسات المتطفلة كفيروس (Cascade) وفيروس.(Vienna)

الثالث :الفيروسات المتعددة الانواع كفيروس (Spanish-Telecom) وفيروس

(Flip)
الرابع : الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوس أو الوندوز الخامس : يعرف بحصان طرواده وهذا النوع يصنفه البعض كنوع مستقل بحد ذاته ،الا انه ادرج في تقسيمنا هنا كاحد انواع الفيروسات، وينسب هذا النوع إلى الحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاء سلمي الا أن اثره التدميري خطير . وتعمل الفيروسات على اخفاء نفسها عن البرامج المضادة للفيروسات باستخدام طرق تشفير لتغيير اشكالها لذلك وجب تحديث برامج الخاصة بمكافحة الفيروسات بصفة دائمة (عيد،١٤١٩هـ : ٦٣-٦٦)

وهناك فريق من الخبراء يضع تقسيما مختلفا للفيروسات على أساس المكان المستهدف بالاصابة داخل جهاز الكمبيوتر ويرون أن هناك ثلاثة أنواع رئيسية من الفيروسات وهي فيروسات قطاع الاقلاع (Boot Sector) وفيروسات الملفات (File Injectors)وفيروسات الماكرو .(Macro Virus) كما أن هناك من يقوم بتقسيم الفيروسات إلى فيروسات الاصابة المباشرة (Direct action) وهي التي تقوم بتنفيذ مهمتها التخريبية فور تنشيطها أو المقيمة (staying) وهي التي تظل كامنة في ذاكرة الكمبيوتر وتنشط بمجرد أن يقوم المستخدم بتنفيذ أمر ما ومعظم الفيروسات المعروفة تندرج تحت هذا المسمى وهناك أيضا الفيروسات المتغيرة (Polymorphs) التي تقوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلل برامج مكافحة الفيروسات).الجزيرة ،٢٠٠٠(

ومن الجرائم المتعلقة بارسال فيروسات حاسوبية قيام شخص امريكي يدعى (Robert Morris)بارسال دودة حاسوبية بتاريخ الثاني من نوفمبر عام (١٩٨٨م) عبر الإنترنت وقد كرر الفيروس نفسه عبر الشبكة بسرعة فاقت توقع مصمم الفايروس وادى ذلك إلى تعطيل ما يقارب من (٦٢٠٠) حاسب إلى مرتبط بالإنترنت ، وقدرت الاضرار التى لحقت بتلك الأجهزة بمئات الملايين من الدولارات. ولو قدر لمصمم الفيروس تصميمه ليكون اشد ضررا لكان قد لحقت اضرار اخرى لا يمكن حصرها بتلك الاجهزة، وقد حكم على المذكور بالسجن ثلاثة سنوات بالرغم من دفاع المذكور بانه لم يكن يقصد احداث مثل تلك الاضرار.(Morningstar, 1998)

20.الاقتحام أو التسلل:

"تتداول الصحف والدوريات العلمية الان أنباء كثيرة عن الاختراقات الأمنية المتعددة في اماكن كثيرة من العالم ليس اخرها اختراق اجهزة الحاسب (الآلي) في البنتاجون (وزارة الدفاع الامريكية) " (داود، ١٤٢٠هـ: ٩٩)، ولكي يتم الاختراق فان المتسللون إلى اجهزة الاخرين يستخدممون ما يعرف بحصان طروادة وهو برنامج صغير يتم تشغيله داخل جهاز الحاسب لكي يقوم بأغراض التجسس على أعمال الشخص التي يقوم بها على حاسوبه الشخصي فهو في أبسط صورة يقوم بتسجيل كل طرقة قام بها على لوحة المفاتيح منذ أول لحظة للتشغيل ويشمل ذلك كل بياناته السرية أو حساباته المالية أو محادثاته الخاصة على الإنترنت أو رقم

بطاقة الائتمان الخاصة به أو حتى كلمات المرور التي يستخدمها لدخول الإنترنت والتي قد يتم إستخدامها بعد ذلك من قبل الجاسوس الذي قام بوضع البرنامج على الحاسب الشخصي للضحية. و" يعتبر الهجوم على المواقع المختلفة في شبكة الإنترنت) اقتحام المواقع) من الجرائم الشائعة في العالم، وقد تعرضت لهذا النوع من الجرائم في الولايات المتحدة مثلا كل من وزارة العدل والمخابرات المركزية والقوات الجوية، كما تعرض له حزب العمال البريطاني " (داود، ١٤٢٠هـ: ٨٣ (وقام قراصنة اسرائيليين باقتحام صفحة الإنترنت الاعلامية الخاصة ببنك فلسطين المحدود ووضعوا بها صورا وشعارات معادية مما اضطر البنك إلى الغاء الصفحة ومحوها كليا، كما تعرضت العديد من الشركات الخاصة في مناطق الحكم الذاتي للهجوم والعبث ومنها شركة اقتحم المتسللون اليها ووضعوا صورة زوجة مدير الشركة وهي عارية بعد تجريدها من الملابس بواسطة الحاسب الآلي (موثق في ابوشامة، ١٤٢٠هـ: ٣٧(

وفي عام(١٩٩٧م) قدّرَتْ وكالة المباحث الفدرالية الامريكية (FBI) تعرض(٤٣٪) من الشركات التى تستخدم خدمة الإنترنت لمحاولة تسلل تتراوح مابين(١-٥) مرات خلال سنة واحدة(Wilson,2000) .، ولا يقتصر التسلل على المحترفين فقط بل انه قد يكون من الهواة ايضا حيث يدفعهم إلى ذلك الفراغ ومحاولة اشغال الوقت، كما حدث مع مراهقة في الخامسة عشر من عمرها قامت بمحاولة التسلل إلى الصفحة العنكبوتية الخاصة بقاعدة عسكرية للغواصات الحربية بسنغافورة وذلك بسبب انها لم تكن تحب مشاهدة التلفزيون لذلك فكرت ان تكون متسللة .(Hacker) (Koerner,1999)

وهذا ايضا هو ما اتضح لوكالة المباحث الفدرالية (FBI) اثناء حرب الخليج الاولى عندما اجروا تحقيقا حول تسلل اشخاص إلى الصفحة العنكبوتية الخاصة باحدى القواعد عسكرية الامريكية، وكانت الشكوك قد اتجهت بداية إلى ارهابين دوليين الا ان الحقيقة تجلت بعد ذلك في ان المتسللين هما مراهقان كانا يعبثان بجهاز الحاسب الآلي في منزلهما(Wilson,2000) ، وفي عام (١٩٩٧م) قام مراهق بالتسلل إلى نظام مراقبة حركة الملاحة الجوية في مطار ماشيتيوشش (Massachusetts) مما ادى إلى تعطيل نظام الملاحة الجوية وأن ظمة اخرى حيوية لمدة ستة ساعات، وبالرغم من فداحة الضرر الذي تسبب فيه الا ان عقوبته اقتصرت على وضعه تحت الرقابة لمدة سنتين مع الزامه باداء خدمة للمجتمع لمدة (٢٥٠) يوما .(Wilson,2000)

وبهذا فان القانون الامريكي يلعب دورا غير مباشر في تشجيع المراهقين على اعمال التسلل حيث نادرا ما يعاقب المتسللين دون سن الثامنة عشر، كما يسأهم اولياء امور المراهقين في ذلك ايضا حيث يعتبرون ابنائهم اذكياء اذا مارسوا انشطة حاسوبية تتعلق بالتسلل إلى اجهزة الاخرين .(Koerner,1999)

ولا يلقي مستخدمي الإنترنت من طلبة الجامعات الامريكية أي اهتمام للعقوبات التى قد يطبقها القانون بحق من يسيئ استخدام الإنترنت ، واوضحت دراسة اجريت عام (١٩٧٩م) على عدد (٥٨١) طالب جامعي ان (٥٠٪) منهم قد اشترك في اعمال

غير نظامية اثناء استخدام الإنترنت خلال ذلك العام، وأن (٤٧) طالبا أو مانسبته (٧,٣٪) سبق وقبض عليه في جرائم تتعلق بالحاسب الآلي، وأن (٧٥) طالبا أو مانسبته (١٣,٣٪) قبض على اصدقائهم في جرائم تتعلق بالحاسب الآلي (Skinner & Fream, 1997).

فالعقوبات الحالية لاتساعد على تقليص الارتفاع المستمر للجرائم المتعلقة بالحاسب الآلي، ففي خلال عام واحد تضاغفت تلك الجرائم على مستوى الولايات المتحدة الامريكية ففي عام (١٩٩٩م) تحرت وكالة المباحث الفدرالية (FBI) عن (٨٠٠ (حالة تتعلق بالتسلل (Hacking)وهو ضعف عدد الحوادث التى قامت بالتحرى عنها في العام السابق أي عام (١٩٩٨م)، أما الهجوم على الشبكات الحاسب الآلية على الإنترنت فقد تضاعف (٣٠٠٪) في ذلك العام ايضا.(Koerner,1999)

وللحد من تزايد عمليات التسلل (Hacking)ونظرا لان المتسللين عادة يطورون تقنياتهم بصفة مستمرة ويملكون مهارات متقدمة، فقد اضطر ذلك ان يلجأ مسئولوا أمن الحاسبات الآلية وشبكات الإنترنت وكذلك رجال الامن على الاستعانة بخبرات بعض محترفين التسلل ليستطيعوا تطوير نظم الحماية ضد المتسللين(Hackers) ، وعلى سبيل المثال يرسل مسئولي امن الحاسبات اسئلة تتعلق باحدث سبل الحماية لغرف الدردشة الخاصة بمواقع المتسللين أو ما تعرف باسم (hacker internet chat room)ولطلب نصائح تقنية حول أحدث سبل الحماية (Staff, 2000, February 17) .

بل ان وكالة المباحث الفدرالية (FBI) استعانت ايضا بخبراء في التسلل (Hackers)لتدريب منسوبي الوكالة على طرق التسلل (Hacking) لتنمية خبراتهم وقدراتهم في هذا المجال وليستطيعوا مواكبة خبرات وقدرات المتخصصين من المتسللين(Hackers) ، ومنهم أحد أشهر المتسللين (Hackers) ويدعى (Brian Martin)والمشهور باسم (Jericho) وهو متهم حاليا بالتسلل والعبث بمجتويات الصفحة الرئيسية لصحيفة (New Youk Times) على شبكة الإنترنت(Staff, 2000 April 2)

واكدت المباحث السرية الامريكية (The US Secret Service) ان الجرائم المنظمة تتجه نحو استغلال التسلل (Hacking)للحصول على المعلومات اللازمة لتنفيذ مخططاتها الاجرامية (Thomas,2000) .

واوضح خبر نشر في موقع ارابيا بتاريخ ٢٠٠١/٦/١٠م من ان صحيفة لوس انجلوس تايمز ذكرت بان متسللين اقتحموا في اليوم السابق نظام الحاسب الآلي الذي يتحكم في تدفق اغلب الكهرباء في مختلف انحاء ولاية كاليفورنيا، وبالرغم من ان الهجوم كان محدودا الا انه كشف عن ثغرات امنية في نظام الحاسب الآلي لشركة الكهرباء. (موقع ارابيا،٢٠٠١/٦/١٠م(

كيف يصل حصان طروادة إلى الجهاز:

لتتم عملية الاقتحام يجب زرع حصان طروادة في جهاز الضحية بعدة طرق منها:

1. يرسل عن طريق البريد الإلكتروني كملف ملحق حيث يقوم الشخص بإستقباله

وتشغيله وقد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى.
.2عند استخدام برنامج المحادثة الشهير (ICQ) وهو برنامج محادثة انتجة اسرائيل.
.3عند تحميل برنامج من أحد المواقع غير الموثوق بها وهي كثيرة جدا.
.4طريقة أخرى لتحميله تتلخص في مجرد كتابة كوده على الجهاز نفسه في دقائق معدودة
.5في حالة اتصال الجهازبشبكة داخلية أو شبكة إنترانت .
.6يمكن نقل الملف أيضا بواسطة برنامج (FTP)أو (Telnet) الخاصة بنقل الملفات .
.7كما يمكن الاصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكروز الموجود في برامج معالجة النصوص(Nanoart,2000) .

خطورة برامج حصان طروادة:
بداية كان تصميم هذه البرامج لأهداف نبيلة كمعرفة ما يقوم به الأبناء أو الموظفون على جهاز الحاسب في غياب الوالدين أو المدراء وذلك من خلال ما يكتبونه على لوحة المفاتيح، الا انه سرعان ما اسيئ استخدامه. وتعد هذه البرامج من أخطر البرامج المستخدمه من قبل المتسللين وذلك يرجع إلى أنه يتيح للدخيل الحصول على كلمات المرور (passwords)وبالتالي الهيمنه على الحاسب الآلي بالكامل. كما أن المتسلل لن يتم معرفته أو ملاحظته كونه يستخدم الطرق المشروعة التي يستخدمها مالك الجهاز. كما تكمن الخطورة ايضا في أن معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات اضافة إلى أن الطبيعة الساكنة لحصان طروادة يجعلها اخطر من الفيروسات فهي لا تقوم بتقديم نفسها للضحية مثلما يقوم الفيروس الذي دائما ما يمكن ملاحظته من خلال الإزعاج أو الأضرار التي يقوم بها للمستخدم وبالتالي فإنه لا يمكن الشعور بهذه الاحصنة أثناء أدائها لمهمتها التجسسية وبالتالي فإن فرص إكتشافها والقبض عليها تكاد تكون معدومه.(Nanoart,2000)
كيف يتم الإختراق؟
برامج القرصنه تعتمد كليا على بروتوكول الـ TCP/IP)) وهناك ادوات (ActiveX)مصممه وجاهزة لخدمة التعامل بهذا البروتوكول ومن اشهرها (WINSOCK.OCX)لمبرمجي لغات البرمجة الداعمة للتعامل مع هذه الادوات .ويحتاج الامر إلى برنامجين، خادم في جهاز الضحية وعميل في جهاز المتسلل حيث يقوم الخادم بفتح منفذ في الجهاز الضحية ويكون هذا المنفذ معروف من قبل العميل اصلا في حين يكون برنامج الخادم في حالة انتظار لحظة محاولة دخول المخترق لجهاز الضحية حيث يتعرف برنامج الخادم (server) على اشارات البرنامج المخترق ويتم الاتصال ومن ثم يتم عرض محتويات جهاز الضحية كاملة لدى المخترق حيث يتمكن من العبث بها أو الاستيلاء على ما يريد

منها .
فالمنافذ أو ما يسمى بالبورتات (Ports) يمكن وصفها ببوابات للجهاز وهناك عدد من المنافذ في كل جهاز ولكل منها غرض محدد ، فمثلا المنفذ (٨٠٨٠ (يكون احيانا مخصص لمزود الخدمة، وقد يعتقد البعض أن هذا المنفذ مادي مثل منفذ الطابعة ،الا انه ليس كذلك فهو منفذ غير مادي ويعتبر جزء من الذاكرة له عنوأن معين يتعرف عليه الجهاز بأنه منطقة يتم إرسال واستقبال البيانات عليها، ويمكن إستخدام عدد كبير من المنافذ للإتصال وهناك ما يقارب الـ(٦٥٠٠٠) منفذ تقريبا ، يميز كل منفذ عن الآخر برقم خاص وكل ما يقوم به المتسلل هو فتح احد هذه المنافذ حتى يستطيع الوصول لجهاز الضحية وهوما يسمى بطريقة الزبون/الخادم ((Client\Serverحيث يتم ارسال ملف لجهاز الضحية يفتح المنافذ فيصبح جهاز الضحية (server) وجهاز المتسلل (Client) و من ثم يقوم المستلل بالوصول لهذه المنافذ باستخدام برامج كثيرة متخصصة كبرنامج NetBus)) أو .NetSphere))ولعل الخطورة الاضافية تكمن في انه عند دخول المتسلل إلى جهاز الضحية فانه لن يكون الشخص الوحيد الذي يستطيع الدخول لذلك الجهاز حيث يصبح ذلك الجهاز مركزا عاما يمكن لأي شخص الدخول عليه بمجرد عمل مسح للمنافذ
(Portscanning)عن طريق احد البرامج المتخصصة في ذلك.
أهم المنافذ المستخدمة :
اذن فأهم مورد لهذه الاحصنة هي المنافذ (البورتات) التي يقوم بفتحها في جهاز الضحية ومن ثم التسلل منها إلى الجهاز والعبث بمحتوياته . فما هي هذه البورتات أو المنافذ ؟ سنحاول هنا التطرق بشكل اجمالي إلى أهم المنافذ التي يمكن استخدامها من قبل المتسللين والبرامج المستخدمة في النفاذ من هذه المنافذ :

المنفذ	إسم البرنامج
21	blade Runner , doly Trojan ,FTP trojan , Invisible FTP , Larva ,WebEX , Win Crash
23	Tiny Telnet Server
25	Antigen , Email Password Sender , Haebu Coceda , Kauang 2 , Pro Mail trojan , Shtrilitz , Stealth , Tapiras ,Terminator , Win Pc ,Win Spy ,Kuang20.17A-0.30
31	Agent 31 , Hackers Paradise , Master Paradise
41	Deep Throat
58	DMSetup
79	Fire hotcker
80	Executor

110	Pro Mail trojan
121	Jammer Killah
421	TCP wrappers
456	Hackers Paradise
531	Rasmin
555	Ini Killer , Phase Zero , Stealth Spy
666	Attack FTP ,Satanz BackDoor
911	Dark Shadow
999	Deep Throat
1001	Silencer , WEBEX
1011 1012	Doly Trojan
1024	Net Spy
1045	Rasmin
1090	Xtreme
1095 1097 1098 1099	Rat
1170	Psyber Stream Server , Voice
1234	Ultors Trojan
1243	Back Door -G , SubSeven
1245	VooDoo Doll
1349	UPD - BO DLL
1492	FTP99CMP
1600	Shivka - Burka
1807	Spy Sender
1981	Shockrave
1999	Back Door
2001	Trojan Cow
2023	Ripper
2115	Bugs

2140	Deep Throat , The Invasor
2565	Striker
2583	Win Crash
2801	Phineas Phucker
3024	Win crash
3129	Master Paradise
3150	Deep Throat , The Invasor
3700	Portal Of Doom
4092	Win crash
4567	File Nail
4590	ICQ Trojan
5000	Bubbel , Back Door Setup , Sockets de troie
5001	Back Door Setup , Sockets de troie
5321	Fire hotcker
5400 5401 5402	Blade Runner
5555	ServeMe
5556 5557	Bo Facil
5569	Robo-Hack
5742	Win Crash
6400	The Thing
6670	Deep Throat
6711	SubSeven
6771	Deep Throat
6776	Back Door-G , SubSeven
6939	Indoctrination
6969	Gate Crasher , Priority
7300 7301 7306	Net Monitor

7307 7308	
7000	Remote Grab
7789	BacK Door Setup , ICKiller
9872 9873 9874 9875 10067 10167	Portal of Doom
9989	iNi - Killer
10520	Acid Shivers
10607	Coma
11000	Senna Spy
11223	Progenic trojan
12223	Hack 99 Key Logger
12345	, Pie Bill Gates , X -billNet busGaban Bus ,
12346	, X-billNet BusGaban Bus ,
12361 12362	Whack - a - mole
12631	WhackJob
13000	Senna Spy
16969	Priority
20001	Millennium
20034	NetBus 2 Pro
21544	Girl Friend
22222	Prosiak
23456	Evil Ftp , Ugly FTP
26274	UPD - Delta Source
29891	UPD - The Unexplained
30029	AOL Trojan
30100	NetSphere

30101 30102	
30303	Sockets de Troie
31337	Baron Night , BO client ,Bo2 , Bo Facil UPD - BackFire , Back Orifice , DeppBo
31338 31339	NetSpy DK
31338	UPD - Back Orific , Deep BO
31666	Bo Whack
33333	Prosiak
34324	Big Gluck , TN
40412	The Spy
40421	Agent 40421 , Master Paradise
40422 40423 40426	Master Paradise
47262	UPD -Delta Source
50505	Sockets de Troie
50766	Fore
53001	Remote Windows Shutdown
54321	School Bus
60000	Deep Throat
61466	Telecommando
65000	Devil

مصدر الجدول موقع
(http://www.nanoart.f2s.com/hack/ports3.htm)

مراجع الدراسة

ابن منظور، أبو الفضل جمال الدين محمد بن مكرم (بدون). لسان العرب . بيروت: دار صادر.

أبوزهرة، محمد (١٩٧٦م). الجريمة والعقوبة في الفقه الإسلامي. القاهرة: دار الفكر العربي.

أحمد، هلالي عبدالاه (٢٠٠٠م). تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي. عابدين : النسر الذهبي للطباعة.

بحر، عبدالرحمن محمد (١٤٢٠هـ). معوقات التحقيق في جرائم الإنترنت : دراسة مسحية على ضباط الشرطة في دولة البحرين. رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.
البداينة، ذياب (١٤٢٠هـ). جرائم الحاسب والإنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (٩٣-١٢٤).
البداينة، ذياب (١٩٩٩م). التطبيقات الاجتماعية للإنترنت، ورقة قُدّمت في الدورة التدريبية حول شبكة الإنترنت من منظور أمنى، أكاديمية نايف العربية للعلوم الأمنية، بيروت، لبنان.
تمّام، أحمد حسام طه (٢٠٠٠م). الجرائم الناشئة عن استخدام الحاسب الآلي. القاهرة : دار النهضة العربية.
داود، حسن طاهر (١٤٢١هـ). الحاسب وامن المعلومات. الرياض: معهد الإدارة العامة.
داود، حسن طاهر (١٤٢٠هـ). جرائم نظم المعلومات. الرياض : أكاديمية نايف العربية للعلوم الأمنية.
السيف، محمد إبراهيم (١٤١٧هـ). الظاهرة الإجرامية في ثقافة وبناء المجتمع السعودي : بين التصور الاجتماعي وحقائق الاتجاه الإسلامي. الرياض : مكتبة العبيكان.
شتا، محمد محمد (٢٠٠١م). فكرة الحماية الجنائية لبرامج الحاسب الآلي. الإسكندرية: دار الجامعة الجديدة للنشر.
الشنيفي، عبدالرحمن عبدالعزيز (١٤١٤هـ). أمن المعلومات وجرائم الحاسب الآلي. (ط١) الرياض : بدون.
الشهاوي، قدري عبدالفتاح (١٩٩٩م). أساليب البحث العلمي الجنائي والتقنية المتقدمة. الإسكندرية :منشأة المعارف.
الشهري، عبدالله محمد صالح (١٤٢٢هـ). المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي : دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض، المملكة العربية السعودية.
الشهري، فايز عبدالله (١٤٢٢هـ). استخدامات شبكة الإنترنت في مجال الإعلام الأمني العربي. مجلة البحوث الأمنية ، ١٠(١٩)، ١٦٥-٢١٤.
صحيفة عكاظ، العدد ١٢٧٨٩، ١٤٢٢/٦/١٣هـ، الصفحة الأولى.
طالب، أحسن (١٩٩٨م). الجريمة والعقوبة والمؤسسات الإصلاحية. الرياض : دار الزهراء.
عجب نور، أسامة محمد (١٤١٧هـ). جريمة الرشوة في النظام السعودي. الرياض : معهد الإدارة العامة.
عودة، عبدالقادر (١٤٠١هـ). التشريع الجنائي الإسلامي. بيروت : مؤسسة الرسالة، (المجلد الأول).

عيد، محمد فتحي (١٤١٩هـ). الإجرام المعاصر. الرياض : أكاديمية نايف العربية للعلوم الأمنية.
الماوردي، محمد حبيب (١٤٠٧هـ). الأحكام السلطانية. القاهرة : دار التراث العربي.
محمد، عادل ريان (١٩٩٥م)، جرائم الحاسب الآلي وأمن البيانات، العربي ، (٤٤٠)، ٧٣ – ٧٧ .
مندورة، محمد محمود (١٤١٠هـ). جرائم الحاسب الآلية، دورة فيروس الحاسب الآلي، مكتب الأفاق المتحدة : الرياض ، ١٩ – ٢٦.
موقع صحيفة الجزيرة - القرية الإلكترونية (١٤٢١/٢/٢)
http://www.al-jazirah.com/2000/may/6/ev.htm#evt3
موقع بوابة عجيب (٢٠٠١/٨/٨م)
http://it.ajeeb.com/viewarticle.asp?article=1976&category=17
موقع صحيفة البيان (٢٠٠٠/٥/١٩)
http://www.albayan.co.ae/albayan/2000/05/19/mhl/2.htm
موقع مجلة الأمن الإلكترونية (١٤٢١/٧/٢٢هـ)
http://safola.com/security.chtml
موقع وحدة خدمات الإنترنت(١٤٢٣/٢/٨هـ)http://www.isu.net.sa/ar/faqs.html
نشرة تعريفية عن مدينة الملك عبدالعزيز للعلوم والتقنية (١٤١٩هـ). الرياض: الإدارة العامة للتوعية العلمية والنشر.

النيسابوري، أبي الحسين مسلم بن الحجاج القشيري (١٣٧٥هـ). صحيح مسلم. (ط١)، (بدون): دار إحياء التراث العربي.

الهاشمي، عبدالحميد محمد (١٩٨٦م). علم النفس التكويني: أسسه وتطبيقه من الولادة إلى الشيخوخة، (الطبعة الثانية). القاهرة: مكتبة الخانجي.

اليامي، محمد (١٩٩٨م). رجال الأعمال ينطلقون إلى الاستفادة من فرص التجارة الإلكترونية. الحياة ، الملحق ، (٩٤- ١٢٩).

اليوسف، عبدالله عبدالعزيز (١٤٢٠هـ). التقنية والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (١٩٥- ٢٣٣).

ثانيا: المراجع الأجنبية :

Rapalus, P.(2000,May). Ninety percent of survey respondents detect cyber attacks. Computer Security Institute. [Online]. Available: [11.10.2001].http://www.gocsi.com/prelen_000321.htm

Reuvid, Jonathan. (1998). The Regulation and Prevention of Economic Crime, London: Kogan, 14.

Thompson, R. (1999, February). Chasing after petty computer crime. IEEE Potentials, 18 (1), 20-22.

Vacca, John. (1996). Internet Security Secrets.USA:IDG Book. Worldwide Inc.

جرائم الانترنت
من منظور شرعي وقانوني

محمد عبدالله منشاوي باحث في جرائم الانترنت

مقدمة - تعريف الإنترنت وبداياته واستخداماته:

"الإنترنت هو جزء من ثورة الاتصالات، ويعرّف البعض الإنترنت بشبكة الشبكات، في حين يعرّفها البعض الآخر بأنها شبكة طرق المواصلات السريعة" (أبو الحجاج، ١٩٩٨م : ١٨)، كما أن الإنترنت " تعنى لغوياً ((ترابط بين شبكات)) وبعبارة أخرى ((شبكة الشبكات)) حيث تتكون الإنترنت من عدد كبير من شبكات الحاسب المترابطة والمتناثرة في أنحاء كثيرة من العالم. ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى ((بروتوكول تراسل الإنترنت)) (TCP/IP)"(الفنتوخ، ١٤٢١هـ:١١).
بدأ الإنترنت في ١٩٦٩/١/٢ عندما شكّلتْ وزارة الدفاع الأمريكية، فريقاً من العلماء، للقيام بمشروع بحثي عن تشبيك الحاسبات، وركّزت التجارب على تجزئة الرسالة المراد بعثها إلى موقع معين في الشبكة، ومن ثم نقل هذه الأجزاء بأشكال وطرق مستقلة، حتى تصل مجّمعة إلى هدفها، وكان هذا الأمر يمثل أهمية قصوى لأمريكا وقت الحرب، ففي حالة نجاح العدو في تدمير بعض خطوط الاتصال في منطقة معينة، فإن الأجزاء الصغيرة يمكن أن تواصل سيرها من تلقاء نفسها، عن أي طريق آخر بديل، إلى خط النهاية، ومن ثم تطّور المشروع وتحوّل إلى الاستعمال السلمي حيث انقسم عام (١٩٨٣م) إلى شبكتين، احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) وبغرضها الأساسي، وهو خدمة الاستخدامات العسكرية، في حين سُمِّيتْ الشبكة الثانية باسم (MILNET) وخصصت للاستخدامات المدنية ،أي تبادل المعلومات، وتوصيل البريد الإلكتروني، ومن ثم ظهر مصطلح ((الإنترنت)) حيث أمكن تبادل المعلومات بين هاتين الشبكتين. وفي عام (١٩٨٦م) أمكن ربط شبكات خمس مراكز للكمبيوترات العملاقة وأطلق عليها اسم (NSFNET) والتي أصبحت فيما بعد العمود الفقري، وحجر الأساس، لنمو وازدهار الإنترنت في أمريكا، ومن ثم دول العالم الأخرى(الفنتوخ،١٤٢١هـ: ٢١- ٢٤).

من يملك الإنترنت؟
لا أحد في الوقت الراهن يملك الإنترنت، وإن كان يمكن القول في البداية بأنّ الحكومة الأمريكية ،ممثلة في وزارة الدفاع، ثم المؤسسة القومية للعلوم، هي المالك الوحيد للشبكة، ولكن بعد تطّور الشبكة، ونمّوها، لم يعد يملكها أحد، واختفى مفهوم التملك، ليحل محله ما أصبح يسمي بمجتمع الإنترنت، كما أنّ تمويل الشبكة تحول من القطاع الحكومي، إلى القطاع الخاص. ومن هنا ولدت العديد من الشبكات الإقليمية ،ذات الصبغة التجارية، والتى يمكن الاستفادة من خدماتها مقابل اشتراك (أبو الحجاج، ١٩٩٨م : ١٨).

وهذه الخصوصية أي عدم وجود مالك محدد أو معروف للانترنت يجعل مهمة رجال الأمن أكثر صعوبة (Thompson, 1999).

توسع الشبكة:

في عام (١٩٨٥م) كان هناك أقلّ من (٢,٠٠٠) ألفي حاسوب آلي مرتبط بالشبكة، ووصل العدد إلى (٥,٠٠٠,٠٠٠) خمسة مليون حاسوب في عام (١٩٩٥م) وفي عام (١٩٩٧م) تجاوز (٦,٠٠٠,٠٠٠) الستة مليون حاسوب، وتستخدم ما يزيد علي (٣٠٠,٠٠٠) ثلاثمائة ألف خادم شبكات (SERVER) ،أي شبكة فرعية، متناثرة في أرجاء العالم, ويمكن القول بأن عدد المستخدمين الجدد يبلغ (٢,٠٠٠,٠٠٠) إثني مليون شهرياً، أي ما يعني انضمام (٤٦) ستة وأربعين مستخدماً جديداً للشبكة في كل دقيقة (السيد،١٩٩٧م : ١٥).

وفي استطلاع أجرته شبكة (NUA) الأمريكية (NUA, 1998) قدّر عدد مستخدمي الشبكة عالمياً في العام (١٩٩٨م) بحوالي (١٣٤,٠٠٠,٠٠٠) مئة وأربعة وثلاثين مليون مستخدم، وتصدرت أمريكا وكندا الصدارة من حيث عدد المستخدمين الذي بلغ (٧٠,٠٠٠,٠٠٠) سبعون مليون مستخدم (NUA ,6/1998).

وفي تقرير أجرته ايضاً شبكة (NUA) الأمريكية وصدر بتاريخ ٢٠٠٠/١٠/٢٦م (NUA, 2000) قدّر أن عدد المستخدمين للشبكة عام (٢٠٠٥م) سيكون حوالي (٢٤٥,٠٠٠,٠٠٠) مئتان وخمسة وأربعون مليون مستخدم، وقدّر أنّ غالبية هذه الزيادة ستكون خارج الولايات المتحدة الأمريكية (NUA ,10/2000).

وقدّرت دراسة أجراها موقع عجيب (Ajeeb.com,25/3/2001) تجاوز عدد المستخدمين العرب الـ(٥,٠٠٠,٠٠٠) الخمسة ملايين مستخدم مع نهاية عام (٢٠٠١م)، وأن يصل العدد إلى (١٢,٠٠٠,٠٠٠) اثني عشر مليون مستخدم عربي مع نهاية عام (٢٠٠٢م)، كما قدرت الدراسة عدد مستخدمي الإنترنت في المملكة العربية السعودية بـ(٥٧٠,٠٠٠) خمسائة وسبعون ألف مستخدم.

وأشار الرئيس الأمريكي السابق بيل كلينتون إلى مشروع مستقبلي، لتطوير شبكة الإنترنت، باسم (الإنترنت ٢) أو الجيل الثاني من الإنترنت فقال: " لا بُدّ من أنْ نبني الجيل الثاني لشبكة الإنترنت لتتاح الفرصة لجامعاتنا الرائدة ومختبراتنا القومية للتواصل بسرعة تزيد ألف مرة من سرعات اليوم، وذلك لتطوير كل من العلاجات الطبية الحديثة ومصادر الطاقة الجديدة، وأساليب العمل الجماعي" (آفاق الإنترنت، ١٩٩٧م : ٣٨).

وظهر حديثاً ما يشير في هذه الأيام إلى وجود سباق فضاء من نوع آخر، حيث استطاعت شركة ستارباند (Star band) في تجربه أجرتها في شمال أميركا، من إكمال مشروع انترنت بواسطة أقمار اصطناعية ذي اتجاهين، وسرعته تبلغ (٥٠٠) خمسمائة ك.ب في الثانية، من الإنترنت إلى الحاسب الآلي، وسيبدأ تسويقه إلى المستهلك قريباً (الجزيرة،٢٠٠٠).

خدمات الإنترنت :

يوفر الإنترنت خدمات عديدة من أهمها:

١. البريد الإلكتروني: لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص له عنوان بريدي اليكتروني بصورة سريعة جداً لا تتعدى ثواني.
٢. القوائم البريدية: تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعات من الأشخاص لهم اهتمامات مشتركة.
٣. خدمة المجموعات الإخبارية: تشبه خدمة القوائم البريدية باختلاف أن كل عضو يستطيع التحكم في نوع المقالات التي يريد استلامها.
٤. خدمة الاستعلام الشخصي: يمكن الاستعلام عن العنوان البريدي لأي شخص أو جهة تستخدم الإنترنت والمسجلين لديها.
٥. خدمة المحادثات الشخصية: يمكن التحدث مع طرف آخر صوتا وصورة وكتابة.

٦. خدمة الدردشة الجماعية: تشبه الخدمة السابقة إلا انه ،وفي الغالب، يمكن لأي شخص ان يدخل في المحادثة ،أو يستمع اليها، دون اختيار الآخرين.
٧. خدمة تحويل أو نقل الملفات: (FTP) لنقل الملفات من حاسب إلى آخر وهي اختصار كلمة (FILE TRANSFER PROTOCOL).
٨. خدمة الأرشيف الإلكتروني: (ARCHIVE) تُمكّن البحث عن ملفات معينة قد تكون مفقودة في البرامج المستخدمة في حاسب المستخدم.
٩. خدمة شبكة الاستعلامات الشاملة: (GOPHER) تفيد في خدمات كثيرة كنقل الملفات والمشاركة في القوائم البريدية حيث يفهرس المعلومات الموجودة علي الشبكة.
١٠. خدمة الاستعلامات واسعة النطاق: (WAIS) تسمي باسم حاسباتها الخادمة وهي أكثر دقة وفاعلية من الأنظمة الاخرى، حيث تبحث داخل الوثائق أو المستندات ذاتها عن الكلمات الدالة التي يحددها المستخدم ثم تقدم النتائج في شكل قائمة بالمواقع التي تحتوي المعلومات المطلوبة.
١١. خدمة الدخول عن بعد: (TELNET) تسمح باستخدام برامج وتطبيقات في حاسب آلي آخر.
١٢. الصفحة الإعلامية العالمية:(WORLD WIDE WEB) أو الويب (WEB) تجمع معاً كافة الموارد المتعددة التي تحتوي عليها الإنترنت للبحث عن كل ما في الشبكات المختلفة وإحضارها بالنص والصوت والصورة، وتعد الويب نظاماً فرعياً من الإنترنت، لكنها النظام الأعظم من الأنظمة الأخرى فهي النظام الشامل باستخدام الوسائط المتعددة (يونس، ١٤٢١هـ : ٣٤-٣٨).

مستلزمات الاتصال بالشبكة:
يلزم الاتصال بالشبكة العالمية (الإنترنت) توفر عدة أشياء هي :
١. حاسب إلى.
٢. جهاز مودم.
٣. خط هاتفي.
٤. الاشتراك في الخدمة.
٥. برامج تصفح الشبكة واشهرها (INTERNET EXPLORER) و (NETSCAPE)

وبعد هذه النبذة عن تاريخ الإنترنت واستخداماته، نعرض فيما يلي مباحث نظرية رئيسة تنطلق منها الدراسة، وهذه المباحث هي:
المبحث الاول: جرائم الحاسب الآلي والإنترنت.
المبحث الثاني: جرائم الإنترنت من منظور شرعي وقانوني.
المبحث الثالث: الأبعاد الفنية للأفعال الجنائية المرتكبة من قبل مستخدمي الإنترنت في المجتمع السعودي (تصور إسلامي
المبحث الأول: جرائم الحاسب الآلي والإنترنت

أُشْتُقّتْ كلمة الجريمة في اللغة من الجُرم وهو التعدي أو الذنب، وجمع الكلمة إجرام وجروم وهو الجريمة. وقد جَرَمَ يَجْرِمُ واجْتَرَمَ وأَجْرَم فهو مجرم وجريم (ابن منظور، بدون : ٦٠٤ – ٦٠٥).
وعَرَّفت الشريعة الإسلامية الجريمة بأنها: " محظورات شرعية زجر الله عنها بحد أو تعزير" (الماوردي، ١٤١٧هـ : ١٩).

وتعرّف جرائم الحاسب الآلي والإنترنت بأنها:" ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها "(مندورة،١٤١٠هـ : ٢١).
كما يمكن تعريفها بأنها " الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني " (محمد ، ١٩٩٥م : ٧٣).
وهناك من عرّفها بأنها " أي عمل غير قانوني يستخدم فيه الحاسب كأداة، أو موضوع للجريمة" (البداينة، ١٤٢٠هـ : ١٠٢).
وفي كل الأحوال فجريمة الحاسب الآلي " لا تعترف بالحدود بين الدول ولا حتى بين القارات،فهي جريمة تقع في أغلب الأحيان عبر حدود دولية كثيرة "(عيد، ١٤١٩هـ: ٢٥٢).
وتعد جريمة الإنترنت من الجرائم الحديثة التي تُستخدم فيها شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها (Vacca , 1996).
وأطلق مصطلح جرائم الإنترنت (Internet Crimes) في مؤتمر جرائم الإنترنت المنعقد في استراليا للفترة من ١٦ – ١٩٩٨/٢/١٧م (بحر، ١٤٢٠هـ : ٢).

أما التعريف الإجرائي لدراسة الباحث فتُعَرَّفُ جرائم الإنترنت بأنها : جميع الأفعال المخالفة للشريعة الإسلامية، وأنظمة المملكة العربية السعودية، المرتكبة بواسطة الحاسب الآلي، من خلال شبكة الإنترنت، ويشمل ذلك: الجرائم الجنسية والممارسات غير الأخلاقية، جرائم الاختراقات، الجرائم المالية، جرائم إنشاء أو ارتياد المواقع المعادية، جرائم القرصنة.
وبالرغم من حداثة جرائم الحاسب الآلي والإنترنت نسبياً، إلا أنها لقيتْ اهتماماً من قبل بعض الباحثين، حيث أُجريتْ العديد من الدراسات المختلفة، لمحاولة فهم هذه الظاهرة، ومن ثم التحكم فيها، ومنها دراسة أجرتها منظمة (Alliance Business Software) في الشرق الأوسط، حيث أظهرت أنّ هناك تباين بين دول منطقة الشرق الأوسط، في حجم خسائر جرائم الحاسب الآلي، حيث تراوحت ما بين (٣٠,٠٠٠,٠٠٠) ثلاثين مليون دولار أمريكي في المملكة العربية السعودية، والإمارات العربية المتحدة، و (١,٤٠٠,٠٠٠) مليون وأربعمائة ألف دولار أمريكي في لبنان (البداينة، ١٤٢٠هـ : ٩٨).
وأظهرت دراسة قامت بها الأمم المتحدة حول جرائم الحاسب الآلي والإنترنت بأنّ (٢٤–٤٢٪) من منظمات القطاع الخاص، والعام، على حد سواء، كانت ضحية لجرائم متعلقة بالحاسب الآلي والإنترنت (البداينة، ١٩٩٩م : ٥).
وقدّرتْ الولايات المتحدة الأمريكية خسائرها من جرائم الحاسب الآلي، مابين ثلاثة وخمسة بلايين دولار سنوياً، كما قدّرتْ المباحث الفيدرالية (FBI)، في نهاية الثمانينات الميلادية، أنّ متوسط تكلفة جريمة الحاسب الآلي الواحدة، حوالي ستمئة ألف دولار سنوياً، مقارنة بمبلغ ثلاثة آلاف دولار سنوياً ،متوسط الجريمة الواحدة، من جرائم السرقة بالإكراه. وبينت دراسة أجراها أحد مكاتب المحاسبة الأمريكية أن (٢٤٠) مئتين وأربعين شركة أمريكية، تضررت من جرائم الغش باستخدام الكمبيوتر (Computer Fraud)، كما بينت دراسة أخرى أُجريتْ في بريطانيا، أنه وحتى أواخر الثمانينات، ارتكب ما يقرب من (٢٦٢) مائتين واثنين وستين جريمة حاسوبية، وقد كلفت هذه الجرائم حوالي (٩٢,٠٠٠,٠٠٠) اثنين وتسعين مليون جنيه إسترليني سنوياً (محمد ، ١٩٩٥م : ٢١).
وأظهر مسح أُجري من قبل (the computer security institute) في عام (١٩٩٩م)، أنّ خسائر (١٦٣) مئة وثلاثة وستون شركة أمريكية ،من الجرائم المتعلقة بالحاسب الآلي، بلغت أكثر من (١٢٣,٠٠٠,٠٠٠) مئة وثلاثة وعشرين مليون دولار أمريكي، في حين أظهر المسح الذي أُجري في عام (٢٠٠٠م) ارتفاع عدد الشركات الأمريكية المتضررة من تلك الجرائم، حيث وصل إلى (٢٧٣) مئتين وثلاث وسبعين شركة، بلغ مجموع خسائرها أكثر من (٢٥٦,٠٠٠,٠٠٠) مائتين وستة وخمسون مليون دولار(Rapalus,2000).

كما بينت إحصائيات الجمعية الأمريكية للأمن الصناعي أن الخسائر التي قد تسببها جرائم الحاسب الآلي للصناعات الأمريكية قد تصل إلى (٦٣,٠٠٠,٠٠٠,٠٠٠) ثلاث وستون بليون دولار أمريكي، وأنّ (٢٥٪) من الشركات الأمريكية تتضرر من جرائم الحاسب الآلي، وقد أصيب (٦٣٪) من الشركات الأمريكية والكندية بفيروسات حاسوبية، ووصل الفقد السنوي بسبب سوء استخدام الحاسب الآلي (٥٥٥,٠٠٠,٠٠٠) خمسائة وخمسة وخمسون مليون دولار (Reuvid,1998).

ومن الصعوبة بمكان، تحديد أيّ جرائم الحاسب الآلي المرتكبة هي الأكبر من حيث الخسائر، حيث لا يعلن الكثير عن مثل هذه الجرائم، ولكن من أكبر الجرائم المعلنة هي جريمة لوس انجلوس، حيث تعرضت أكبر شركات التأمين على الاستثمارات المالية (EFI) للإفلاس، وبلغت خسائرها (٢,٠٠٠,٠٠٠,٠٠٠) ملياري دولار أمريكي. وهناك أيضاً حادثة انهيار بنك بارينجر البريطاني في لندن، إثر مضاربات فاشلة في بورصة الأوراق المالية في طوكيو، حيث حاول البنك إخفاء الخسائر الضخمة، باستخدام حسابات وهمية، أدخلها في الحسابات الخاصة بالبنك، بمساعدة مختصين في الحاسب الآلي، وقد بلغت إجمالي الخسائر حوالي مليار ونصف دولار أمريكي (داود، ١٤٢٠هـ: ٣١).

وتعتبر هذه الخسائر بسيطة نسبيا مع الخسائر التي تسببتها جرائم نشر الفيروسات والتي تضر بالأفراد والشركات وخاصة الشركات الكبيرة حيث ينتج عنها توقف أعمال بعض تلك الشركات نتيجة إتلاف قواعد بياناتها، وقد يصل الضرر في بعض المنشئات التجارية والصناعية إلى تكبد خسائر مادية قد تصل إلى مبالغ كبيرة، وعلى سبيل المثال وصلت خسائر فيروس (Code Red) إلى ملياري دولار أمريكي، في حين وصلت الأضرار المادية لفيروس الحب الشهير (٨,٧) مليون دولار واستمر انتشار الفيروس لخمسة اشهر وظهر منه (٥٥) نوعا.

وتتراوح أضرار الفيروسات ما بين عديمة الضرر إلى البسيط الهين وقد تصل إلى تدمير محتويات كامل الجهاز، وأن كان الأكثر شيوعا هو ما يسبب ضرراً محصوراً في إتلاف البيانات التي يحتويها الجهاز (Ajeebb.com,8/8/2001).

وجرائم الإنترنت كثيرة ومتنوعة ويصعب حصرها ولكنها بصفة عامة تشمل الجرائم الجنسية كإنشاء المواقع الجنسية وجرائم الدعارة أو الدعاية للشواذ أو تجارة الأطفال جنسيا، وجرائم ترويج المخدرات أو زراعتها، وتعليم الإجرام أو إرهاب كصنع المتفجرات، إضافة إلى جرائم الفيروسات واقتحام المواقع.

وكثيراً ما تكون الجرائم التي ترتكب بواسطة الإنترنت وثيقة الصلة بمواقع أرضية على الطبيعة كما حدث منذ حوالي سنتين عندما قام البوليس البريطاني بالتعاون مع أمريكا ودول أوروبية بمهاجمة مواقع أرضية لمؤسسات تعمل في دعارة الإنترنت.

وإن كانت متابعة جرائم الحاسب الآلي والإنترنت والكشف عنها من الصعوبة بمكان حيث أن " هذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة وأن ما هي أرقام تتغير في السجلات. ومعظم جرائم الحاسب الآلي تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستر عنها"
مندورة ، ١٤١٠هـ : ٢٢).

وتعود أسباب صعوبة إثبات جرائم الحاسب الآلي إلى خمسة أمور هي :

أولا: أنها كجريمة لا تترك اثر لها بعد ارتكابها.

ثانيا: صعوبة الاحتفاظ الفني بآثارها إن وجدت.

ثالثا: أنها تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.

رابعا: أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.

خامسا: أنها تعتمد على قمة الذكاء في ارتكابها (موثق في شتا،٢٠٠١م : ١٠٣).

إلا أن أهم خطوة في مكافحة جرائم الإنترنت هي تحديد هذه الجرائم بداية ومن ثم تحديد الجهة التي يجب أن تتعامل مع هذه الجرائم والعمل على تأهيل منسوبيها بما يتناسب وطبيعة هذه

الجرائم المستجدة ويأتي بعد ذلك وضع تعليمات مكافحتها والتعامل معها والعقوبات المقترحة ومن ثم يركز على التعاون الدولي لمكافحة هذه الجرائم .
والإنترنت ليس قاصرا على السلبيات الأمنية فقط حيث يمكن أن يكون مفيدا جدا في النواحي الأمنية كأن يستخدم الإنترنت في إيصال التعاميم والتعليمات بسرعة وكذلك في إمكانية الاستفادة من قواعد البيانات المختلفة والموجودة لدى القطاعات الأخرى وتبادل المعلومات مع الجهات المعنية، ويفيد أيضا في مخاطبة الإنتربول ومحاصرة المجرمين بسرعة.
وحددت دراسة أمنية لشرطة دبي حول الاستخدامات الأمنية للانترنت عشر خدمات أمنية يمكن تقديمها للجمهور عن طريق شبكة الإنترنت، وأبرزت (١٥) سلبية أبرزها الإباحية والمعاكسات والاحتيال والتجسس والتهديد والابتزاز (البيان،٢٠٠٠م).
كما حددت دراسة الشهري الايجابيات الأمنية لشبكة الإنترنت في تلقي البلاغات، توفير السرية للمتعاونين مع الأجهزة الأمنية، طلب مساعدة الجمهور في بعض القضايا، نشر صور المطلوبين للجمهور، نشر المعلومات التي تهم الجمهور، تكوين جماعات أصدقاء الشرطة، توعية الجمهور امنيا، استقبال طلبات التوظيف، نشر اللوائح والأنظمة الجديدة، توفير الخدمة الأمنية خارج أوقات العمل الرسمي، سهولة الوصول إلى العاملين في الجهاز الأمني ، إجراء استفتاءات محايدة لقياس الرأي العام، وسيط فاعل في عملية تدريب وتثقيف منسوبي القطاع وأخيرا وسيط مهم للإطلاع على خبرات الدول المتقدمة ولاتصال مع الخبراء والمختصين في مختلف دول العالم (الشهري، فايز، ١٤٢٢هـ).
وليس الأمر قاصرا على ذلك بل بادرت الدول الأوروبية إلى الاستخدام الفعلي لشبكة الإنترنت في البحث عن المجرمين والقبض عليهم " فقد تمكنت العديد من الدول وفي مقدمتها ألمانيا وبريطانيا وتأتي في المرتبة الثالثة فرنسا من استخدام شبكة الإنترنت في السعي نحو ضبط المجرمين – بل التعرف على كل الحالات المشابهة في كل أنحاء أوروبا والاتصال فورا بالانتربول عبر شبكة الإنترنت" (الشهاوي، ١٩٩٩م : ٢٥) فئات الجناة في جرائم الحاسب الآلي :
يمكن حصر أنواع الجناة في جرائم الحاسب الآلي في أربعة فئات(محمد،١٩٩٥م :٧٤- ٧٥):
الفئة الأولي : العاملون على أجهزة الحاسب الآلي في منازلهم نظرا لسهولة اتصالهم بأجهزة الحاسب الآلي دون تقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز.
الفئة الثانية : الموظفون الساخطون على منظماتهم التي يعملون بها فيبعودون إلى مقار عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو حتى سرقته.
الفئة الثالثة : فئة المتسللين (Hackers) ومنهم الهواة أو العابثون بقصد التسلية، وهناك المحترفين اللذين يتسللون إلى أجهزة مختارة بعناية ويعبثون أو يتلفون أو يسرقون محتويات ذلك الجهاز، وتقع اغلب جرائم الإنترنت حاليا تحت هذه الفئة بقسميها.
الفئة الرابعة:العاملون في الجريمة المنظمة كعصابات سرقة السيارات حيث يحددون بواسطة الشبكة أسعار قطع الغيار ومن ثم يبيعون قطع الغيار المسروقة في الولايات الأعلى سعرا.

خصائص وأنواع جرائم الحاسب الآلي والإنترنت :
من الصعوبة الفصل بين جرائم الحاسب الآلي وجرائم الإنترنت،فلابد للأول لارتكاب الثاني، ويُصنِّف محمد ومندورة (محمد،١٩٩٥م؛ مندورة،١٤١٠هـ) تلك الجرائم إلى مجموعات:
المجموعة الأولي : تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي لاستغلالها بطريقة غير مشروعة كمن يدخل إلى إحدى الشبكات ويحصل على أرقام بطاقات ائتمان يحصل بواسطتها على مبالغ من حساب مالك البطاقة ، وما النوع من الجرائم انه من الصعوبة بمكان اكتشافه مالم يكن هناك تشابهه في بعض أسماء أصحاب هذه البطاقات.
المجموعة الثانية : تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها أو تدميرها كليا أو جزئيا ويمثل هذا النوع الفيروسات المرسلة عبر البريد الإلكتروني أو

بواسطة برنامج مسجل في احد الوسائط المتنوعة والخاصة بتسجيل برامج الحاسب الآلي ويمكن اكتشاف مثل هذه الفيروسات في معظم الحالات بواسطة برامج حماية مخصصة للبحث عن هذه الفيروسات ولكن يشترط الأمر تحديث قاعدة بيانات برامج الحماية لضمان أقصى درجة من الحماية . ومع أن وجود هذه البرامج في جهاز الحاسب الآلي لا يعنى إطلاقا الحماية التامة من أي هجوم فيروسي وأن ما هو احد سبل الوقاية والتي قد يتسلل الفيروس إلى الجهاز بالرغم من وجودها ويلحق أذى بالجهاز ومكوناته خاصة إذا كان الفيروس حديث وغير معروف من السابق .

المجموعة الثالثة :تشمل استخدام الحاسب الآلي لارتكاب جريمة ما، وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحبا على جوائز اليانصيب حيث قام احد الموظفين بالشركة بتوجيه الحاسب الآلي لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة إلى شخص بطريقة غير مشروعة[وإن كان اليانصيب غير مشروع أصلاً].

المجموعة الرابعة : تشمل إساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه ومن هذا استخدام الموظف لجهازه بعد انتهاء عمله في أمور لا تخص العمل. المبحث الثاني: جرائم الإنترنت من منظور شرعي وقانوني

" يمكن النظر للانترنت كمهدد للأمن الاجتماعي وخاصة في المجتمعات المغلقة والشرقية، حيث أن تعّرض مثل هذه المجتمعات لقيم وسلوكيات المجتمعات الأخرى قد تسبب تلوثا ثقافيا يؤدي إلى تفسخ اجتماعي وانهيار في النظام الاجتماعي العام لهذه المجتمعات. إن الاستخدام غير الأخلاقي واللاقانوني للشبكة قد يصل إلى مئات المراهقين والهواة مما يؤثر سلبا على نمو شخصياتهم النمو السليم ويوقعهم في أزمات نمو، وأزمات قيمية لا تتماشى مع النظام الاجتماعي السائد، وبخاصة عند التعامل مع المواضيع الجنسية وتقديم الصور والمواد الإباحية" (البداينة، ١٩٩٩م : ١٠١)

والمخاطر الأمنية متجددة وليست قاصرة على وقت أو نوع معين و" مع دخول الكمبيوتر (الحاسب الآلي) الذكي إلى المنازل فان ذلك سيفتح الباب لأنواع متطورة من الجرائم التي تستغل إمكانية برمجة الأجهزة المنزلية ووصلها بالحاسب الآلي وبشكبة الانترنت، فطالما انك تستطيع مثلا وصل خزانة الأموال في مكتبك بشبكة الانترنت لإعطاء إنذار عند محاولة فتحها فربنا يكون من الممكن فتحها عن بعد بواسطة الكمبيوتر (الحاسب الآلي) ثم الوصول إليها وإفراغها " (داود، ١٤٢٠هـ : ٣٢).

واستلزم التطور التقني تطور في طرق إثبات الجريمة والتعامل معها، فالجرائم العادية يسهل – غالباً - تحديد مكان ارتكابها، بل أن ذلك يعتبر خطوة أولى وأساسية لكشف ملابسات الجريمة، في حين انه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع جرائم الانترنت، لكون الرسائل والملفات الحاسوبية تنتقل من نظام إلى آخر في ثواني قليلة، كما انه لا يقف أمام تنقل الملفات والرسائل الحاسوبية أي حدود دولية أو جغرافية. ونتيجة لذلك فإن تحديد أين تكون المحاكمة وما هي القوانين التي تخضع لها أمر في غاية الحساسية والتعقيد خاصة وان كل دولة تختلف قوانينها عن الدولة الأخرى، فما يعتبر جريمة في الصين مثلا قد لا يعتبر جريمة في أمريكا والعكس صحيح، بل أن الأمر يصل إلى حد اختلاف قوانين الولايات المختلفة داخل الدولة الواحدة كما في الولايات المتحدة الأمريكية (Thompson, 1999).

وأدى التطور التقني إلى ظهور جرائم جديدة لم يتناولها القانون الجنائي التقليدي، مما اجمع معه مشرعي القانون الوضعي في الدول المتقدمة على جسامة الجريمة المعلوماتية والتهديدات التي يمكن أن تنشأ عن استخدام الحاسب الآلي وشبكة الإنترنت، ودفعهم هذا إلى دراسة هذه الظاهرة الإجرامية الجديدة وما اثارته من مشكلات قانونية حول تطبيق القانون الجنائي من حيث الاختصاص القضائي ومكان وزمان ارتكاب الجريمة حيث يسهل على المجرم في مثل هذه

الجرائم ارتكاب جريمة ما في مكان غير المكان الذي يتواجد فيه أو الذي حدثت فيه نتائج فعله (تمام، ٢٠٠٠م : ١- ٣).
وتطوير القوانيين الجنائية وتحديثها امر يستغرق بعض الوقت فـ" هناك تعديلات كثيرة مطلوب ادخالها على التشريعات التي تتعامل مع الجريمة كي تأخذ في الاعتبار المعطيات الجديدة التي نشأت عن إستخدام الحاسب الآلي في مجال المعلومات وعن ظهور شبكات المعلومات العالمية" (داود، ١٤٢١هـ : ٦٨).
ولاقت جرائم الحاسب الآلي اهتماما عالميا فعقدت المؤتمرات والندوات المختلفة ومن ذلك المؤتمر السادس للجمعية المصرية للقانون الجنائي عام (١٩٩٣م) الذي تناول موضوع جرائم الحاسب الآلي والجرائم الأخرى في مجال تكنلوجيا المعلومات وتوصل الي توصيات احاطت بجوانب مشكلة جرائم الحاسب الآلي الا انها لم تتعرض لجزئية هامة وهي التعاون الدولي الذي يعتبر ركيزة اساسية عند التعامل مع هذه النوعية من الجرائم (عيد، ١٤١٩هـ:٥٦ ــ ٢٥٩).
وهذا المؤتمريعتبر تحضيرا للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في البرازيل عام (١٩٩٤م) والذي وضع توصيات حول جرائم الحاسب الآلي والانترنت والتحقيق فيها ومراقبتها وضبطها وركز على ضرورة ادخال بعض التعديلات في القوانين الجنائية لتواكب مستجدات هذه الجريمة وافرازاتها (احمد،٢٠٠٠م : ٥ ــ ١٠).
والتعاون الدولي مهم عند التعامل مع جرائم الإنترنت، كونه سيطّور اساليب متشابهة لتحقيق قانون جنائي واجرائي لحماية شبكات المعلومات الدولية ،خاصة ان هذه الجرائم هي عابرة للقارات ولا حدود لها، وفي المقابل فان عدم التعاون الدولي سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين من الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية (الشنيفي، ١٤١٤هـ :١١٣).

وتعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (١٩٧٣م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها (الشنيفي، ١٤١٤هـ : ١٠٨؛ عيد، ١٤١٩هـ : ٢٥٥)
وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (١٩٧٦م ــ ١٩٨٥م)، وفي عام (١٩٨٥م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي:
جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (١٩٨٦م) صدر قانونا تشريعاً يحمل الرقم (١٢١٣) عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي، وقد خولت وزارة العدل الأمريكية في عام (٢٠٠٠م) خمسة جهات منها مكتب التحقيقات الفيدرالي (FBI) للتعامل مع جرائم الحاسب الآلي والانترنت (الشنيفي، ١٤١٤هـ: ١٠٩؛ عبدالمطلب، ٢٠٠١م: ٩٢ ــ ٩٤؛ عيد، ١٤١٩هـ: ٢٥٥).
وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (١٩٨١م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى (الشنيفي، ١٤١٤هـ : ١٠٩؛ عيد، ١٤١٩هـ : ٢٥٥)

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت في عام (١٩٨٥م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي، كما وضّح فيه صلاحيات جهات التحقيق كما جاء في قانون المنافسة (The Competition Act) مثلا الذي يخول لمأمور الضبط القضائي متى ما حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها (احمد، ٢٠٠٠م : ٢٦٣؛ الشنيفي، ١٤١٤هـ : ١١٠؛ عيد، ١٤١٩هـ : ٢٥٥)

وفي عام (١٩٨٥م) سنّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها (الشنيفي، ١٤١٤هـ : ١١٠؛ عيد، ١٤١٩هـ : ٢٥٥)

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (١٩٨٨م) القانون رقم (١٩-٨٨) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها، كما تم عام (١٩٩٤م) تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية وأوكل إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب التحريات وسماع الأقوال (تمام، ٢٠٠٠م : ٩١- ٩٢، ١١٥؛ شتا، ٢٠٠١م : ٧٠)

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقل ثلاثة أيام (احمد، ٢٠٠٠م : ٢٢٢، ٢٦٣)

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته،كما أقرت عام (١٩٩١م) شرعية التنصت على شبكات الحاسب الآلي للبحث عن دليل (احمد، ٢٠٠٠م : ٢٢٢، ٢٧٦).

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج، كما تعطي الشاهد أيضا الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى ما كان ذلك إلى إدانته أو إدانة احد أقاربه. بل تذهب القوانين الجنائية المعمول بها في بولندا إلى ابعد من هذا حيث أنها تنص على أن لا يقابل ذلك أي إجراء قسري أو تفسيره بما يضر المتهم (احمد، ٢٠٠٠م : ٢٧٦).

هذا وعلى مستوى الدول العربية فانه وحتى تاريخه ،وبحسب علم الباحث، لم تقم أي دولة عربية بسن قوانين خاصة بجرائم الحاسب الآلي والانترنت، ففي مصر مثلا لا يوجد نظام قانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية، ومن ذلك مثلا اعتبر أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات، كما تم تطويع نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاء الأسرار بحيث يمكن تطبيقها على بعض الجرائم المعلوماتية، وأوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية (تمام، ٢٠٠٠م : ٩١- ١٠٤، ١٢٦).

وكذا الحال بالنسبة لمملكة البحرين فلا توجد قوانين خاصة بجرائم الإنترنت، وان وجد نص قريب من الفعل المرتكب فان العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة على جريمة الإنترنت. وقد أوكل إلى شركة البحرين للاتصالات السلكية واللاسلكية (بتلكو) مهمة تقديم خدمة الإنترنت للراغبين في ذلك، كما أنيط بها مسئولية الحد من إساءة استخدام شبكة الإنترنت من قبل مشتركيها (بحر، ١٤٢٠هـ : ٣٩، ٤٣).

وعلى المستوي المحلي نجد أن المملكة العربية السعودية أيضا لم تسن قوانين خاصة بجرائم الإنترنت ،إلا أن الوضع مختلف هنا، فهي ليست في حاجة لتحديث قوانينها وتشريعاتها كونها تنطلق من الشريعة الإسلامية الكاملة، فالمشرع واحد لا ثاني له والتشريع أزلي لا تجديد له، وهو مع كونه أزلي فانه صالح لكل زمان ومكان كونه صادر من خالق الكون والعليم بما يَصْلُحُ له ويُصْلِحُهُ " وتركت الشريعة الإسلامية الباب مفتوحا لتجريم الجرائم المستحدثة تحت قواعد فقهية واضحة منها لا ضرر ولا ضرار وتركت لولي الأمر تقرير العقوبات لبعض الجرائم المستحدثة مراعاة لمصلحة المجتمع ويندرج ذلك تحت باب التعازير" (الشهري، عبدالله، ١٤٢٢هـ : ٣٨)، وهناك قاعدة سد الذرائع أي "دفع الوسائل التي تؤدي إلى المفاسد، والأخذ بالوسائل التي تؤدي إلى المصالح" (أبو زهرة، ١٩٧٦م : ٢٢٦)

"ومن المقرر فقهياً أن دفع المفاسد مقدم على جلب المصالح" (أبو زهرة، ١٩٧٦م : ٢٢٨)

ونظراً لأن "الظاهرة الإجرامية من الظواهر الاجتماعية التي تتميز بالنسبية، لأنها تختلف باختلاف الثقافات، فما يعد جريمة أو جنحة في مجتمع ما قد يعد مقبولا في مجتمع آخر. فالتشريع والثقافة السائدان في كل مجتمع هما اللذان يحددان الجرائم والفضائل" (السيف، ١٤١٧هـ:١).

لذا فان هذا البحث وعند دراسته لجرائم الانترنت في المجتمع السعودي فانه ينطلق من القوانين الشرعية المعمول بها في المملكة العربية السعودية التي تستمد قوانينها من كتاب الله وسنة نبيه محمد عليه أفضل الصلاة وأزكى التسليم، وليس من القوانين الوضعية التي قد تتفق في تعريف الجريمة إلا أنها تختلف حتما في تقسيمها للجريمة.

فالجريمة في القوانين الوضعية تعّرف بأنها كل فعل يعاقب عليه القانون، أو امتناع عن فعل يقضي به القانون، ولا يعتبر الفعل أو الترك جريمة إلا إذا كان مجرّماً في القانون. أما التعريف الشرعي للجريمة فهي إتيان فعل محرم معاقب على فعله أو ترك فعل محرم الترك معاقب على تركه، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه. (عودة، ١٤٠١هـ : ٦٦). أو بمعنى آخر هي "فعل ما نهي الله عنه، وعصيان ما أمر الله به" (أبو زهرة، ١٩٧٦م : ٢٤).

وقد لا يبدوا أن هناك اختلاف كبير بين التعريفين ،وهذا صحيح إلى حد كبير، ولكن يتّضح الاختلاف في التقسيم الذي يأخذ به كل فريق، ففي الشريعة الإسلامية تقّسم الجريمة من حيث جسامة العقوبة إلى حدود، قصاص أو دية، وتعازير، في حين تقّسم القوانين الوضعية الجريمة من حيث العقوبة إلى جنايات، جنح، ومخالفات (الدمينى، ١٤٠٢هـ، طالب، ١٩٩٨م : ١٦٨). أو بمعنى آخر فان القوانين الوضعية " تقسم الجريمة أساسا على مقدار العقوبة، وبذلك كأن تحديد الجريمة يعتبر فرعا من العقوبة، في حين أن التشريع الإسلامي يجعل الأساس في العقوبة هو جسامة الجريمة وخطرها من حيث المساس بالضرورات الخمس" (منصور، ١٤١٠هـ : ٢١٣ – ٢١٤).

وبشكل أدق فالاختلاف يقع في التقسيم الثالث أي في قسم التعازير في الشريعة وقسم المخالفات في القوانين الوضعية، ففي الأولي أشمل واعم حيث انه يدخل في التعازير كل الأفعال سواء المجرمة أو غير المجرمة، أي التي لها عقوبة محددة أو التي لم ينص علي عقوبة محددة لها، فالعقوبة هنا تقديرية للقاضي وتبدأ من الزجر والتوبيخ وتصل إلى حد إيقاع عقوبة القتل تبعا للفعل المرتكب ولنظرة القاضي لذلك الفعل. في حين يحدد القانون الوضعي عقوبات محددة للمخالفات بمعنى انه لا يمكن معاقبة أي فعل ما لم يكن هناك نص محدد له في القانون وإلا لم

يعتبر جرما، ومن هنا تختلف النظرة إلى الجريمة في الشريعة الإسلامية عنها في القوانين الوضعية حيث أنها أشمل وأعم في الشريعة عنها في القوانين الوضعية، الأمر الذي يجعل معه الشريعة الإسلامية متطورة ومتجددة دوما فهناك عقوبة لكل فعل شاذ أو غير مقبول وان لم ينص على تجريمه قانونيا.

ولا يعنى هذا أن كل الأفعال مجرّمة في الشريعة بل المقصود هو أن أي فعل شاذ أو منافي لتعاليم الدين الإسلامي ولو كان جديدا فان هناك عقاب له في الشريعة، فـ"الأساس بلاشك في اعتبار الفعل جريمة في نظر الإسلام هو مخالفة أوامر الدين"(أبوزهرة، ١٩٧٦م: ٣١)، أما العقوبة المقررة لكل جريمة فمتفاوتة حيث "تتفاوت الجرائم في الإسلام بتفاوت ما فيها من مفاسد" (أبو زهرة، ١٩٧٦م: ١٨٥)، فالشريعة حددت إطار عام للأفعال المقبولة وغير المقبولة جديدها وقديمها، كما حددت العقوبة المناسبة لكل جريمة أو فعل غير مقبول، وهنا سر تفوق الشريعة الإسلامية.

ومن هذا فقضية الجريمة والعقوبة ومستجداتها أمر محسوم في المملكة العربية السعودية ويميزها عن غيرها من الدول، فالقانون الجنائي لديها ،والمستمد من الشريعة، يتسم "بوضع متميز بين سائر التقنيات الجنائية المقارنة، حيث عالجها الشارع الحكيم في إطار النظام القانوني الشامل المتكامل الذي يغطي كل جوانب الحياة ويصلح لكل زمان ومكان. فالتجريم والعقاب في النظام الإسلامي يتوجه مباشرة إلى صيانة وحماية المصالح المعتبرة في الإسلام، وهي الدين والنسل والنفس والمال والعقل، وأي اعتداء على مصلحة من تلك المصالح يعتبر جريمة يعاقب فاعلها، ويختلف بالطبع مقدار العقوبة حسب جرامة الفعل الإجرامي" (عجب نور، ١٤١٧هـ : ١٣).

ومع ذلك فالأمر يحتاج إلى وضع أسس تنظيمية فاعلة وشاملة لتحديد الجهة المخولة بداية للتعامل مع جرائم الإنترنت والأفعال غير الأخلاقية والتصرفات السلبية التي تحدث أثناء استخدام شبكة الإنترنت تحقيقاً وضبطاً ووقايةً، وكذلك تحديد كيفية التعامل الإداري والإجرائي في هذه القضايا، فلا بد أن يواكب استخدام المملكة العربية السعودية لتقنية الإنترنت ظهور أنماط جديدة من الإجرام -كغيرها من الدول التي أخذت بالتقنية الحديثة- فهذه الأنماط ليست قاصرة على دولة دون أخرى.

فلا بد إذن من وضع تنظيم إداري واضح للحد من سلبيات هذه الأفعال ومحاسبة مرتكبيها وإعطاء الحق للمتضررين منها. فهذه التنظيمات سوف تُفَعِّلْ قوانين وتشريعات المملكة المستمدة من الشريعة الإسلامية لتضع بعض الحواجز والروادع أمام من يرتكب مثل هذه الجرائم من داخل المملكة.

وقد بدأت المملكة بالعمل في هذا الاتجاه حيث أوكلت المهمة مبدئيا إلى مدينة الملك عبدالعزيز للعلوم والتقنية لتقديم هذه الخدمة عبر مزودي خدمة تجاريين، كما شكلت لجنة أمنية دائمة برئاسة وزارة الداخلية وعضوية ممثلين من القطاعات الأمنية والدينية والاجتماعية والاقتصادية المختصة للإشراف على أمن خدمة الإنترنت في المملكة وتشمل مهمتها تحديد المواقع غير المرغوبة والتي تتنافى مع الدين الحنيف والأنظمة الوطنية ومتابعة كل ما يستجد منها لحجبها خاصة تلك المواقع الإباحية أو الفكرية أو الأمنية (النشرة التعريفية، ١٤١٩هـ).

وفي تقرير صحفي نشر في موقع صحيفة الجزيرة بتاريخ ١٤٢١/٢/٢هـ (الجزيرة، ١٤٢١هـ)، كشفت مدينة الملك عبدالعزيز للعلوم والتقنية من خلال وحدة الإنترنت المشرفة على عمل مقدمي خدمة الإنترنت في المملكة عن إجراءات فنية تهدف إلى محاصرة أعمال المخربين أو المتسللين ومنعهم ومخالفتهم. وأوضحت الوحدة أنها قد ألزمت جميع مقدمي خدمة الإنترنت في المملكة بتطبيق عدد من الإجراءات الفنية لمنع أعمال المتسللين وإساءة استخدام البريد الإلكتروني وغيرها من المخالفات المتعلقة بالجوانب الأمنية لاستخدام شبكة الإنترنت في المملكة ومن بين هذه الإجراءات ما يلي:

١. منع انتحال أرقام الإنترنت أو ما يعرف بـ(Ip-spoofing) والتي يقوم خلالها بعض المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة.
٢. منع إساءة استخدام البريد الإلكتروني أو ما يعرف بـ(E-Mail Spamming) سواء للتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ما عرف اصطلاحا باسم البريد المهمل والذي ينتشر بشكل كبير في الدول المتقدمة.
٣. الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمشتركين (Dialup-Server) وسجل استخدام البروكسي (Proxy) لمدة لا تقل عن (٦) أشهر.
٤. الحصول على خدمة الوقت (NTP) عن طريق وحدة البروكسي ومزود الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات.
٥. تحديث سجلات منظمة رايب (www.ripe.com) الخاصة بمقدمي الخدمة.
٦. ضرورة تنفيذ ما تتوصل إليه اللجنة الأمنية الدائمة بخصوص متابعة ومعاقبة المخالفات الأمنية.

كما أشارت صحيفة عكاظ في عددها رقم (١٢٧٨٩) وتاريخ١٤٢٢/٦/١٣هـ (عكاظ،١٤٢٢هـ)، بأن مجلس الوزراء السعودي يدرس نظاما جديدا للإنترنت يتضمن فرض عقوبات من بينها السجن وغرامات مالية على مخربي شبكة المعلوماتية (المتسللين)، وأن العقوبات على مخربي الإنترنت ستحدد وفقا للضرر الناجم عن عمليات الاختراق والأعمال التخريبية وأن العقوبة قد تصل إلى السجن سبع سنوات إلى جانب غرامات مالية.

وهذه التنظيمات مفيدة ولا شك إلا أنها ليست كافية، فالمهم هنا وبداية تحديد جهة متخصصة ومؤهلة للتعامل مع جرائم الإنترنت تحقيقا وضبطا ووقاية، خلاف مدينة الملك عبدالعزيز التي تضطلع بمهام كثيرة ومختلفة عن المهام التي ستوكل للجهة التي ستحدد لمثل هذا العمل. وعلى كل حال فيجب أن لا يركن إلى الأنظمة والتعليمات فقط عند التعامل مع الجرائم والتجاوزات، فالأنظمة ليست وحدها الرادع لأي مخالفات أو سلبيات وخاصة في بيئة دينية محافظة كالمملكة العربية السعودية حيث يلعب الوازع الديني والرقابة الذاتية دور مهم في عملية في عملية الردع والحد من أي تجاوزات، فمن المهم أن يؤخذ

" الجانب الديني في الاعتبار عند مناقشة أخلاقيات تدوال المعلومات كنوع من الضوابط الدينية التي تحكم أخلاقيات استخدام وتداول المعلومات، والتي تردع أي اتجاه لدى الأفراد نحو ارتكاب جرائم نظم المعلومات (الانترنت)، فالملاحظ انه توجد معلومات تقدمها جهات كثيرة بالمجان وشبكة الانترنت متخمة بكميات هائلة من هذه المعلومات الصالح منها والمفسد. وينطبق هذا على جميع أنواع العلوم والفنون من خلال ملايين المواقع التي يطلع على محتواها أكثر من ستين إلى مائة مليون متصل بالشبكة يوميا ويتضاعف عددهم بسرعة مخيفة. ومن ثم يجب أن نركز على ضرورة وجود الضوابط الدينية والأخلاقية، فالذي لا وازع ولا ضمير له قد أتيحت له وسيلة سهلة للغاية في توصيل أفكاره ونشر مفاسده بالدرجة نفسها المتاحة أمام النافعين للناس، وقوانين الدول تختلف فيما تتبناه من أساليب للتحكم فيما ينشر عبر شبكة الانترنت، والمحرمات تختلف من مكان لآخر." (داود ، ١٤٢٠هـ : ٢١٧).

ولعلنا لا نغفل العادات والتقاليد المستوحاة من شريعتنا الإسلامية وتقاليدنا العربية الأصيلة والتي تزرع بداخل المواطن الوازع الديني الرادع عن ارتكاب المخالفات والنواهي، ومع كل هذه الضوابط فالنفس أمارة بالسوء والشيطان يجري من ابن ادم مجرى الدم، فيجب أن يكون هناك ضوابط عقابية تحد من يضعف رادعه الإيماني ليجد الرادع السلطاني له بالمرصاد فان الله ليردع بالسلطان ما لا يردع بالقرآن.

المبحث الثالث:

الأبعاد الفنية للأفعال الجنائية المرتكبة

من قبل مستخدمي الإنترنت في المجتمع السعودي (تصور إسلامي)

الاستعراض السابق كان يتحدث بصفة عامة عن مواكبة القوانين الدولية والعربية والمحلية للجرائم المستحدثة ومنها جرائم الإنترنت، ولكن ما هي المنطلقات الشرعية والقانونية لإطلاق مصطلح جريمة على الأفعال المرتكبة أثناء استخدام الإنترنت في المجتمع السعودي. وللإجابة على هذا السؤال يستحسن التطرق بشيء من التفصيل للجرائم والأفعال التي تطرقت إليها الدراسة وتكيفها شرعياً وقانونياً وهذه الأفعال هي:

أولا : الجرائم الجنسية والممارسات غير الأخلاقية وتشمل:

١. المواقع والقوائم البريدية الإباحية:

يندرج تحت هذا البند جرائم ارتياد المواقع الإباحية، الشراء منها، الاشتراك فيها، أو إنشائها. وقد" أصبح الانتشار الواسع للصور والأفلام الإباحية على شبكة الإنترنت يشكل قضية ذات اهتمام عالمي في الوقت الراهن، بسبب الازدياد الهائل أعداد مستخدمي الإنترنت حول العالم" (الزعاليل، ١٤٢٠هـ: ٧٦)، وتختلف المواقع الإباحية عن القوائم البريدية - التي تخصص لتبادل الصور والأفلام الجنسية - في أن المواقع الإباحية غالبا ما يكون الهدف منها الربح المادي حيث يستوجب على متصفح هذه المواقع دفع مبلغ مقطوع مقابل مشاهدة فيلم لوقت محدد أو دفع اشتراك شهري أو سنوي مقابل الاستفادة من خدمات هذه المواقع، وأن كانت بعض هذه المواقع تحاول استدراج مرتاديها بتقديم خدمة إرسال صور جنسية مجانية يومية على عناوينهم البريدية، كما أن تصفح الموقع يتطلب في الغالب الاتصال المباشر بشبكة الإنترنت مما يعنى انه قد يتم حجبه من قبل مدينة الملك عبدالعزيز للعلوم والتكنولوجيا فلا يمكن الوصول إليه إلا باستخدام البروكسي.

أما القوائم البريدية فهي أسهل إنشاءً، وغالباً مجانية ويقوم أعضائها من المشتركين بتبادل الصور والأفلام على عناوينهم البريدية وربما تكون القوائم البريدية ابعد عن إمكانية المتابعة الأمنية حيث يركز نشاطها على الرسائل البريدية والتي تكون من الصعوبة بمكان منعها عن أعضاء أي مجموعة، حتى وأن تم الانتباه إلى تلك القائمة لاحقا وتم حجبها، فان الحجب يكون قاصرا على المشتركين الجدد واللذين لا يتوفر لديهم وسائل تجاوز المرشحات، أما الأعضاء السابقين فلا حاجة لهم إلى الدخول إلى موقع القائمة حيث يصل إلى بريدهم ما يردونه دون أن تستطيع وسائل الحجب التدخل. ويشترك في القوائم البريدية ألاف الأشخاص التي تصل أي رسالة يرسلها مشترك منهم إلى جميع المشتركين مما يعنى كم هائل من الرسائل والصور الجنسية التي يتبادلها مشتركي القائمة بشكل يومي.

واستفادت هذه المواقع والقوائم من الانتشار الواسع للشبكة والمزايا الأخرى التي تقدمها حيث " تتيح شبكة الإنترنت أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخليعة بشكل علني فاضح يقتحم على الجميع بيوتهم ومكاتبهم، فهناك على الشبكة طوفان هائل من هذه الصور والمقالات والأفلام الفاضحة بشكل لم يسبق له مثيل في التاريخ" (داود،١٤٢٠هـ : ٩٣)، فكل مستخدم للانترنت معرض للتأثر بما يتم عرضه على الإنترنت الذي لا يعترف بأي حدود دولية أو جغرافية فهو يشكل خطرا حقيقيا للأطفال فضلا عن الكبار نتيجة تأثيراته المؤذية وغير المرغوبة (موثق في الزغاليل، ١٤٢٠هـ : ٧٨). ويوجد على الإنترنت ألاف المواقع الإباحية وعدد كبير جدا من القوائم الجنسية والتي أصبحت أكثر تخصصا فهناك قوائم خاصة للشواذ من الجنسين وهناك قوائم أخرى تصنف تحت دول محددة ومن المؤسف انه وجدت بعض المواقع الشاذة بمسميات عربية بل وسعودية والأدهى والأمَرْ أن يربط بين بعض القوائم الإباحية والإسلام كموقع أسمى نفسه " السحاقيات المسلمات " وهكذا.

وكشفت إحدى الدراسات أن معدل التدفق على الواقع الإباحية في أوقات العمل التي تبدأ من الساعة التاسعة صباحا إلى الخامسة عصرا تمثل (٧٠٪) من إجمالي نسبة التدفق على تلك المواقع (بي بي سي، ٢٠٠١م).

كما كشفت دراسة قام بها الدكتور مشعل القدهي (القدهي،١٤٢٢هـ) بان هناك إقبال كبير جدا على المواقع الإباحية حيث تزعم شركة (Playboy) الإباحية بأن (٤,٧) مليون زائر يزور صفحاتهم على الشبكة أسبوعياً، وبأن بعض الصفحات الإباحية يزورها (٢٨٠,٠٣٤) زائر يوميا وأن هناك مائة صفحة مشابهة تستقبل أكثر من (٢٠,٠٠٠) ألف زائر يوميا وأكثر من ألفين صفحة مشابهة تستقبل أكثر من (١٤٠٠) زائر يوميا، وأن صفحة واحدة من هذه الصفحات استقبلت خلال عامين عدد (٤٣,٦١٣,٥٠٨) مليون زائر، كما وجد أن (٨٣,٥٪) من الصور المتداولة في المجموعات الإخبارية هي صور إباحية، وبأنّ أكثر من (٢٠٪) من سكان أمريكا يزورون الصفحات الإباحية حيث تبدأ الزيارة غالبا بفضول وتتطور إلى إدمان، وغالبا لا يتردد زوار هذه المواقع من دفع رسوم مالية لقاء تصفح المواد الإباحية بها أو شراء مواد خليعة منها وقد بلغت مجموعة مشتروات مواد الدعارة في الإنترنت في عام (١٩٩٩م) ما نسبته (٨٪) من دخل التجارة الإلكترونية البالغ (١٨) مليار دولار أمريكي في حين بلغت مجموعة الأموال المنفقة للدخول على المواقع الإباحية (٩٧٠) مليون دولار ويتوقع ارتفاع المبلغ ليصل إلى (٣) مليار دولار في عام (٢٠٠٣م)، وقد أتضح أن أكثر مستخدمي المواد الإباحية تتراوح أعمارهم ما بين (١٢) و (١٥) عام في حين تمثل الصفحات الإباحية أكثر صفحات الإنترنت بحثا وطلبا.

كما وضحت دراسة أدست (Adsit) (Adsit, 1999) أن المواقع الإباحية أصبحت مشكلة حقيقية وأن الآثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون الآخر، ويمكن أن يلمس أثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة واغتصاب الأطفال بصفة خاصة، العنف الجنسي، فقد العائلة لقيمها ومبادئها وتغيير الشعور نحو النساء إلى الابتذال بدل الاحترام. ويبدوا أن لكثرة المواقع الإباحية على الإنترنت والتي يقدر عددها بحوالي (٧٠,٠٠٠) ألف موقع دور كبير في إدمان مستخدمي الإنترنت عليها حيث أتضح أن نسبة (١٥٪) من مستخدمي الإنترنت البالغ عددهم(٩,٦٠٠,٠٠٠) مليون شخص تصفحوا المواقع الإباحية في شهر ابريل عام (١٩٩٨م).

وقد جرى حصر القوائم العربية الإباحية فقط دون القوائم الأجنبية في بعض المواقع على شبكة الإنترنت ومنها موقع الياهو (YAHOO) فوجد أنها تصل إلى (١٧١) قائمة، بلغ عدد أعضاء اقل تلك القوائم (٣) في حين وصل عدد أكثرها أعضاء (٨٦٨٣) أما موقع قلوب لست (GLOBELIST) فقد احتوى على (٦) قوائم إباحية عربية، في حين وجد عدد (٥) قوائم عربية إباحية على موقع توبيكا (TOPICA) وقد قامت مدينة الملك عبدالعزيز للعلوم والتقنية مشكورة بإغلاق تلك المواقع.

فارتياد مثل هذه المواقع ومشاهدة المواد الجنسية بها من المحظورات الشرعية التي حرص الشارع الحكيم على التنبيه عليها وتحريمها، بل أن الشارع الحكيم امرنا بغض البصر وحرّم النظر إلى الأجنبيات سواء بصورة أو حقيقة وليس فقط تجنب النظر إلى الحرام فقال عز وجل في كتابه الحكيم في سورة النور: (قُلْ لِلْمُؤْمِنِينَ يَغُضُّوا مِنْ أَبْصَارِهِمْ وَيَحْفَظُوا فُرُوجَهُمْ ذَلِكَ أَزْكَى لَهُمْ إِنَّ اللَّهَ خَبِيرٌ بِمَا يَصْنَعُونَ(٣٠)).

فهناك ولا شك علاقة بين " ارتكاب الأفعال الجنسية المحرمة والنظر إلى الصور الجنسية العارية، فالدين الإسلامي الحنيف حذر من ظاهرة النظر للعراة، لما تحدثه من تصدعات أخلاقية في الفرد والمجتمع" (السيف، ١٤١٧هـ : ١٠٠).

ويذهب الشارع إلى ابعد من ذلك لعلمه بمخاطر النظر وما يمكن أن يوصل إليه، فحرّم رسول الله صلى الله عليه وسلم أن تصف المرأة لزوجها جمال امرأة أخرى لا تحل له وكأنه ينظر إليها فقال عليه الصلاة والسلام في الحديث الذي رواه البخاري في صحيحه واحمد في مسنده واللفظ للبخاري: " قَالَ النَّبِيُّ صَلَّى اللَّهم عَلَيْهِ وَسَلَّمَ لَا تُبَاشِرُ الْمَرْأَةُ الْمَرْأَةَ فَتَنْعَتَهَا لِزَوْجِهَا كَأَنَّهُ يَنْظُرُ إِلَيْهَا".

كل هذه الأمور اهتم بها الشارع وحرمها كونها موصلة لجريمة الزنا التي تعد من الكبائر والتي متى ما اجتب الأفراد هذه الأفعال فلن يقعوا في الزنا. ولعل من حكمة الشارع ومعرفته بالغرائز البشرية التي يساهم الشيطان في تأجيجها ليوقع الإنسان فيما حرم الله، ولعظمة جريمة الزنا فانه لم يحرم الزنا فقط بل حرم الاقتراب منه فقال تعالى في سورة الإسراء: (وَلَا تَقْرَبُوا الزِّنَى إِنَّهُ كَانَ فَاحِشَةً وَسَاءَ سَبِيلًا(٣٢))

يقول القرطبي رحمه الله في تفسير هذه الاية " قال العلماء قوله تعالى "ولاتقربوا الزنى" ابلغ من ان يقول ولا تزنوا فإن معناه فلا تدنوا من الزنا. فاي اقتراب من المحظور هو فعل محظور في حد ذاته، ومن ذلك مشاهدة المواد الجنسة فضلا عن الاشتراك في تلك القوائم الاباحية أو شراء مواد جنسية منها أو ،وهو الاخطر ضررا، انشائها كون الفعل الاخير متعدي ضرره للغير ويدخل فاعله في وعيد الله عز وجل حين قال في سورة النور: (إِنَّ الَّذِينَ يُحِبُّونَ أَنْ تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالْآخِرَةِ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لَا تَعْلَمُونَ(١٩))

وقد اثبتت بعض الدراسات في المجتمع السعودي ان (٦٨,٨ ٪) من مجموعة المبحوثين يرون ان هناك علاقة بين الانحراف والجرائم المرتبكة وبين مشاهدةاشرطة الفيدوا الجنسية، كما اثبتت احدى الدراسات المتخصصة بتفسير ارتكاب الجريمة الجنسية في المجتمع السعودي والتي اجريت في الاصلاحيات المركزية بالمملكة ان (٥٣,٧ ٪) من مرتكبي الجرائم الجنسية كان لهم اهتمامات بالصور الجنسية وان فئة كبيرة منهم كانوا يميلون إلى مشاهدة الافلام الجنسية الخليعة وقت فراغهم، كما تبين من الدراسة قوة تأثير مثل هذه الصور في ارتكاب جرائم الاعتداء الجنسي من قبل مجرمي اغتصاب الاناث وهاتكي اعراض الذكور بقوة (السيف، ١٤١٧هـ : ٩٩).

. المواقع المتخصصة في القذف وتشويه سمعة الاشخاص:

تعمل هذه المواقع على ابراز سلبيات الشخص المستهدف ونشر اسراره، والتي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، أو بتلفيق الاخبار عنه. وهناك حادثة مشهورة جرىتدأولها بين مستخدمى الإنترنت في بداية دخول الخدمة للمنطقة حيث قام شخص في دولة خليجية بإنشاء موقع ونشر صور احدى الفتيات وهي عارية وفي أوضاع مخلة مع صديقها، وقد حصل علي تلك الصور بعد التسلل إلى حاسبها الشخصي وحأول ابتزازها جنسيا ورفضت فهددها بنشر تلك الصور على الإنترنت وفعلا قام بتنفيذ تهديده بانشاء الموقع ومن ثم وزع الرابط لذلك الموقع على العديد من المنتديات والقوائم البريدية وادى ذلك إلى انتحار الفتاة حيث فضحها بين ذويها ومعارفها.

كما وقعت حادثة تشهير أخرى من قبل من اسموا نفسهم " الامجاد هكرز " حيث اصدروا بيان نشر على الإنترنت بواسطة البريد الالتكروني ووصل العديد من مشتركي الإنترنت أوضحوا فيه قيام شخص يكنى بحجازي نادي الفكر على التطاول في احدى المنتديات بالقدح والسب السافر على شيخ الإسلام ابن تيمية والشيخ محمد بن عبدالوهاب وغيرهم من رموز الدعوة السلفية وقد استطاع (الأمجاد هكرز) اختراق البريد الإلكتروني الشخصي للمذكور ومن ثم تم نشر صوره وكشف اسراره في موقعهم على الإنترنت حيث خصصوا صفحة خاصة للتشهير به وعنوانها على الشبكة هو : http://216.169.120.174/hijazi.htm (موقع منتدى الفوائد،١٤٢١هـ)

وحوادث التشهير والقذف في شبكة الإنترنت كثيرة فقد وجد ضعفاء النفوس في شبكة الإنترنت، وفي ظل غياب الضوابط النظامية والجهات المسئولة عن متابعة السلبيات التي تحدث اثناء إستخدام الإنترنت، متنفسا لاحقداهم ومرتعا لشهواتهم المريضة دون رادع أو خوف من المحاسبة وقد قيل قديما "من أمن العقوبة أساء الادب".

والقذف مُجَّرم شرعاً، ونظرا لشناعة الجرم ومدى تاثيره السلبي على المجنى عليه والمجتمع كونه يساعد على اشاعة الفاحشة بين الناس بكثرة الترامي به، فقد جعل عقوبته من الحدود والتي لا يملك احد حق التنازل عنه ولا يجوز العفو عنها بعد طلب المخاصمة امام القضاء،كما

جعلها عقوبة ذات شقين الأول عقوبة بدنية بجلده ثمانين جلدة لقوله تعالى في سورة النور(وَالَّذِينَ يَرْمُونَ الْمُحْصَنَاتِ ثُمَّ لَمْ يَأْتُوا بِأَرْبَعَةِ شُهَدَاءَ فَاجْلِدُوهُمْ ثَمَانِينَ جَلْدَةً (٤))،والشق الثاني عقوبة معنوية بعدم قبول شهادة الجاني بعد ثبوت جلده لقوله تعالى في ذات الاية وذات السورة: (وَلَا تَقْبَلُوا لَهُمْ شَهَادَةً أَبَدًا وَأُولَئِكَ هُمُ الْفَاسِقُونَ (٤)) وشدد رسول الله صلى الله عليه وسلم في جريمة القذف حيث اعتبرها من الموبقات فقال عليه الصلاة والسلام في الحديث المتفق عليه "اجتنبوا السبع الموبقات، قالوا يارسول الله، وما هن؟ قال الشرك بالله، والسحر، وقتل النفس التي حرم الله الا بالحق، وأكل الربا، واكل مال اليتيم، والتولي يوم الزحف، وقذف المحصنات المؤمنات الغافلات". ولا تعاقب الشريعة على القذف الا اذا كان كذبا واختلاقا فان كان حقيقة واقعية فلا جريمة ولاعقوبة (عودة، ١٤٠١هـ: ٦٤٥-٦٤٦؛ فرحات، ١٤٠٤هـ : ١٥١-١٦٤).

. استخدام البروكسي للدخول إلى المواقع المحجوبة:

البروكسي هو برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز موحد، والمعنى المتعارف عليه لدي مستخدمي الانترنت للبروكسي هو ما يستخدم لتجأوز المواقع المحجوبة وهو ما نقصده في هذه الدراسة حيث يستخدم البروكسي من قبل مستخدمي الإنترنت في المجتمع السعودي لتجأوز المواقع المحجوبة من قبل مدينة الملك عبدالعزيز للعلوم والتقنية والتي عادة ما تكون هذه المواقع المحجوبة اما مواقع جنسية أو سياسية معادية للدولة، وقد يتم حجب بعض المواقع التي لا يفترض حجبها كبعض المواقع العلمية والتي تنشر احصائيات عن الجرائم أو حتى بعض المواقع العادية ويعود ذلك للالية التي يتم بها عملية ترشيح المواقع وربما لخطأ بشري في حجب موقع غير مطلوب حجبه، ولذلك فقد تجد من يستخدم البروكسي للدخول إلى موقع علمي أو موقع عادي حجب خطأً، وهذا في حكم النادر والشاذ لا حكم له، في حين ان الغالبية العظمى تستخدم البروكسي للدخول إلى المواقع الجنسية أو المواقع السياسية ولكن بدرجة اقل.

ومن هنا فاستعمال البروكسي للدخول إلى المواقع المجوبة يعتبر امرا مخالفا للنظام الذي اقر حجب تلك المواقع حتى لو افترضنا جدلا ان هناك نسبة بسيطة جدا قد تستخدم البروكسي للدخول إلى المواقع التي قد تكون حجبت بطريق الخطأ، الا ان هذه النسبة سواء من الافراد أو من المواقع التي تحجب بالخطأ تكاد لاتذكر وهي في حكم الشاذ، اضف إلى ذلك انه يفترض في المواطن والمقيم احترام النظام والتقيد به دون ان يعمل بوسيلة أو بأخرى تجاوز هذا النظام لاي مبرر حتى وان شاب النظام خلل اثناء تنفيذه، ففتح مثل هذه الثغرة والسماح للافراد بتجأوز التعليمات التي اقرها النظام لمبرر قد يكون واهي أو لخطأ قد يكون واكب تنفيذ امر فيه من الخطورة الشي العظيم حيث سيجرأ الافراد على تجاوز النظام لاي مبرر وتعم الفوضي وتسود الجريمة.

هذا من ناحية مخالفة إستخدام البروكسي للنظام، اما من ناحية مخالفة إستخدام البروكسي للشرع فهو من شقيين :

أ- ان النظام أُقِّر من ولي الامر و مخالفة ولي الامر من المحظورات الشرعية ، ما دامت تلك الأنظمة لا تخرج عن تعاليم الشرع، والدليل على ذلك قوله تعالى في سورة النساء (َاأَيُّهَا الَّذِينَ آمَنُوا أَطِيعُوا اللَّهَ وَأَطِيعُوا الرَّسُولَ وَأُولِي الْأَمْرِ مِنْكُمْ(٥٩)) وقوله صلى الله عليه وسلم في الحديث الذي روي في المعجم الكبير " يا أيها الناس اتقوا الله واسمعوا وأطيعوا لمن كان عليكم وان عبدا حبشيا مجدعا فاسمعوا وأطيعوا ما أقام فيكم كتاب الله" وفي الحديث الذي رواه احمد في مسنده " قد تركتكم على البيضاء ليلها كنهارها، لا يزيغ عنها بعدي إلا هالك، ومن يعش منكم فسيرى اختلافا كثيرا، فعليكم بما عرفتم من سنتي و سنة الخلفاء الراشدين المهديين، و عليكم بالطاعة و إن عبدا حبشيا عضوا عليها بالنواجذ ، فإنما المؤمن كالجمل الأنف حيثما انقيد انقاد".

ب- اذا كان مشاهدة المواقع الجنسية حرام، فإن إستخدام البروكسي للدخول إلى تلك المواقع حرام ايضا فما بني على باطل فهو باطل، والفعل اذا كان محرماً فان الوسيلة الموصله اليه

تكون محرمة. وتنطبق هنا قاعدة سد الذرائع أي "دفع الوسائل التي تؤدي إلى المفاسد، والاخذ بالوسائل التي تؤدي إلى المصالح" (ابوزهرة، ١٩٧٦م : ٢٢٦)، كما انه "من المقرر فقهياً أن دفع المفاسد مقدم على جلب المصالح" (ابوزهرة، ١٩٧٦م : ٢٢٨).

. إخفاء الشخصية:

توجد الكثير من البرامج التي تمكن المستخدم من إخفاء شخصيته سواء اثناء إرسال البريد أو اثناء تصفح المواقع. ولا شك ان اغلب من يستخدم هذه البرامج هدفهم غير نبيل، فيسعون من خلالها إلى إخفاء شخصيتهم خوفا من مسائلة نظامية أو خجلا من تصرف غير لائق يقومون به. ومن الامور المسلمة بها شرعا وعرفا ان الافعال الطيبة لا يخجل منها الاشخاص بل يسعون عادة ،الا في حالات معينة، إلى الاعلان عنها والافتخار بها، اما الافعال المشينة فيحرص الغالبية على اخفائها. فاخفاء الشخصية غالبا امر مشين وتهرب من المسئولية التي قد تلحق بالشخص متى ما عرفت شخصيته، ولعل ما يدل على ذلك حديث رسول الله صلى الله عليه وسلم الذي رواه مسلم في صحيحه "البر حسن الخلق، والاثم ما حاك في صدرك وكرهت ان يطلع عليه الناس".

٥. إنتحال الشخصية:

وهي تنقسم إلى قسمين:

أ- انتحال شخصية الفرد :

تعتبر جرائم انتحال شخصية الآخرين من الجرائم القديمة الا ان التنامي المتزايد لشبكة الإنترنت اعطى المجرمين قدرة اكبر على جمع المعلومات الشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم. فتنتشر في شبكة الإنترنت الكثير من الاعلانات المشبوهة والتي تداعب عادة غريزة الطمع الانساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك مثلا اعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية والذي يتطلب بطبيعة الحال الافصاح عن بعض المعلومات الشخصية كالاسم والعنوان والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، وبالرغم من ان مثل هذا الاعلان من الوضوح بمكان انه عملية نصب واحتيال الا انه ليس من المستبعد ان يقع ضحيته الكثير من مستخدمي الإنترنت. ويمكن ان تؤدي جريمة انتحال الشخصية إلى الاستيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو حتى الاساءة إلى سمعة الضحية (داود، ١٤٢٠هـ: ٨٤-٨٩).

ب- انتحال شخصية المواقع :

مع ان هذا الاسوب يعتبر حديث نسبياً، الا انه اشد خطورة واكثر صعوبة في اكتشافه من انتحال شخصية الافراد، حيث يمكن تنفيذ هذا الاسلوب حتى مع المواقع التي يتم الاتصال بها من خلال نظم الاتصال الامن (Secured Server) حيث يمكن وبسهولة اختراق مثل هذا الحاجز الامني، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني، أو يحأول المجرم اختراق موقع لاحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور. ويتوقع ان يكثر استخدام اسلوب انتحال شخصية المواقع في المستقبل نظرا لصعوبة اكتشافها (داود، ١٤٢٠هـ:٨٩-٩٣).

والمحاذير الامنية والمخالفات النظامية والشرعية واضحة في هذه الفقرة سواء ماكان منها قاصرا على انتحال شخصية الافراد أو المواقع، فقد حفظت الشريعة السماوية والأنظمة الوضعية الحقوق الشخصية وصانت الملكيات الفردية وجعل التعدي عليها امرا محظورا شرعيا ومعاقب عليه جنائياً.

وفي انتحال شخصية الآخرين تعدي صارخ على حقوقهم وانتهاكا لملكياتهم التي صانها الشرع لهم، كما انه ترتب على انتحال شخصية الاخرين اضرار متنوعة قد تلحق بهم، وتتفأوت هذه

الاضرار بتفأوت نتيجة الفعل والذي قد تقتصر على اضرار معنوية كتشويه سمعة الشخص وقد تصل إلى اضرار مادية كالاستيلاء غير المشروع على ممتلكات ومقتنيات مادية للمجنى عليه.
ومهما كان حجم هذه الاضرار الناتجة عن هذا الفعل غير النظامي فانه لا يمكن الا ان يتضرر المجنى عليه من هذا الفعل وخاصة ان الهدف الغالب من وراء انتحال الشخصية لن يكون حميدا أو بحسن نية أو لخدمة شخص اخر خلاف منتحل الشخصية.
وتتفق الشريعة مع القوانيين الوضعية في جعل الانسان مسئولا عن كل فعل ضار بغيره، سواء اعتبر القانون ذلك الفعل جريمة ام لم يعتبره (عودة، ١٤٠١هـ :٧٧)،
ولا شك ان انتحال شخصية الافراد أو المواقع مضر باصحابها الاساسيين ولذلك فهي جريمة قانونية ومخالفة شرعية.
ثانيا: جرائم الاختراقات:
يشمل هذه القسم جرائم تدمير المواقع، اختراق المواقع الرسمية أو الشخصية، اختراق الأجهزة الشخصية، اختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه أو إغراقه، الاستيلاء على اشتراكات الآخرين وأرقامهم السرية و إرسال الفيروسات والتروجنات.
ولعل جميع هذه الجرائم والافعال مع اختلافها الا انها يجمعها امر واحد وهي كونها جميعا تبدأ بانتهاك خصوصة الشخص ، وهذا سببا كافيا لتجريمها، فضلا عن الحاق الضرر المادي والمعنوي بالمجنى عليهم.
وتتفق التشريعات السماوية والأنظمة الوضعية على ضرورة احترام خصوية الفرد ويعتبر مجرد التطفل على تلك المعلومات سواء كانت مخزنة في الحاسب الآلي أو في بريده الالتكروني أو في أي مكان اخر انتهاكاً لخصوصيته الفردية وحقوقه.
ومن المعلوم "ان الفقهاء يقسمون الحقوق إلى حقوق لله وحقوق للافراد إلا أن الكثيرين منهم يرون بحق ان كل ما يمس حق الجماعة الخالص أو حق الافراد الخالص يعتبر حقا لله تعإلى أي من حقوق الجماعة ونظامها" (عودة، ١٤٠١هـ :٢٠٦)، ومن هنا يعتبر التعدى على حقوق الافراد وانتهاك خصوصياتهم الشخصية مخالفة شرعية وجريمة نظامية كونه ينظر اليه شرعا تعدياً على حق الله.
وقد أدى انتشار الإنترنت إلى تعرض الكثير من مستخدمي الإنترنت لانتهاك خصوصياتهم الفردية سواء عمدا أو مصادفة، فبكل بساطة ما أن يزور مستخدم الإنترنت أي موقع على شبكة الإنترنت حتى يقوم ذلك الموقع باصدار نسختين من الكعكة الخاصة باجهزتهم (Cookies) وهي نصوص صغيرة يرسلها العديد من مواقع الويب لتخزينها في جهاز من يزور تلك المواقع لعدة اسباب لعل منها التعرف على من يكرر الزيارة للموقع أولاسباب أخرى، وتبقى واحدة من الكعكات في الخادم (السيرفر) الخاص بهم والأخرى يتم تخزينها على القرص الصلب لجهاز الزائر للموقع في أحد الملفات التي قامت الموقع الأخرى بتخزينها من قبل دون أن يشعر صاحب الجهاز بذلك أو حتى الاستئذان منه! وفورا يتم اصدار رقم خاص ليميز ذلك الزائر عن غيره من الزوار وتبدأ الكعكة بأداء مهمتها بجمع المعلومات وارسالها إلى مصدرها أو احدى شركات الجمع والتحليل للمعلومات وهي عادة ما تكون شركات دعاية وإعلان وكلما قام ذلك الشخص بزيارة الموقع يتم ارسال المعلومات وتجديد النسخة الموجودة لديهم ويقوم المتصفح لديه بعمل المهمة المطلوبة منه مالم يقم صاحب الجهاز بتعديل وضعها، وقد تستغل بعض المواقع المشبوهة هذه الكعكات بنسخ تلك الملفات والاستفادة منها بطريقة أو بأخرى. كما قد يحصل اصحاب المواقع على معلومات شخصية لصاحب الجهاز طوعا حيث يكون الشخص عادة اقل ترددا عندما يفشى معلوماته الشخصية من خلال تعامله مع جهاز الحاسب الآلي بعكس لو كان الذي يتعامل معه انسان اخر (موقع مجلة الأمن الإلكترونية، ١٤٢١هـ ؛ داود،١٤٢٠هـ: ٥٠- ٥٢).
هذا وان كانت هناك وسائل لحماية الخصوصية اثناء تصفح الإنترنت، الا انه " من الصعب جدا السيطرة على مايحدث للمعلومة بمجرد خروجها من جهاز الحاسب (الآلي) وعلى ذلك فان

حماية الخصوصية يجب ان تبدأ من البداية بتحديد نوعية البيانات التي لاينبغي ان تصبح عامة ومشاعة ثم بتقييد الوصول إلى تلك المعلومات"(داود، ١٤٢٠هـ:٥٣).
يتضح من كل ما تقدم ان هذه الافعال غير شرعية أو حتى اخلاقية ولا تتمشى مع تعاليم ديننا الحنيف الذي حرّص على احترام الحقوق الشخصية وحفظ الملكية الفردية وراع خصوصية الافراد والجماعات، بل اعتبر التعدي على الحقوق الشخصية تعدي على حقوق الله، مما يعنى انها افعال اجرامية وتصرفات لا اخلاقية يعاقب عليها الشرع بعقوبات تختلف بحسب نوع الفعل المرتكب وبحسب الضرر الواقع على المجنى عليه، وقد يدخل الفعل وعقوبته تحت جرائم الحدود أو القصاص أو التعازير وليس المجال هنا مجال تفصيل لهذه الانواع بقدر ما هو مجال تحديد وايضاح ان هذه الافعال مجرّمة وان هناك عقوبة شرعية بحق من يرتكب هذه الافعال.
وقد اجْمَلْتُ ايضاح التكييف الشرعي والنظامي لهذه الافعال كونها متشابهة ومتداخلة إلى حد كبير، الا انه ونظرا لخطورتها وشيوعها فيلزم الامر النتطرق وبشيئ من التفصيل إلى شرح فني لهذه الافعال واضرارها لعله يضيف بعدا اخر يساهم وبوضوح اكثر في التَعَرُفْ على كونها مجرَّمة، وهذه الافعال هي:
١. الاقتحام أو التسلل :
يشمل هذا البند جرائم الاختراقات سواء للمواقع الرسمية أو الشخصية أو إختراق الأجهزة الشخصية، إختراق البريد الإلكتروني أو الاستيلاء عليه، الاستيلاء على اشتراكات الآخرين وأرقامهم السرية. وهي افعال اصبحت تنشر يوميا في الصحف والاخبار فكثيراً ما " تتدأول الصحف والدوريات العلمية الان أنباء كثيرة عن الاختراقات الأمنية المتعددة في اماكن كثيرة من العالم ليس اخرها اختراق اجهزة الحاسب (الآلي) في البنتاجون (وزارة الدفاع الأمريكية) " (داود، ١٤٢٠هـ: ٩٩).
ولكي يتم الاختراق فان المتسللون إلى اجهزة الاخرين يستخدممون ما يعرف بحصان طروادة وهو برنامج صغير يتم تشغيله داخل جهاز الحاسب لكي يقوم بأغراض التجسس على أعمال الشخص التي يقوم بها على حاسوبه الشخصي فهو في أبسط صورة يقوم بتسجيل كل طرقة قام بها على لوحة المفاتيح منذ أول لحظة للتشغيل ويشمل ذلك كل بياناته السرية أو حساباته المالية أو محادثاته الخاصة على الإنترنت أو رقم بطاقة الائتمان الخاصة به أو حتى كلمات المرور التي يستخدمها لدخول الإنترنت والتي قد يتم إستخدامها بعد ذلك من قبل الجاسوس الذي قام بوضع البرنامج على الحاسب الشخصي للضحية.
و" يعتبر الهجوم على المواقع المختلفة في شبكة الإنترنت (اقتحام المواقع) من الجرائم الشائعة في العالم، وقد تعرضت لهذا النوع من الجرائم في الولايات المتحدة مثلا كل من وزارة العدل والمخابرات المركزية والقوات الجوية، كما تعرض له حزب العمال البريطاني" (داود، ١٤٢٠هـ: ٨٣).
وقد قام قراصنة اسرائيلين باقتحام صفحة الإنترنت الاعلامية الخاصة ببنك فلسطين المحدود ووضعوا بها صورا وشعارات معادية مما اضطر البنك إلى الغاء الصفحة ومحوها كليا، كما تعرضت العديد من الشركات الخاصة في مناطق الحكم الذاتي للهجوم والعبث ومنها شركة اقتحم المتسللون اجهزتها ووضعوا صورة زوجة مدير الشركة وهي عارية بعد تجريدها من الملابس بواسطة الحاسب الآلي (ابوشامة، ١٤٢٠هـ: ٣٧).
وفي عام (١٩٩٧م) قدّرَتْ وكالة المباحث الفدرالية الأمريكية (FBI) تعرض(٤٣٪) من الشركات التي تستخدم خدمة الإنترنت لمحولة تسلل تتراوح مابين (١-٥) مرات خلال سنة واحدة (Wilson,2000)، ولا يقتصر التسلل على المحترفين فقط بل انه قد يكون من الهواة ايضا حيث يدفعهم إلى ذلك الفراغ ومحاولة اشغال الوقت، كما حدث مع مراهقة في الخامسة عشر من عمرها قامت بمحاولة التسلل إلى الصفحة العنكبوتية الخاصة بقاعدة عسكرية للغواصات الحربية بسنغافورة وذلك بسبب انها لم تكن تحب مشاهدة التلفزيون لذلك فكرت ان تكون متسللة (Hacker) (Koerner,1999).

وهو ايضا ما اتضح لوكالة المباحث الفدرالية (FBI) اثناء حرب الخليج الأولى عندما اجروا تحقيقا حول تسلل اشخاص إلى الصفحة العنكبوتية الخاصة باحدى القواعد العسكرية الأمريكية، وكانت الشكوك قد اتجهت بداية إلى ارهابين دوليين الا ان الحقيقة تجلت بعد ذلك في ان المتسللين هما مراهقان كانا يعبثان بجهاز الحاسب الآلي في منزلهما (Wilson,2000).

وفي عام (١٩٩٧م) قام مراهق بالتسلل إلى نظام مراقبة حركة الملاحة الجوية في مطار ماشيتيوشش (Massachusetts) مما ادى إلى تعطيل نظام الملاحة الجوية وأنظمة أخرى حيوية لمدة ستة ساعات، وبالرغم من فداحة الضرر الذي تسبب فيه الا ان عقوبته اقتصرت على وضعه تحت الرقابة لمدة سنتين مع الزامه باداء خدمة للمجتمع لمدة (٢٥٠) يوما (Wilson,2000)، وبهذا فان القانون الامريكي يلعب دورا غير مباشر في تشجيع المراهقين على اعمال التسلل حيث نادرا ما يعاقب المتسللين دون سن الثامنة عشر، كما يساهم أولياء امور المراهقين في ذلك ايضا حيث يعتبرون ابنائهم اذكياء اذا مارسوا انشطة حاسوبية تتعلق بالتسلل إلى اجهزة الاخرين (Koerner,1999).

وأوضحت دراسة اجريت عام (١٩٧٩م) على عدد (٥٨١) طالب جامعي امريكي ان (٥٠٪) منهم قد اشترك في اعمال غير نظامية اثناء استخدام الإنترنت خلال ذلك العام، وأن (٤٧) طالبا أو مانسبته (٧,٣٪) سبق وقبض عليه في جرائم تتعلق بالحاسب الآلي، وأن (٧٥) طالبا أو مانسبته (١٣,٣٪) قبض على اصدقائهم في جرائم تتعلق بالحاسب الآلي (Skinner & Fream, 1997).

فالعقوبات الحالية لاتساعد على تقليص الارتفاع المستمر للجرائم المتعلقة بالحاسب الآلي، ففي خلال عام واحد تضاغفت تلك الجرائم على مستوى الولايات المتحدة الأمريكية، ففي عام (١٩٩٩م) تحرت وكالة المباحث الفدرالية (FBI) عن (٨٠٠) حالة تتعلق بالتسلل(Hacking) وهو ضعف عدد الحوادث التي قامت بالتحرى عنها في العام السابق أي عام (١٩٩٨م)، أما الهجوم على شبكات الحاسب الآلي على الإنترنت فقد تضاعف (٣٠٠٪) في ذلك العام ايضا (Koerner,1999).

وللحد من تزايد عمليات التسلل(Hacking) ونظرا لان المتسللين عادة يطورون تقنياتهم بصفة مستمرة ويملكون مهارات متقدمة، فقد اضطر مسئولوا أمن الحاسبات الآلية وشبكات الإنترنت وكذلك رجال الامن على الاستعانة بخبرات بعض محترفين التسلل ليستطيعوا تطوير نظم الحماية ضد المتسللين (Hackers)، وعلى سبيل المثال يرسل مسئولي امن الحاسبات اسئلة تتعلق باحدث سبل الحماية لغرف الدردشة الخاصة بمواقع المتسللين أو ما تعرف باسم (hacker internet chat room) ولطلب نصائح تقنية حول أحدث سبل الحماية (Staff, 2000, February 17).

بل ان وكالة المباحث الفدرالية (FBI) استعانت ايضا بخبراء في التسلل (Hackers) لتدريب منسوبي الوكالة على طرق التسلل (Hacking) لتنمية خبراتهم وقدراتهم في هذا المجال وليستطيعوا مواكبة خبرات وقدرات المتخصصي (Hackers)، ومنهم أحد أشهر المتسللين (Hackers) ويدعى (Brian Martin) والمشهور باسم (Jericho) وهو متهم حاليا بالتسلل والعبث بمجتويات الصفحة الرئيسية لصحيفة (New Youk Times) على شبكة الإنترنت (Staff, 2000 April 2).

واكدت وحدة الخدمات السرية الأمريكية (The US Secret Service) ان الجرائم المنظمة تتجه نحو استغلال التسلل (Hacking) للحصول على المعلومات اللازمة لتنفيذ مخططاتها الإجرامية (Thomas,2000).

وفي خبر نشرته صحيفة لوس انجلوس تايمز أوضحوا ان متسللين قاموا باقتحام نظام الحاسب الآلي الذي يتحكم في تدفق اغلب الكهرباء في مختلف انحاء ولاية كاليفورنيا الأمريكية (موقع ارابيا،٢٠٠١/٦/١٠م).

-2 . الاغراق بالرسائل :
يلجأ بعض الاشخاص إلى إرسال مئات الرسائل إلى البريد الإلكتروني لشخص ما بقصد الاضرار به حيث يؤدى ذلك إلى تعطل الشبكة وعدم امكانية استقبال أي رسائل فضلا عن امكانية انقطاع الخدمة وخاصة اذا كانت الجهة المضررة من ذلك هي مقدمة خدمة الإنترنت مثلا حيث يتم ملء منافذ الاتصال (Communication-Ports) وكذلك قوائم الانتظار (Queues) مما ينتج عنه انقطاع الخدمة وبالتالي تكبد خسائر مادية ومعنوية غير محدودة، ولذلك لجأت بعض الشركات إلى تطوير برامج تسمح باستقبال جزء محدود من الرسائل في حالة تدفق اعداد كبيرة منها(داود،١٤٢٠هـ:٩٣).
واذا كان هذا هو حال الشركات الكبيرة فلنا ان نتصور حال الشخص العادي اذا تعرض بريده لمحاولة الاغراق بالرسائل حيث لن يصمد بريده طويلا امام هذا السيل المنهمر من الرسائل عديمة الفائدة أو التي قد يصاحبها فيروسات أو صور أو ملفات كبيرة الحجم، خاصة اذا علمنا ان مزود الخدمة عادة يعطي مساحة محددة للبريد لا تتجاوز عشرة ميقا كحد اعلى.

٣. الفيروسات الحاسب الآلية :
الفيروسات الحاسب الآلييية هي احدى انواع البرامج الحاسب الآلية الا أن الأوامر المكتوبة في هذه البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما أو حتى مجرد فتح البرنامج الحامل لفيروس أو الرسالة البريدية المرسل معها الفيروس اصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به.
وقد عرفها احد خبراء الفيروسات (Fred Cohen) بانها نوع من البرامج التي تؤثر في البرامج الأخرى بحيث تعدل في تلك البرامج لتصبح نسخة منها، وهذا يعنى ببساطة أن الفيروس ينسخ نفسه من حاسب آلي إلى حاسب آلي اخر بحيث يتكاثر باعداد كبيرة (Highley,1999).
ويمكن تقسيم الفيروسات إلى خمسة انواع :
الأول: فيروسات الجزء التشغيلي للاسطوانة كفيروس (Brain) و(Newzeland)
الثاني: الفيروسات المتطفلة كفيروس (Cascade) وفيروس (Vienna).
الثالث: الفيروسات المتعددة الانواع كفيروس (Spanish-Telecom) وفيروس (Flip)
الرابع: الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوس أو الوندوز
الخامس: يعرف بحصان طرواده وهذا النوع يصنفه البعض كنوع مستقل بحد ذاته ،الا انه ادرج في تقسيمنا هنا كاحد انواع الفيروسات، وينسب هذا النوع إلى الحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاء سلمي الا أن اثره التدميري خطير. وتعمل الفيروسات على اخفاء نفسها عن البرامج المضادة للفيروسات باستخدام طرق تشفير لتغيير اشكالها لذلك وجب تحديث برامج الخاصة بمكافحة الفيروسات بصفة دائمة (عيد،١٤١٩هـ : ٦٣-٦٦).
وهناك فريق من الخبراء يضع تقسيما مختلفا للفيروسات على أساس المكان المستهدف بالاصابة داخل جهاز الكمبيوتر ويرون أن هناك ثلاثة أنواع رئيسية من الفيروسات وهي فيروسات قطاع الاقلاع (Boot Sector) وفيروسات الملفات (File Injectors) وفيروسات الماكرو (Macro Virus). كما أن هناك من يقوم بتقسيم الفيروسات إلى فيروسات الاصابة المباشرة (Direct action) وهي التي تقوم بتنفيذ مهمتها التخريبية فور تنشيطها أو المقيمة (staying) وهي التي تظل كامنة في ذاكرة الكمبيوتر وتنشط بمجرد أن يقوم المستخدم بتنفيذ أمر ما، ومعظم الفيروسات المعروفة تندرج تحت هذا التقسيم، وهناك أيضا الفيروسات المتغيرة (Polymorphs) التي تقوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلل برامج مكافحة الفيروسات (الجزيرة ،٢٠٠٠).

ومن الجرائم المتعلقة بارسال فيروسات حاسوبية قيام شخص امريكي يدعى (Robert Morris) بارسال بتاريخ الثاني من نوفمبر عام (١٩٨٨م) عبر الإنترنت وقد كرر الفيروس نفسه عبر الشبكة بسرعة فاقت توقع مصمم الفايروس وادى ذلك إلى تعطيل ما يقارب من (٦٢٠٠) حاسب إلى مرتبط بالإنترنت، وقدرت الاضرار التي لحقت بتلك الأجهزة بمئات الملايين من الدولارات. ولو قدر لمصمم الفيروس تصميمه ليكون اشد ضررا لكان قد لحقت اضرار أخرى لا يمكن حصرها بتلك الاجهزة، وقد حكم على المذكور بالسجن ثلاثة سنوات بالرغم من دفاع المذكور بانه لم يكن يقصد احداث مثل تلك الاضرار(Morningstar, 1998).

كيف يتم اقتحام الجهاز :

لتتم عملية الاقتحام يجب زرع حصان طروادة في جهاز الضحية بعدة طرق منها:

١. يرسل عن طريق البريد الإلكتروني كملف ملحق حيث يقوم الشخص بإستقباله وتشغيله وقد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى.

٢. عند استخدام برنامج المحادثة الشهير (ICQ) وهو برنامج محادثة انتجة اسرائيل.

٣.عند تحميل برنامج من أحد المواقع غير الموثوق بها وهي كثيرة جدا.

٤.طريقة أخرى لتحميله تتلخص في مجرد كتابة كوده على الجهاز نفسه في دقائق قليلة.

٥.في حالة اتصال الجهازبشبكة داخلية أو شبكة إنترانت.

٦.يمكن نقل الملف أيضا بواسطة برنامج (FTP) أو (Telnet) الخاصة بنقل الملفات.

٧.كما يمكن الاصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكروز الموجود في برامج معالجة النصوص (Nanoart,2000).

وبصفة عامة فإن برامج القرصنه تعتمد كليا على بروتوكول الـ (TCP/IP) وهناك ادوات (ActiveX) مصممه وجاهزة لخدمة التعامل بهذا البروتوكول ومن اشهرها (WINSOCK.OCX) لمبرمجي لغات البرمجة الداعمة للتعامل مع هذه الادوات. ويحتاج الامر إلى برنامجين، خادم في جهاز الضحية وعميل في جهاز المتسلل حيث يقوم الخادم بفتح منفذ في الجهاز الضحية ويكون هذا المنفذ معروف من قبل العميل اصلا في حين يكون برنامج الخادم في حالة انتظار لحظة محاولة دخول المخترق لجهاز الضحية حيث يتعرف برنامج الخادم (server) على اشارات البرنامج المخترق ويتم الاتصال ومن ثم يتم عرض محتويات جهاز الضحية كاملة لدى المخترق حيث يتمكن من العبث بها أو الاستيلاء على ما يريد منها . فالمنافذ (Ports) يمكن وصفها ببوابات للجهاز وهناك وهناك ما يقارب الـ(٦٥٠٠٠) منفذ تقريبا في كل جهاز يميز كل منفذ عن الآخر برقم خاص ولكل منها غرض محدد، فمثلا المنفذ (٨٠٨٠) يخصص احيانا لمزود الخدمة، وهذه المنافذ غير مادية مثل منفذ الطابعة، وتعتبر جزء من الذاكرة لها عنوان معين يتعرف عليها الجهاز بأنها منطقة إرسال واستقبال البيانات، وكل ما يقوم به المتسلل هو فتح احد هذه المنافذ للوصول لجهاز الضحية وهوما يسمى بطريقة الزبون/الخادم (Client\Server) حيث يتم ارسال ملف لجهاز الضحية يفتح المنافذ فيصبح جهاز الضحية (server) وجهاز المتسلل (Client) ومن ثم يقوم المتسلل بالوصول لهذه المنافذ باستخدام برامج كثيرة متخصصة كبرنامج (NetBus) أو (NetSphere) ولعل الخطورة الاضافية تكمن في انه عند دخول المتسلل إلى جهاز الضحية فانه لن يكون الشخص الوحيد الذي يستطيع الدخول لذلك الجهاز حيث يصبح ذلك الجهاز مركزا عاما يمكن لأي شخص الدخول عليه بمجرد عمل مسح للمنافذ (Portscanning) عن طريق احد البرامج المتخصصة في ذلك.

خطورة برامج حصان طروادة:

بداية تصميم هذه البرامج كان لأهداف نبيلة كمعرفة ما يقوم به الأبناء أو الموظفون على جهاز الحاسب في غياب الوالدين أو المدراء وذلك من خلال ما يكتبونه على لوحة المفاتيح، الا

انه سرعان ما اسيئ استخدامه. وتعد هذه البرامج من أخطر البرامـج المستخـدمه من قبل المتسللين كونه يتيح للدخيل الحصول على كلمات المرور (passwords) وبالتالي الهيمنه على الحاسب الآلي بالكامل. كما أن المتسلل لن يتم معرفته أو ملاحظته كونه يستخدم الطرق المشروعة التي يستخدمها مالك الجهاز. كما تكمن الخطورة ايضا في أن معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات إضافة إلى أن الطبيعة الساكنة لحصان طروادة يجعلها اخطر من الفيروسات فهي لا تقوم بتقديم نفسها للضحية مثلما يـقوم الفيروس الذي دائما ما يمكن ملاحظته من خلال الإزعاج أو الأضرار التي يقوم بها للمستخدم وبالتالي فإنه لا يمكن الشعور بهذه الاحصنة أثناء أدائها لمهمتها التجسسية وبالتالي فإن فرص إكتشافها والقبض عليها تكاد تكون معدومه(Nanoart,2000).

أهم المنافذ المستخدمة لاختراق الجهاز:

إذن فأهم مورد لهذه الاحصنة هي المنافذ (Ports) التي تقوم بفتحها في جهاز الضحية ومن ثم التسلل منها إلى الجهاز والعبث بمحتوياته. فما هي هذه المنافذ ؟

سنحاول هنا التطرق بشكل اجمالي إلى أهم المنافذ التي يمكن استخدامها من قبل المتسللين والبرامج المستخدمة في النفاذ من هذه المنافذ :

راجع هذا الموقع (http://www.nanoart.f2s.com/hack/ports3.htm)

ثالثا: الجرائم المالية

تشمل جرائم السطو على أرقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمة المنظمة، المخدرات، غسيل الاموال، ولعل جرائم هذا القسم أوضح من ناحية معرفة كونها مُجَرَمة حيث لا تختلف في نتيجتها عن الجرائم التقليدية التي تحمل نفس المسمى والتي يعرف الجميع انها مخالفة للنظام وللشرع كونهم من الجرائم التي اشتهر محاربتها جنائيا. ونظرا للاختلاف البسيط في تصنيف كل جريمة من جرائم هذا القسم فسيتم توضيح التكييف الشرعي والقانوني لكل جريمة بشكل مفصل.

١. جرائم السطو على أرقام البطاقات الائتمانية:

بدأ مفهموم التجارة الإلكترونية ينتشر في السبعينات الميلادية وذلك لسهولة الاتصال بين الطرفين ولامكانية اختزال العمليات الورقية والبشرية فضلا عن السرعة في ارسال البيانات وتخفيض تكلفة التشغيل والأهم هو ايجاد اسواق اكثر اتساعا. ونتيجة لذلك فقد تحول العديد من شركات الاعمال إلى استخدام الإنترنت والاستفادة من مزايا التجارة الإلكترونية، كما نحول تبعا لذلك الخطر الذي كان يهدد التجارة السابقة ليصبح خطرا متوافقا مع التجارة الإلكترونية.

فالاستيلاء على بطاقات الائتمان عبر الإنترنت امر ليس بالصعوبة بمكان اطلاقا، فـ" لصوص بطاقات الائتمان مثلا يستطيعون الان سرقة مئات الالوف من ارقام البطاقات في يوم واحد من خلال شبكة الإنترنت، ومن ثم بيع هذه المعلومات للاخرين " (داود، ١٤٢٠هـ: ٧٣)، وقد وقعت بالفعل عدة حوادث ومن ذلك حادثة شخص الماني قام بالدخول غير المشروع إلى احد مزود الخدمات واستولى على ارقام بطاقات ائتمانية الخاصة بالمشتركين ومن ثم هدد مزود الخدمة بافشاء ارقام تلك البطاقات ما لم يستلم فدية وقد تمكنت الشرطة الالمانية من القبض عليه. كما قام شخصان في عام (١٩٩٤م) بانشاء موقع على الإنترنت مخصص لشراء طلبات يتم بعثها فور تسديد قيمتها الكترونيا، ولم تكن الطلبات لتصل اطلاقا حيث كان الموقع وهمي قصد منه النصب والاحتيال وقد قبض على مؤسسيه لاحقا (موثق في عبدالمطلب، ٢٠٠١م : ٨٥)

واثبت شبكة (MSNBC) عمليا سهولة الحصول على ارقام بطاقات الائتمان من الإنترنت، حيث قامت بعرض قوائم تحتوي على اكثر من (٢٥٠٠) رقم بطاقة ائتمان حصلت عليها من سبعة مواقع للتجارة الإلكترونية باستخدام قواعد بيانات متوفرة تجاريا، ولم يكن يصعب على اي متطفل استخدام ذات الوسيلة البدائية للاستيلاء على ارقام تلك البطاقات واستخدامها في عمليات شراء يدفع قيمتها اصحابها الحقيقين. ويقترح بعض الخبراء باستخدام بطاقة ائتمان

خاصة بالإنترنت يكون حدها الائتماني معقول بحيث يقلل من مخاطر فقدانها والاستيلاء غير المشروع عليها، وهو الامر الذي بدأت بعض البنوك الدولية والمحلية في تطبيقه اخيرا (عبدالمطلب،٢٠٠١م : ٨٦ – ٩٠).
ويتعدى الامر المخاطر الأمنية التي تتعرض لها بطاقات الائتمان فنحن في بداية ثورة نقدية تعرف باسم النقود الإلكترونية (Electronic Cach) أو (Cyber Cash) والتي يتنبأ لها ان تكون مكملة للنقود الورقية والبلاستيكية (بطاقات الائتمان) وأن يزداد الاعتماد عليها والثقة بها، كما ان هناك الاسهم والسندات الإلكترونية المعمول بها في دول الاتحاد الأوروبي والتي اقر الكونجرس الامريكي التعامل بها في عام ١٩٩٠م، وبالتالي فان التعامل معها من خلال الإنترنت سيواجه مخاطر امنية ولا شك.
ولذلك لجأت بعض الشركات والبنوك إلى العمل سويا لتجاوز هذه المخاطر كالاتفاق الذي وقع بين مؤسسة هونج كونج وشنغهاي البنكية (HSBC) وهي من اكبر المؤسسات المصرفية في هونج كونج وشركة كومباك للحاسب لتطوير أول نظام الي آمن للتجارة الالتكرونية والذي يمنح التجار خدمة نظام دفع امن لتمرير عمليات الشراء عبر الإنترنت (داود، ١٤٢٠هـ : ١٢٣ – ١٢٤).
وجرائم السطو على أرقام البطاقات الائتمانية مُجَّرمة شرعا وقانونا حيث تصنف ضمن جرائم السرقات، "فالشارع الاسلامي يرغب في المحافظة على اموال الناس وصيانتها من كل اعتداء غير مشروع بحيث يهدد الامن والاستقرار" (فرحات،١٤٠٤هـ:٢٩).
والسرقة من الكبائر المحرمة التي نصت الايات القرآنية والاحاديث النبوية على تحريمها ووضعت عقوبة رادعة لمرتكبها. قال تعالى في سورة المائدة (َالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءً بِمَا كَسَبَا نَكَالًا مِنْ اللَّهِ وَاللَّهُ عَزِيزٌ حَكِيمٌ (٣٨))
بل لعن رسول الله السارق نظراً لشناعة فعله وعظيم جرمه، ففي الحديث الذي رواه البخاري في صحيحه عن أبي هريرة رضي الله عنه عن النبي صلى الله عليه وسلم قال: " لعن الله السارق، يسرق البيضة فتقطع يده، ويسرق الحبل فتقطع يده".
كما نفى الحبيب المصطفى عليه الصلاة والسلام صفة الايمان عن السارق فروى البخاري في صحيحه عن ابن عباس رضي الله عنهما، عن النبي صلى الله عليه وسلم قال: " لا يزني الزاني حين يزني وهو مؤمن، ولا يسرق السارق حين يسرق وهو مؤمن".

٢. القمار عبر الإنترنت:
كثيرا ما تتداخل عملية غسيل الاموال مع اندية القمار المنتشرة، الامر الذي جعل مواقع الكازيهونات الافتراضية على الإنترنت محل اشتباه ومراقبة من قبل السلطات الأمريكية.
وبالرغم من ان سوق القمار في امريكا يعتبر الاسرع نموا على الاطلاق الا ان المشكلة القانونية التي تواجه اصحاب مواقع القمار الافتراضية على الإنترنت انها غير مصرح لها حتى الان في امريكا بعكس نوادي القمار الحقيقية كالمنتشرة في لاس فيجاس وغيرها، ولذلك يلجأ بعض اصحاب تلك المواقع الافتراضية على الإنترنت إلى انشائها وادارتها من اماكن مجاورة لامريكا وخاصة في جزيرة انتيجوا على الكاريبي.
ويوجد على الإنترنت اكثر من الف موقع للقمار يسمح لمرتاديه من مستخدمى الإنترنت ممارسة جميع انواع القمار التي توفرها المواقع الحقيقية، ومن المتوقع ان ينفق الامريكيون ما يزيد عن (٦٠٠) مليار دولار سنويا في اندية القمار وسيكون نصيب مواقع الإنترنت منها حوالي مليار دولار.
وقد حاول المشرعون الامريكيون تحريك مشروع قانون يمنع المقامرة عبر الإنترنت ويسمح بملاحقة اللذين يستخدمون المقامرة السلكية أو اللذين يروجون لها سواء كانت هذه المواقع في امريكا أو خارجها (عبدالمطلب، ٢٠٠١م : ٧٨ – ٨٢).

فإذا كان هذا هو حال القمار ونظرة القوانيين الوضعية له، فما هو نظرة الشرع له وهل يوجد في تعاليم الدين الاسلامي ما يُجرِّم لعب القمار ويجعله من الافعال المحرمة شرعا والمعاقب عليه قانونا؟

ينظر الاسلام إلى القمار كمحظور شرعي منهي عن فعله وماعقب على ارتكابه، وقد وردت ادلة متعددة في كتاب الله وفي كتب الاحاديث، اما دليل تحريم القمار من القرآن فهو قوله تعالى في سورة المائدة (يَاأَيُّهَا الَّذِينَ آمَنُوا إِنَّمَا الْخَمْرُ وَالْمَيْسِرُ وَالْأَنصَابُ وَالْأَزْلَامُ رِجْسٌ مِنْ عَمَلِ الشَّيْطَانِ فَاجْتَنِبُوهُ لَعَلَّكُمْ تُفْلِحُونَ (٩٠))

ولم يكتفي الشرع بالنهي عن هذا الفعل بل وضح لاتباعه ان هذا العمل انما هو من اعمال الشيطان التي يسعى من خلالها إلى ايقاع العدأوة والبغضاء بين الناس ووضح ان في اجتاب هذا الفعل فلاح وصلاح وفوز في الدنيا والاخرة ، قال تعالى في سورة المائدة: (إِنَّمَا يُرِيدُ الشَّيْطَانُ أَنْ يُوقِعَ بَيْنَكُمْ الْعَدَاوَةَ وَالْبَغْضَاءَ فِي الْخَمْرِ وَالْمَيْسِرِ وَيَصُدَّكُمْ عَنْ ذِكْرِ اللَّهِ وَعَنْ الصَّلَاةِ فَهَلْ أَنْتُمْ مُنتَهُونَ (٩١))

واتفق المفسرون على ان الميسر هو القمار فورد توضيح كلمة الميسر في تفسير الجلالين بانها القمار، اما ابن كثير فقد أورد في تفسيره لهذه الاية، حديثاً رواه احمد في مسنده عن ابي هريرة رضي الله عنه ان امير المؤمنين عمر بن الخطاب رضي الله عنه فسَّر الميسر هنا بالقمار، كما ورد تفسير كلمة الميسر ايضا في فتح القدير بانها قمار العرب بالازلام، وكذلك اكد تفسير البغوي بان المراد بالميسر هو القمار، اما البيضأوي فقد وضح ان الميسر سمي به القمار لانه اخذ مال الغير بيسر.

وفي كتب الحديث ورد ذكر القمار ايضا فقد ورد في مصنف ابن أبي شيبة عن وكيع قال حدثنا حماد بن نجيح قال: رأيت ابن سيرين مر على غلمان يوم العيد المربد و هم يتقامرون بالجوز، فقال: يا غلمان! لا تقامروا فإن القمار من الميسر، كما أورد في مصنفه ايضا عن ابن سيرين قال: كل شيء فيه قمار فهو من الميسر، وفيه ايضاً عن عبد الله بن عمرو قال بالنرد قماراً كان كآكل لحم الخنزير، ومن لعب بها من غير قمار كان كالمدهن بودك الخنزير. كما أخبر عبد الرزاق في مصنفه عن معمر عن ليث عن مجاهد قال: الميسر القمار كله، حتى الجوز الذي يلعب به الصبيان.

٣-. تزوير البيانات:

تعتبر من اكثر جرائم نظم المعلومات انتشارا فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من اشكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها أو إضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك. وقد وقعت حادثة في ولاية كاليفورنيا الأمريكية حيث عمدت مدخلة البيانات بنادي السيارات وبناء لاتفاقية مسبقة بتغيير ملكية السيارات المسجلة في الحاسب الآلي بحث تصبح باسم احد لصوص السيارات والذي يعمد إلى سرقة السيارة وبيعها وعندما يتقدم مالك السيارة للابلاغ يتضح عدم وجود سجلات للسيارة باسمه وبعد بيع السيارة تقوم تلك الفتاة باعادة تسجيل السيارة باسم مالكها وكانت تتقاضي مقابل ذلك مبلغ مائة دولار واستمرت في عملها هذا إلى ان قبض عليها، وفي حادثة الخرى قام مشرف تشغيل الحاسب باحد البنوك الأمريكية بعملية تزوير حسابات اصدقائه في البنك بحيث تزيد ارصدتهم ومن ثم يتم سحب تلك المبالغ من قبل اصدقائه وقد نجح في ذلك وكان ينوى التوقف قبل موعد المراجعة الدورية لحسابات البنك الا ان طمع اصدقاءه اجبره على الاستمرار إلى ان قبض عليه (داود، ١٤٢٠هـ :٤٥- ٤٧).

ومما لاشك فيه ان البدء التدريجي في التحول إلى الحكومات الإلكترونية سيزيد من فرص ارتكاب مثل هذه الجرائم حيث سترتبط الكثير من الشركات والبنوك بالإنترنت مما يسهل الدخول على تلك الأنظمة من قبل محترفي اختراق الأنظمة وتزوير البيانات لخدمة اهدافهم الإجرامية. وجرائم التزوير ليست بالجرائم الحديثة، ولذا فانه لاتخلوا الأنظمة من قوانيين

واضحة لمكافحتها والتعامل معها جنائيا وقضائيا و" تكفي التشريعات الحالية لتجريمها وتحديد العقوبة عليها" (داود ، ١٤٢١هـ : ٦٧).
وعالجت أنظمة المملكة العربية السعودية جرائم التزوير بشكل مفصل حيث صدر المرسوم الملكي رقم (١١٤) وتاريخ ١٣٨٠/١١/٢٦هـ بالمصادقة على نظام مكافحة التزوير، ومن ثم تم التعديل على هذا النظام ليواكب المستجدات وذلك بالمرسوم الملكي رقم (٥٣) وتاريخ ١٣٨٢/١١/٥هـ،كما صدر نظام جزائي خاص بتزوير وتقليد النقود وذلك بالمرسوم الملكي رقم (١٢) وتاريخ١٣٧٩/٧/٢٠هـ(موقع السوق الخليجي، ١٤٢٣هـ).

٤-. الجرائم المنظمة*:

يتبادر إلى الذهن فور التحدث عن الجريمة المنظمة عصابات المافيا كون تلك العصابات من اشهر المؤسسات الإجرامية المنظمة والتي بادرت بالاخذ بوسائل التقنية الحديثة سواء في تنظيم أو تنفيذ اعمالها، ومن ذلك انشاء مواقع خاصة بها على شبكة الإنترنت لمساعدتها في ادارة العمليات وتلقي المراسلات واصطياد الضحايا وتوسيع اعمال وغسيل الاموال، كما تستخدم تلك المواقع في انشاء مواقع افتراضية تساعد المنظمة في تجاوز قوانين بلد محدد بحيث تعمل في بلد اخر يسمح بتلك الانشطة.
ويوجد على الشبكة (٢١٠) موقع يحتوي اسم نطاقها على كلمة مافيا، في حين يوجد (٢٤) موقعا يحتوى على كلمة مافيا، كما وجد (٤) مواقع للمافيا اليهودية. وقد خصص بعض هذه المواقع للاعضاء فقط ولم يسمح لغيرهم بتصفح تلك المواقع في حين سمحت بعض المواقع للعامة بتصفح الموقع وقامت مواقع أخرى بوضع استمارة تسجيل لمن يرغب في الانضمام إلى العصابة من الاعضاء الجدد (الجنيدي(أ)، ١٩٩٩م : ٣٦).
والجريمة المنظمة ليست وليدة التقدم التقني وإن كانت استفادت كثيرا منه فـ" الجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنلوجيا والعولمة أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان وأن ما أصبح إنتشارها على نطاق واسع وكبير وأصبحت لاتحدها الحدود الجغرافية"(اليوسف، ١٤٢٠هـ ، ص : ٢٠١)، كما أستغلت عصابات الجريمة المنظمة " الامكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة " (حبوش،١٤٢٠هـ: ٢٥٣).
وهناك من يرى ان الجريمة المنظمة والارهاب هما وجهان لعملة واحدة، فأوجه التشابه بينهما كبير حيث يسعى كلاهما إلى إفشاء الرعب والخوف، كما انهما يتفقان في اسلوب العمل والتنظيم وقد يكون اعضاء المنظمات الارهابية هم اساساً من محترفي الجرائم المنظمة حيث يسعون للاستفادة من خبراتهم الإجرامية في التخطيط والتنفيذ، فهناك صلة وتعاون وثيق بينهما (عزالدين، ١٤١٤هـ : ٢٣- ٣٥).
وحظيت مكافحة الجريمة المنظمة باهتمام دولي بدأ بمؤتمر الامم المتحدة السابع عام (١٩٨٥م) لمنع الجريمة حيث اعتمد خطة عمل ميلانو والتي أوصت بعدة توصيات حيال التعامل مع الجريمة المنظمة والقضاء عليها.
وتبع ذلك الاجتماع الاقاليمي التحضيري عام (١٩٨٨م) الذي أقر فيه المبادئ التوجيهية لمنع الجريمة المنظمة ومكافحتها، ثم المؤتمر الثامن لمنع الجريمة بفنزويلا عام (١٩٩٠م)، فالمؤتمر الوزاري العالمي المعنى بالجريمة المنظمة عبر الوطنية في نابولي بايطاليا عام (١٩٩٤م) والذي عبّر عن ارادة المجتمع الدولي بتعزيز التعاون الدولي واعطاء أولوية عليا لمكافحة الجريمة المنظمة.
كما وضعت لجنة مكافحة الجرائم المنظمة مقترحات للعمل العربي في مكافحة الارهاب والتي وافق عليها مجلس وزراء الداخلية العرب في دورته السادسة، وفي عام (١٩٩٦م) وافق المجلس في دورته الثالثة عشر على مدونة سلوك طوعية لمكافحة الارهاب، ووافق في عام (١٩٩٧م) وفي الدورة الرابعة عشر على استراتيجية عربية لمكافحة الارهاب وفي عام

(١٩٩٨م) تم اقرار الاتفاقية العربية لمكافحة الارهاب من قبل مجلس وزراء الداخلية والعدل العرب (عيد، ١٤١٩هـ :٧٧-١٩٤).

٥-. تجارة المخدرات عبر الإنترنت:

كثيرا ما يحذّر أولياء الامور ابنائهم من رفقاء السوء خشية من تأثيرهم السلبي عليهم وخاصة في تعريفهم على المخدرات فالصاحب ساحب كما يقول المثل وهذا صحيح ولا غبار عليه ولكن وفي عصر الإنترنت اضيف إلى أولياء الامور مخأوف جديدة لا تقتصر على رفقاء السوء فقط بل يمكن ان يضاف اليها مواقع السوء - ان صح التعبير- ومن تلك المواقع طبعا المواقع المنتشرة في الإنترنت والتي لاتتعلق بالترويج للمخدرات وتشويق النشئ لاستخدانها بل تتعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافة اصنافها وأن واعها وبأبسط الوسائل المتاحة. والامر هنا لايحتاج إلى رفاق سوء بل يمكن للمراهق الانزواء في غرفته والدخول إلى اي من هذه المواقع ومن ثم تطبيق ما يقرأه ويؤكد هذه المخأوف أحد الخبراء التربوين في بتسبيرج بالولايات المتحدة والذي أكد إن ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات وانترنت.

ولا تقتصر ثقافة المخدرات على تلك المواقع فقط بل تسأهم المنتديات وغرف الدردشة في ذلك ايضا. وبالرغم من انتشار المواقع الخاصة بالترويج للمخدرات وتعليم كيفية صنعها الا ان هذه المواقع لم تدق جرس الانذار بعد ولم يهتم باثارها السلبية وخاصة على النشئ كما فعلته المواقع الاباحية وخاصة في الدول التي تعرف باسم الدول المتقدمة.

وقد اعترف الناطق الرسمي للتحالف المناهض للمخدرات بانهم خسروا الجولة الأولي في ساحة الإنترنت حيث لم يطلق موقعهم الخاص على الشبكة http://www.cadca.org الا منذ عامين فقط.

وبالإضافة إلى هذا الموقع توجد مواقع أخرى تحارب المخدرات وتساعد المدمنين على تجاوز محنتهم ومن ذلك الموقع الخاص بجماعة (Join-Together) وعنوانهم على النت هو http://192.12.191.21 إلا أن هذه المواقع قليلة العدد والفائدة مقارنة بكثرة وقوة المواقع المضادة (الجنيدي(ب)، ١٩٩٩م : ٣٩-٤٠).

واهتمت دول العالم قاطبة بمكافحة جرائم المخدرات وعقدت المؤتمرات والاتفاقيات الدولية المختلفة ومنها الاتفاقية الوحيدة لمكافحة المخدرات عام (١٩٦١م)، اتفاقية المؤثرات العقلية عام (١٩٧١م)، واتفاقية الامم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية عام (١٩٨٨م).

وعلى المستوى العربي تم عام (١٩٩٦م) اقرار الاتفاقية العربية لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية، كما تم عام (١٩٨٦م) اقرار القانون العربي النموذجي الموحد للمخدرات.

اما على المستوى المحلي فقد صدر نظام مكافحة الاتجار بالمواد المخدرة في المملكة العربية السعودية بقرار مجلس الوزراء رقم (١١) عام (١٣٧٤هـ) والحق به قرار هيئة كبار العلماء رقم (١٣٨) وتاريخ ١٤٠٧/٦/٢٠هـ الخاص باعدام مهربي المخدرات أو من يقبض عليه في قضية ترويج للمرة الثانية، والموافق عليه بالامر السامي رقم (٤/ب/٩٦٦) وتاريخ ١٤٠٧/٧/١٠هـ (عيد، ١٤٢٢هـ :٩٤-١١٠)

٦-. غسيل الاموال :

مصطلح حديث نسبيا ولم يكن معروفا لرجال الشرطة فضلا عن العامة وقد بدأ استخدام المصطلح في امريكا نسبة إلى مؤسسات الغسيل التي تملكها المافيا، وكان أول استعمال قانوني لها في عام (١٩٣١م) إثر محاكمة لاحد زعماء المافيا تمت في امريكا واشتملت مصادرة اموال قيل انها متأتية من الاتجار غير المشروع بالمخدرات.

واختلف الكثير في تعريف غسيل الاموال وقد يكون التعريف الاشمل هو " أي عملية من شأنها اخفاء المصدر غير المشروع الذي اكتسبت منه الاموال"(عيد، ١٤٢٢هـ: ١٢٤).

ومن البديهي ان ياخذ المجرمون باحدث ما توصلت اليه التقنية لخدمة أنشطتهم الإجرامية ويشمل ذلك بالطبع طرق غسيل الاموال التي استفادت من عصر التقنية فلجأت إلى الإنترنت لتوسعة وتسريع اعمالها في غسيل اموالها غير المشروعة، ويجد المتصفح للانترنت مواقع متعددة تتحدث عن غسيل اموال ومنها الموقع :http://www.laundryman.u.net.com

كما يجد ولا شك ايضا المواقع التي تستخدم كساتر لعمليات غسيل الاموال ومنها المواقع الافتراضية لنوادي القمار والتي قام مكتب المباحث الفدرالية (FBI) الامريكي بمراقبة بعض هذه المواقع واتضح انها تتواجد في كاراكأو، جزر الانتيل، جزيرة أنتيجوا وجمهورية الدومينكان وقد اسفرت التحريات التي استمرت خمسة اشهر عن اعتقالات واتهامات للعديد من مدراء تلك المواقع.

ومن المميزات التي يعطيها الإنترنت لعملية غسيل الاموال السرعة، اغفال التوقيع وأن عدام الحواجز الحدودية بين الدول، كما تسأهم البطاقات الذكية، والتي تشبه في عملها بطاقات البنوك المستخدمة في مكائن الصرف الآلية، في تحويل الاموال بواسطة المودم أو الإنترنت مع ضمان تشفير وتأمين العملية.

كل هذا جعل عمليات غسيل الاموال عبر الإنترنت تتم بسرعة اكبر وبدون ترك اي اثار في الغالب. ويقدر المتخصصون المبالغ التي يتم تنظيفها سنويا بـحوالي (٤٠٠) مليار دولار (عبدالمطلب،٢٠٠١م : ٦٨ - ٧٢).

وإلى عهد قريب لم تكن جرائم غسيل اموال تشكل جرما بذاتها إلى ان تضخمت الاموال المتحصلة من الجرائم وخاصة من تجارة المخدرات فاصدرت بعض الدول قوانين خاصة تسمح بتعقب وتجميد ومصادرة عائدات الجرائم الخطرة، فأصدرت الولايات المتحد الأمريكية عام (١٩٧٠م) قانون المنظمات القائمة على الابتزاز والنساء، وقانون منع ومكافحة جرائم اساءة إستخدام العقاقير المخدرة، كما اصدرت مصر عام (١٩٧١م) القانون رقم (٣٤) والخاص بتنظيم فرض الحراسة على الاموال المكتسبة بطرق غير مشروعة، كما اقر القانون العربي النموذجي الموحد للمخدرات الصادر عن مجلس وزراء الداخلية العرب عام (١٩٨٦م) مكافحة جرائم غسيل الاموال وخاصة في مادته التاسعة والاربعون والتي سمحت للمحكمة المختصة بحجز الاموال المتحصلة من تجارة المخدرات والتحقق من مصادر تلك الاموال. كما اصدرت بريطانيا وايرلندا عام (١٩٨٦م) قانون يسمح بمصادرة عائدات الجريمة. واصدرت استراليا عام (١٩٨٧م) قانونا يسمح بمصادرة اموال الشخص المدان في جرائم اتحادية.

ولم تتخلف المملكة العربية السعودية عن ركب محاربة جرائم غسيل الاموال فقد كانت المملكة من ضمن دول العالم الـ(١٠٦) اللذين وقعوا عام (١٩٨٨م) على اتفاقية الامم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية والتي كانت أول خطوة دولية مهمة لتعريف غسيل الاموال وتحديد الافعال الواجب تجريمها (عيد، ١٤١٩هـ : ٢٦٣-٣١٩)

رابعا: المواقع المعادية:

يكثر انتشار الكثير من المواقع غير المرغوب فيها على شبكة الإنترنت ومن هذه المواقع ما يكون موجها ضد سياسة دولة ما، أو ضد عقيدة أو مذهب معين أو حتى ضد شخص ما. وهي تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد أو الشخص المستهدف.

ففي المواقع السياسية المعادية يتم غالبا تلفيق الاخبار والمعلومات ولو زورا وبهتانا أو حتى الاستناد إلى جزيئ بسيط جدا من الحقيقة ومن ثم نسج الاخبار الملفقة حولها، وغالبا ما يعمد اصحاب تلك المواقع إلى انشاء قاعدة بيانات بعناوين اشخاص يحصلون عليها من الشركات التي تبيع قواعد البيانات تلك أو بطرق أخرى ومن ثم يضيفون تلك العناوين قسرا إلى قائمتهم البريدية ويبدأو في اغراق تلك العناوين بمنشوراتهم، وهم عادة يلجئون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضون له ولايصال اصواتهم إلى اكبر قدر ممكن.

اما المواقع المعادية للعقيدة فمنها ما يكون موجهاً من قبل اعداء حاقدين من اتباع الديانات الأخرى كالمواقع التي تنشئها الجاليات اليهودية أو النصرانية تحت مسميات اسلامية بقصد بث

معلومات خاطئة عن الاسلام والقرآن، أو بهدف الدعاية للاديان الأخرى ونشر الشبهه والافتراءت حول الاسلام ومن أمثلة هذه المواقع:
موقع http://www.answering-islam.org/
وموقع http://www.aboutislam.com/
وموقع http://www.thequran.com/
اما القسم الثاني من المواقع المعادية للعقيدة فهي المواقع التي يكون افرادها من ذات العقيدة واحدة ولكن يختلفون في المذاهب.
وهناك مواقع معادية لاشخاص أو جهات وهي قد تكون شبيهة وإلى حد كبير بالمواقع المخصصة للقذف التي سبق التحدث عنها سابقا في القسم الخاص بالجرائم الجنسية، حيث تهدف اساسا لتشويه سمعة الشخص أو الجهة ولذلك فسيكتفى بما سبق التطرق اليه في هذا المجال وسيركز على الحديث عن المواقع السياسية والدينية والتي لم يتم التطرق لها.

والمواقع المعادية بانواعها مخالفة نظامية وجريمة جنائية وتفصيل ذلك كالاتي:
أ. المواقع السياسية المعادية: قد ينظر البعض إلى إنشاء هذه المواقع كظاهرة حضارية تتمشي مع الديموقراطية والحرية الشخصية، وهذا غير صحيح فللديموقراطية والحرية الشخصية حدود يجب ان لاتتجاوزها والا اصبحت سوء ادب وبغي. وهناك ولا شك طرق واساليب يمكن معها التعبير عن الاراء الشخصية وضّحتها الشريعة الاسلامية قبل الديمقراطية الوضعية، وحددتها عاداتاتنا وتقاليدنا المنبثقة من قيمنا العربية الاصيلة في حين غفلت عنها قيم الدول الغربية وابسط هذه القواعد ان يكون النصح بالرفق واللين وبالكلمة الطيبة وليس بالشتم والقذف، قال تعالى في سورة النحل (ادْعُ إِلى سَبِيلِ رَبِّكَ بِالْحِكْمَةِ وَالْمَوْعِظَةِ الْحَسَنَةِ وَجَادِلْهُمْ بِالَّتِي هِيَ أَحْسَنُ إِنَّ رَبَّكَ هُوَ أَعْلَمُ بِمَنْ ضَلَّ عَنْ سَبِيلِهِ وَهُوَ أَعْلَمُ بِالْمُهْتَدِينَ (١٢٥)) وقال تعالى في سورة ال عمران (فَبِمَا رَحْمَةٍ مِنْ اللَّهِ لِنْتَ لَهُمْ وَلَوْ كُنْتَ فَظًّا غَلِيظَ الْقَلْبِ لَانْفَضُّوا مِنْ حَوْلِكَ فَاعْفُ عَنْهُمْ وَاسْتَغْفِرْ لَهُمْ وَشَاوِرْهُمْ فِي الْأَمْرِ فَإِذَا عَزَمْتَ فَتَوَكَّلْ عَلَى اللَّهِ إِنَّ اللَّهَ يُحِبُّ الْمُتَوَكِّلِينَ (١٥٩))، كما ان من الآداب ان يكون النقد أو النصيحة في السر لا في العلن وفي هذا يقول الامام الشافعي: تعمدني بنصحك في انفراد وجنبني النصيحة في الجماعة
فإن النصح بين الناس نوع من التوبيخ لا ارضى استماعه
وان خالفتني وعصيت قولي فلا تجزع إذا لم تعط طاعة
وهذه الاداب هي ابسط الاداب الواجب اتباعها مع العامة فما بالك مع ولي الامر الذي قرن الله طاعته بطاعة الله ورسوله - مالم يأمر ولي الامر بأمر مخالف لله – ولذلك فليس في إنشاء المواقع السياسية المعادية أي حرية رأي أو ديمقراطية بل هي سوء ادب ان لم يكن بغي يعاقب عليه الشرع بالقتل فـ" جريمة البغي موجهة إلى نظام الحكم والقائمين بأمره، وقد تشددت فيها الشريعة؛ لإن التساهل فيها يؤدي إلى الفتن والاضطرابات وعدم الاستقرار وهذا يؤدي بدوره إلى تأخر الجماعة وانحلالها. ولا شك ان عقوبة القتل أقدر العقوبات على صرف الناس عن هذه الجريمة التي يدفع اليها الطمع وحب الاستيلاء" (عودة، ١٤٠١هـ :٦٦٣).
والدليل على ان البغي محرم شرعا ومعاقب عليه بالقتل قوله تعالى في سورة الحجرات (وَإِنْ طَائِفَتَانِ مِنْ الْمُؤْمِنِينَ اقْتَتَلُوا فَأَصْلِحُوا بَيْنَهُمَا فَإِنْ بَغَتْ إِحْدَاهُمَا عَلَى الْأُخرى فَقَاتِلُوا الَّتِي تَبْغِي حَتَّى تَفِيءَ إِلى أَمْرِ اللَّهِ فَإِنْ فَاءَتْ فَأَصْلِحُوا بَيْنَهُمَا بِالْعَدْلِ وَأَقْسِطُوا إِنَّ اللَّهَ يُحِبُّ الْمُقْسِطِينَ(٩))، وفي الحديث الشريف الذي رواه مسلم "إنه ستكون هنّات وهنّات، فمن أراد أن يفرق أمر هذه الأمة، وهي جميع، فاضربوه بالسيف، كائناً من كان" كما ورد عن رسول الله صلى الله عليه وسلم حديثا رواه مسلم وابي داود واللفظ لابي دواد: عن عبد الله بن عمرو أن النبي صلى الله عليه و سلم قال"من بايع إماماً فأعطاه صفقة يده وثمرة قلبه فليطعمه ما استطاع، فإن جاء آخر ينازعه فاضربوا رقبة الآخر قلت: أنت سمعت هذا من رسول الله صلى الله عليه

وسلم؟ قال: سمعته أذناي ووعاه قلبي، قلت: هذا ابن عمك معأوية يأمرنا أن نفعل ونفعل، قال: أطعه في طاعة الله واعصه في معصية الله"
وقد كانت القوانيين الوضعية وإلى عهد قريب تعتبر الجريمة السياسية أشد خطرا من الجريمة العادية، بل كانت تعامل المجرم السياسي معاملة تتنافى مع ابسط قواعد العدالة حيث تشدد عليه العقوبة وتصادر امواله وتعاقب اهله بجريمته (عودة، ١٤٠١هـ : ١٠٧).
ب. المواقع الدينية المعادية: الدين الاسلامي هو خاتم الاديان السماوية وبه أكمل رسوله صلى الله عليه وسلم تعاليم الدين قال تعإلى في سورة المائدة (الْيَوْمَ أَكْمَلْتُ لَكُمْ دِينَكُمْ وَأَتْمَمْتُ عَلَيْكُمْ نِعْمَتِي وَرَضِيتُ لَكُمُ الْإِسْلَامَ دِينًا فَمَنْ اضْطُرَّ فِي مَخْمَصَةٍ غَيْرَ مُتَجَانِفٍ لِإِثْمٍ فَإِنَّ اللَّهَ غَفُورٌ رَحِيمٌ(٣))، ولذلك فلا يقبل أي دين غير الاسلام قال تعإلى في سورة ال عمران (وَمَنْ يَبْتَغِ غَيْرَ الْإِسْلَامِ دِينًا فَلَنْ يُقْبَلَ مِنْهُ وَهُوَ فِي الْآخِرَةِ مِنْ الْخَاسِرِينَ(٨٥))، ليس ذلك فحسب بل عاقب من بدل دينه بعد اسلامه ففي الحديث الذي رواه البخاري قال النبي صلى الله عليه وسلم: "من بدل دينه فاقتلوه"
ج. المواقع المعادية للاشخاص أو الجهات: لعل التشابه الكبير بين هذه المواقع والمواقع المخصصة للقذف والتي سبق الحديث عنها في الجرائم الجنسية، ما يغنى عن التكرار فما ينطبق على تلك المواقع من تجريم قانوني وشرعي ينطبق على هذه المواقع ايضاً.
خامساً: جرائم القرصنة:
يقصد بجرائم القرصنة هنا الاستخدام أو/و النسخ غير المشروع لنظم التشغيل أو/ولبرامج الحاسب الآلي المختلفة.
وقدتطورت وسائل القرصنة مع تطور التقنية، ففي عصر الإنترنت تطورت صور القرصنة واتسعت واصبح من الشائع جدا العثور على مواقع بالإنترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي رمزي.
وادت قرصنة البرامج إلى خسائر مادية باهضة جدا وصلت في العام (١٩٨٨م) إلى (١١) مليار دولار امريكي في مجال البرمجيات وحدها، ولذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد وأن شاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات ومن ذلك منظمة اتحاد برمجيات الاعمال (Busines Software Alliance) أو ما تعرف اختصارا بـ(BSA)، والتي اجرت دراسة تبين منها ان القرصنة على الإنترنت ستطغى على انواع القرصنة الأخرى، ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الإنترنت ومنها تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم على الإنترنت لمعرفة مدى استخدام المتصفح للموقع لبرامج مقرصنة الا ان تلك الشركات تراجعت عن هذا التهديد اثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الإنترنت.
كما قامت بعض تلك الشركات بالاتفاق مع مزودي الخدمة لابلاغهم عن اي مواقع مخصصة للبرامج المقرصنة تنشأ لديهم وذلك لتقديم شكوي ضدهم ومقاضاتهم ان امكن أو اقفال تلك المواقع على اقل تقدير.
والقرصنة عربيا لا تختلف كثيرا عن القرصنة عالميا ان لم تسبقها بخطوات خاصة في ظل عدم توفر حقوق الحماية الفكرية أو في عدم جدية تطبيق هذه القوانين ان وجدت (الجنيدي، نوفمبر ١٩٩٩م : ٢٨-٣٥).
وقوانيين حماية الملكية تعتبر من الأنظمة الحديثة في الدول العربية حيث بدأت الفكرة من الدول الرأسمالية ومن ثم بدأت الدول الأخرى تطبيقها وادراجها في انظمتها، وقد اهتمت دول الخليج بحماية الملكية الفكرية ايضا فقامت امانة مجلس التعاون الخليجي وفي الاجتماع الثاني للوزراء المسئولين عن الثقافة المنعقد بالرياض في ١٩٨٧/٩/١٥م بوضع لائحة استرشادية للنظام الموحد لحماية حقوق المؤلف في دول المجلس (موقع مجلس التعاون لدول الخليج العربية، ١٤٢٣هـ).

ولم يكن هذا هو اخر المشوار بل البداية حيث توالت دول الخليج في اصدار قوانيين الحماية الفكرية، ففي سلطنة عمان مثلاً صدر قانون الملكية الفكرية بالمرسوم السلطاني رقم (٩٧/٦٥) وتاريخ ١٤١٨/٥/٣هـ وفي الكويت صدر القانون رقم (٦٤) لعام (١٩٩٩م) بشأن حقوق الملكية الفكرية.

امّا المملكة العربية السعودية فكانت سبّاقة إلى اصدار تنظيمات خاصة لمحاربة القرصنة فصدر قرار مجلس الوزراء رقم (٥٦) و تاريخ ١٤٠٩/٤/١٤هـ بالموافقة على نظام براءات الاختراع، ثم صدر قرار مجلس الوزراء رقم (٣٠) و تاريخ ١٤١٠/٢/٢٥هـ بالموافقة على نظام حماية حقوق المؤلف (موقع محامو المملكة، ١٤٢٣هـ).

ووافق مجلس الوزراء الموقر في جلسته بتاريخ ١٤٢٠/٦/١٧هـ على تشكيل اللجنة الدائمة لحقوق الملكية الفكرية من ممثلين عن وزارات التجارة، الإعلام، الداخلية، الخارجية، العدل، الصناعة والكهرباء، البترول والثروة المعدنية، المالية والاقتصاد الوطني (مصلحة الجمارك)، ديوان المظالم، ومدينة الملك عبدالعزيز للعلوم والتقنية، ويكون مقرها ورئاستها بوزارة التجارة، وحددت مهام اللجنة بمتابعة ودراسة ما يستجد من أمور في مجال حقوق الملكية الفكرية، وإعداد التوصيات اللازمة بما يتناسب مع متطلبات الاتفاقيات الدولية ذات العلاقة، وفي مقدمتها إتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (موقع وزارة التجارة، ١٤٢٣هـ).

سادساً: جرائم اختراقات أخرى لم تتطرق اليها الدراسة:

لقد ركزت الدراسة على الافعال الجنائية التي ترتكب من قبل مستخدمي الإنترنت في المجتمع السعودي والتي حصرها الباحث من خلال الدراسة الاستطلاعية لمزودي خدمة الإنترنت في المملكة، لكن ينبغى لفت النظر إلى أن هناك جرائم أخرى لم يتبين ممارستها من قبل الافراد في المجتمع السعودي ولذلك لم تدرج ضمن عناصر الدراسة لبحثها، وان كان هذا لايعنى الجزم بعدم وجودها، أو على اقل تقدير عدم امكانية حدوثها في المجتمع السعودي، ولذا لم تدرج في الدراسة كون الدراسة تركز على الجرائم الاكثر شيوعا في المجتمع السعودي.

الا انه ونظرا لاهمية هذه الجرائم على المستوى الامني وجب اخذ الاحتياطات اللازمة للتوقي منها واخذها في الحسبان عند وضع الضوابط النظامية للتعامل مع جرائم الإنترنت وللفت نظر الباحثين في هذا المجال، ولذا وجب التطرق اليها هنا بالشرح والايضاح وهذه الجرائم:

. التجسس الإلكتروني:*

" في عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي" (البداينة، ١٩٨٨م)، والعالم العربي والاسلامي كان ولا يزال مستهدف امنيا وثقافيا وفكريا وعقديا لاسباب لاتخفى على احد.

وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية خاصة مع استخدام الإنترنت وانتشاره عربيا وعالميا.

ولا تكمن الخطورة في استخدام الإنترنت ولكن في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية ولايمكن حتما الاعتماد على وسائل الحماية التي تنتجها الشركات الاجنبية فهي ليست في مأمن ولا يمكن الاطمئنان لها تماما.

ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الأنظمة أو ما يعرفون اصطلاحا (hackers) فمخاطر هؤلاء محدودة وتقتصر غالبا على العبث أو اتلاف المحتويات والتي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة في موقع امن، اما الخطر الحقيقي فيكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخباراتية للحصول على اسرار ومعلومات الدولة ومن ثم افشائها لدول أخرى تكون عادة معادية، أو استغلالها بما يضر بالمصلحة الوطنية للدولة.

وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف اخيرا عن مفتاح وكالة الامن القومي الأمريكية (NSA) والتي قامت بزاعته في نظام التشغيل الشهير وندوز، وربما يكون هذا هو

احد الاسباب الرئيسية التي دعت الحكومة الالمانية باعلانها في الأونة الاخيرة عن استبدالها لنظام التشغيل وندوز بأنظمة أخرى.
كما كشف اخيرا النقاب عن شبكة دولية ضخمة للتجسس الالتكروني تعمل تحت اشراف وكالة الامن القومية الأمريكية بالتعاون مع اجهزة الاستخبارات والتجسس في كندا،بريطانيا، استراليا ونيوزيلندا ويطلق عليها اسم (ECHELON) لرصد المكالمات الهاتفية والرسائل بكافة انواعها سواء ماكان منها برقيا، تلكسيا، فاكسيا أو الكترونيا.
وخصص هذا النظام للتعامل مع الاهداف غير العسكرية وبطريقة تجعله يعترض كميات هائلة جدا من الاتصالات والرسائل الالكترونية عشوائيا باستخدام خاصية الكلمة المفتاح بواسطة الحاسبات المتعددة والتي تم انشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية ومنها محطة رصد الاقمار الصناعية الواقعة في منطقة واي هوباي بجنوب نيوزيلندا، ومحطة جير الدتون الموجودة باستراليا، والمحطة الموجودة في منطقة موروينستو في مقاطعة كورنوول ببريطانيا، والمحطة الواقعة في الولايات المتحدة الأمريكية بمنطقة شوجرجروف وتبعد (٢٥٠) كيلومترا جنوب واشنطن دي سي، وايضا المحطة الموجودة بولاية واشنطن على بعد(٢٠٠) كيلومتر جنوب غرب مدينة سياتل.
ولا يقتصر الرصد على المحطات الموجهة إلى الاقمار الصناعية والشبكات الدولية الخاصة بالاتصالات الدولية، بل يشمل رصد الاتصالات التي تجرى عبر أنظمة الاتصالات الارضية وكذا الشبكات الإلكترونية.
أي انه يرصد جميع الاتصالات التي تتم بأي وسيلة. ويعتبر الافراد والمنظمات والحكومات اللذين لا يستخدمون أنظمة الشفرة التامينية أو أنظمة كودية لحماية شبكاتهم واجهزتهم، اهدافا سهلة لشبكة التجسس هذه، وأن كان هذا لا يعنى بالضرورة ان الاهداف الأخرى التي تستخدم أنظمة الشفرة في مأمن تام من الغزوات الاستخباراتية لهذه الشبكة ومثيلاتها، ولا يقتصر التجسس على المعلومات العسكرية أو السياسية بل تعداه إلى المعلومات التجارية والاقتصادية بل وحتى الثقافية (عبدالمطلب، ٢٠٠١م : ٣٠-٤٥).
فمع توسع التجارة الإلكترونية عبر شبكة الإنترنت تحولت الكثير من مصادر المعلومات إلى اهداف للتجسس التجاري ففي تقرير صدر عن وزارة التجارة والصناعة البريطانية أشار إلى زيادة نسبة التجسس على الشركات من (٣٦٪) عام (١٩٩٤م) إلى (٤٥٪) عام (١٩٩٩م)، كما اظهر استفتاء اجرى عام (١٩٩٦م) لمسؤلي الامن الصناعي في الشركات الامريكة حصول الكثير من الدول وبشكل غير مشرع على معلومات سرية لانشطة تجارية وصناعية في الولايات المتحدة الأمريكية(داود،١٤٢٠هـ: ٦٢).
ومن الاساليب الحديثة للتجسس الإلكتروني اسلوب إخفاء المعلومات داخل المعلومات وهو أسلوب شائع وإن كان ليس بالامر السهل، ويتلخص هذا الاسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها وبذلك لا يشك احد في ان هناك مكان حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبسا، كما قد يلجأ إلى وسائل غير تقليدية للحصول على المعلومات السرية (داود، ١٤٢٠هـ : ٦٧).
وبعد الاعتداءات الاخيرة على الولايات المتحدة الأمريكية صدرت تعليمات جديدة لأقمار التجسس الاصطناعية الأمريكية بالتركيز على أفغانستان والبحث عن أسامة بن لادن والجماعات التابعة له، وقررت السلطات الأمريكية الاستعانة في عمليات التجسس على أفغانستان بقمرين اصطناعيين عسكريين مصممان خصيصا لالتقاط الاتصالات التي تجرى عبر أجهزة اللاسلكي والهواتف المحمولة، بالإضافة لقمرين اصطناعيين آخرين يلتقطان صورا فائقة الدقة وفي نفس الوقت طلب الجيش الأمريكي من شركتين تجاريتين الاستعانة بقمرين تابعين لهما لرصد الاتصالات ومن ثم تحول بعد ذلك إلى الولايات المتحدة حيث تدخل في أجهزة كمبيوتر متطورة لتحليلها.

وتشارك في تلك العمليات شبكة إشيلون المستخدمة في التجسس على المكالمات الهاتفية ورسائل الفاكس والبريد الإلكتروني، الأمر الذي يتيح تحليل الإشارات التي تلتقطها الأقمار الصناعية حتى إن كانت واهنة أو مشفرة (BBC,2001).

٢. الارهاب الإلكتروني:
في عصر الازدهار الإلكتروني وفي زمن قيام حكومات الكترونية كما في الامارات العربية المتحدة، تبدل نمط الحياة وتغيرت معه اشكال الاشياء وانماطها ومنها ولا شك انماط الجريمة والتي قد يحتفظ بعضها بمسماها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها القديمة في اسمها جريمة الارهاب والتي اخذت منحنى حديث يتماشى مع التطور التقنى.
وقد انتبه الغرب إلى قضية الارهاب الإلكتروني منذ فترة مبكرة، فقد شكل الرئيس الامريكي بيل كلنتون لجنة خاصة (www.nipc.gov) مهمتها حماية البنية التحتية الحساسة في امريكا، والتي قامت في خطوة أولى بتحديد الاهداف المحتملة استهدافها من قبل الارهابين ومنها مصادر الطاقة الكهربائية والاتصالات إضافة إلى شبكات الحاسب الآلي، ومن ثم تم انشاء مراكز خاصة في كل ولاية للتعامل مع احتمالات أي هجمات ارهابية الكترونية.
كما قامت وكالة الاستخبارات المركزية بانشاء مركز حروب المعلوماتية وظفت به الفا من خبراء امن المعلومات، كما شكلت قوة ضاربة لمواجهة الارهاب على مدار الساعة ولم يقتصر هذا الامر على هذه الوكالة بل تعداه إلى الأجهزة الحكومية الأخرى كالمباحث الفدرالية والقوات الجوية.
وحذّر تقرير صدر من وزارة الدفاع الأمريكية عام (١٩٩٧م) من ((بيرل هاربور الكترونية)) وتوقع التقرير ان يزداد الهجوم على نظم المعلومات في الولايات المتحدة الأمريكية من قبل الجماعات الارهابية أو عملاء المخابرات الاجنبية وأن يصل هذا الهجوم إلى ذروته عام (٢٠٠٥م)، وأوضح التقرير ان شبكة الاتصالات ومصادر الطاقة الكهربائية والبنوك وصناعات النقل في امريكا معرضة للهجوم من قبل أي جهة تسعى لمحاربة الولايات المتحدة الأمريكية دون ان تواجه قواتها المسلحة (داود، ١٤٢٠هـ).
وبعد الهجمات الاخيرة على الولايات المتحدة الأمريكية ارتفعت اصوات البعض بممارسة الارهاب الإلكتروني ضد المواقع الاسلامية والعربية التي يشتبه بانها تدعم الارهاب، وأوردت شبكة (CNET) الاخبارية خبرا عن اتفاق (٦٠) خبيرا في امن الشبكات ببدء تلك الهجمات الارهابية على مواقع فلسطينية وافغانية.
٣-. جرائم ذوي الياقات البيضاء:
هذا المصطلح من الجرائم حديث نسبياً، وأول من اطلقته عالم الاجتماع سذرلاند (Sutherland) حيث وضّح أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الادارية الكبيرة، وتشمل انواعا مختلفة من الجرائم كالرشوة والتلاعب بالشيكات والاختلاس والسرقة وتزوير العلامات التجارية للشركات العالمية ووضعها على منتجات محلية أو عالمية غير مشهورة وشراء المعلبات قبل انتهاء صلاحيتها واستبدال تاريخ صلاحيتها.
وهذا النوع من المشاكل يصعب ارتكابها أو كشفها والتحقيق فيها دون المام جيد بظروف الانتاج والحسابات الجارية والعمل التجاري ومبادي التقنية الحسابية الالتكرونية. وقدرت خسائر المجتمع الامريكي بمبلغ (١٢– ٤٢) مليون دولار سنويا نتيجة خداع المستهلكين باستخدام جميع وسائل التكنلوجيا المتقدمة(اليوسف،١٤٢٠هـ: ٢٠٩-٢١١).
واستفاد الجناة من انتشار الإنترنت في تطوير جرائمهم وتوسعة الرقعة الجغرافية لها بحيث اصبحت عالمية بعد محلية.
٤-. الجرائم الاقتصادية:

تتنوع الجرائم الاقتصادية بتنوع النظام السائد في الدولة فعلى سبيل المثال في الدول الراسمالية نجد ان اغلب الجرائم الاقتصادية تتمحور حول الاحتكارات والتهرب الضريبي والجمركي والسطو على المصارف وتجارة الرقيق الابيض والاطفال، في حين تتمحور تلك الجرائم في النظام الاشتراكي على الرشوة والاختلاس والسوق السوداء.

وهذا لا يعنى بالضرورة انه لايمكن ارتكاب كل انواع هذه الجرائم في مجتمع واحد حيث يمكن ان تجد في المجتمع الراسمالي مثلا جرائم رشوة واختلاسات والعكس صحيح.وكما في الجرائم الأخرى فان الإنترنت ساهم في تطوير طرق واساليب ارتكاب هذه الجرائم ووسّع منطقة عملها ،خاصة مع توجه الكثير من الدول في التحول إلى الحكومات اللالكترونية كما في دولة الامارات العربية المتحدة مثلا، حيث استفاد المجرمون من التقدم التقني في اختلاس الاموال وتحويل الارصدة النقدية وكذلك في سرقة التيار الكهربائي والمياه وخطوط الهاتف والعبث بها واتلافها (اليوسف،١٤٢٠هـ : ٢١١-٢١٤).

الخاتمة

وبعد، فهذا جهد المقّل في محاولة لتحديد جرائم الانترنت المرتكبة أثناء استخدام الشبكة العنكوبيتية،مع تكيفها قانوينا وشرعيا، والتى آمل ان تساهم هذه الدراسة في مواجهة هذه الجرائم الحديثة والتعامل معها ومكافحتها، وفي طرح افتراضات تصورية تلفت انتباه الباحثين في العلوم الشرطية والعلوم الاجتماعية والعلوم الإنسانية، بشكل عام، إلى كثير من الظواهر السلوكية المتعلقة باستخدام الإنترنت، والتي تتطلب البحث والدراسة.

كما اتمنى لفت انتباه المعنيين والمسئولين عن الأجهزة والتنظيمات التربوية، والإعلامية، وخطباء المساجد، والمؤسسات العلمية، للمساهمة في مكافح هذه الانماط الحديثة من الجرائم والحد منها، ولتحذير أولياء الأمور وكافة شرائح المجتمع من التعامل معها، ولبيان عظيم خطورتها بشكل عام.

واخيراً ارجوا ان اكون قد وفقت في ابراز الصورة الحقيقية لجرائم الانترنت، فإن كان ذلك فمن الله وحده وله الفضل والمنة، وان لم اوفق فمن نفسي والشيطان ولكن عذري انني اجتهدت ولكل مجتهد نصيب.

المراجع:

اولاً- المراجع العربية:

١. ابن منظور، أبي الفضل جمال الدين محمد بن مكرم.(بدون). لسان العرب . بيروت: دار صادر.

٢. أبو الحجاج، أسامة.(١٩٩٨م). دليلك الشخصي إلى عالم الإنترنت . القاهرة : نهضة مصر.

٣. ابوزهرة، محمد.(١٩٧٦م). الجريمة والعقوبة في الفقة الاسلامي. القاهرة : دار الفكر العربي.

٤. احمد، هلالي عبدالاله.(٢٠٠٠م). تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي. عابدين : النسر الذهبي للطباعة.

٥. بحر، عبدالرحمن محمد.(١٤٢٠هـ). معوقات التحقيق في جرائم الإنترنت : دراسة مسحية على ضباط الشرطة في دولة البحرين. رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

٦. البداينة، ذياب.(١٤٢٠هـ). جرائم الحاسب والإنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية ، تونس، تونس (٩٣-١٢٤).

٧. البداينة، ذياب.(١٩٨٨م). الأمن الوطني في عصر المعلومات. الجزيرة، ٩٤٢١.

٨. البداينة، ذياب.(١٩٩٩م). التطبيقات الاجتماعية للإنترنت، ورقة قدمت في الدورة التدريبية حول شبكة الإنترنت من منظور أمنى، أكاديمية نايف العربية للعلوم الأمنية ، بيروت، لبنان.
٩-. تمّام، احمد حسام طه. (٢٠٠٠م). الجرائم الناشئة عن استخدام الحاسب الآلي. القاهرة : دار النهضة العربية .
١٠. الجنيدي، ماهر (أ). (١٩٩٩م). النصر للأقوى والأذكى والقذر، مجلة إنترنت العالم العربي ، (نوفمبر)، ٣٦.
١١. الجنيدي، ماهر (ب). (١٩٩٩م). رائحة الماريجوانا تنبعث من أوكار إنترنت ، مجلة إنترنت العالم العربي ، (نوفمبر)، ٣٩ – ٤٠.
١٢. داود، حسن طاهر. (١٤٢٠هـ). جرائم نظم المعلومات. الرياض : أكاديمية نايف العربية للعلوم الأمنية.
١٣. داود، حسن طاهر. (١٤٢١هـ). الحاسب وامن المعلومات. الرياض : معهد الادارة العامة.
١٤. الدمينى، مسفر غرم الله.(١٤٠٢هـ). الجناية بين الفقه الإسلامي والقانون الوضعي. (ط.٢) الرياض : دار طيبة للنشر والتوزيع.
١٥. الزغاليل، أحمد سليمان.(١٤٢٠هـ). الاتجار بالنساء والأطفال، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية ، تونس، تونس (٤٣-٩٠).
١٦. السيد، سمير.(١٩٩٧م). محاضرات في شبكة المعلومات العالمية . القاهرة : مكتبة عين شمس.
١٧. السيف، محمد ابراهيم.(١٤١٧هـ). الظاهرة الإجرامية في ثقافة وبناء المجتمع السعودي : بين التصور الاجتماعي وحقائق الاتجاه الاسلامي. الرياض : مكتبة العبيكان.
١٨. شتا، محمد محمد.(٢٠٠١م). فكرة الحماية الجنائية لبرامج الحاسب الآلي. الإسكندرية: دار الجامعة الجديدة للنشر.
١٩. الشنيفي، عبدالرحمن عبدالعزيز.(١٤١٤هـ). أمن المعلومات وجرائم الحاسب الآلي. (ط١) الرياض : بدون.
٢٠. الشهاوي، قدري عبدالفتاح.(١٩٩٩م). اساليب البحث العلمي الجنائي والتقنية المتقدمة. الاسكندرية :منشأة المعارف.
٢١. الشهري، عبدالله محمد صالح.(١٤٢٢هـ). المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي : دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض، المملكة العربية السعودية.
٢٢. الشهري، فايز عبدالله.(١٤٢٢هـ). استخدامات شبكة الإنترنت في مجال الاعلام الامني العربي. مجلة البحوث الأمنية ، ١٠(١٩)، ١٦٥-٢١٤.
٢٣. صحيفة عكاظ، العدد ١٢٧٨٩، ١٤٢٢/٦/١٣هـ، الصفحة الأولى.
٢٤. طالب، احسن.(١٩٩٨م). الجريمة والعقوبة والمؤسسات الاصلاحية. الرياض : دار الزهراء.
٢٥. عبدالمطلب، ممدوح عبدالحميد.(٢٠٠١ م). جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية : الجريمة عبر الإنترنت . الشارقة: مكتبة دار الحقوق.
٢٦. عجب نور، اسامة محمد.(١٤١٧هـ). جريمة الرشوة في النظام السعودي. الرياض : معهد الادارة العامة.
٢٧. عزالدين، أحمد جلال.(١٤١٤هـ). أساليب التعاون العربي في مجال التخطيط لمواجهة جرائم الارهاب. الرياض : أكاديمية نايف العربية للعلوم الأمنية.

٢٨. عودة، عبدالقادر.(١٤٠١هـ). التشريع الجنائي الإسلامي. بيروت : مؤسسة الرسالة، (المجلد الأول).
٢٩. عيد، محمد فتحي.(١٤١٩هـ). الإجرام المعاصر. الرياض : أكاديمية نايف العربية للعلوم الأمنية.
٣٠. فرحات، محمد نعيم.(١٤٠٤هـ). التشريع الجنائي الاسلامي. جدة : مكتبة الخدمات الحديثة.
٣١. الفنتوخ، عبدالقادر.(١٤٢١هـ). الإنترنت للمستخدم العربي. الرياض: مكتبة العبيكان.
٣٢. القدهي، مشعل عبدالله. (١٤٢٢هـ). المواقع الإباحية على شبكة الإنترنت وأثرها على الفرد والمجتمع. [١٤٢٢/٧/٢٩هـ]http://www.minshawi.com/gadhi.htm
٣٣. الماوردي، محمد حبيب.(١٤٠٧هـ). الاحكام السلطانية. القاهرة : دار التراث العربي.
٣٤. مجلة أفاق الإنترنت. (١٩٩٧)، إنترنت ٢، المؤلف، السنة ١ (٣)، ٣٨-٤١.
٣٥. محمد، عادل ريان. (١٩٩٥م)، جرائم الحاسب الآلي وأمن البيانات، العربي ، (٤٤٠)، ٧٣ – ٧٧ .
٣٦. مندورة، محمد محمود.(١٤١٠هـ). الجرائم الحاسب الآلية، دورة فيروس الحاسب الآلي، مكتب الأفاق المتحدة : الرياض ، ١٩ – ٢٦.
٣٧. منصور، عبدالمجيد سيد احمد.(١٤١٠هـ). السلوك الاجرامي والتفسير الاسلامي. الرياض : مركز ابحاث الجريمة.
٣٨-. موقع صحيفة الجزيرة - القرية الإلكترونية (١٤٢١/٢/٢)
http://www.al-jazirah.com/2000/may/6/ev.htm#evt3
٣٩. موقع أرابيا (٢٠٠١/٦/١٠م)
http://www.arabia.com/tech/article/arabic/0,4884,48801,00.html
٤٠. موقع السوق الخليجي (١٤٢٣/٤/١هـ)
http://www.gulfforum.com/ksa1/20/1.html
٤١. موقع بوابة عجيب (٢٠٠١/٣/٢٥م)
http://it.ajeeb.com/viewarticle=1662&category=34
٤٢. موقع بوابة عجيب (٢٠٠١/٨/٨م)
http://it.ajeeb.com/viewarticle.asp?article=1976&category=17
٤٣. موقع صحيفة البي بي سي (٢٠٠١)
http://news.bbc.co.uk/hi/arabic/news/newsid_1550000/1550726.stm
٤٤. موقع صحيفة البيان (٢٠٠٠/٥/١٩)
http://www.albayan.co.ae/albayan/2000/05/19/mhl/2.htm
٤٥. موقع صحيفة الجزيرة (٢٠٠٠) http://www.al-jazirah.com/
٤٦. موقع مجلة الأمن الإلكترونية (١٤٢١/٧/٢٢هـ)
http://safola.com/security.chtml
٤٧. موقع مجلس التعاون لدول الخليج العربية (١٤٢٣/٤/٢هـ)
http://www.gcc-sg.org/index.html
٤٨. موقع محامو المملكة (١٤٢٣/٤/٢هـ)
http://www.mohamoon-ksa.com/dir.asp?DirID=1&Status=1

٤٩. موقع منتدى الفوائد (١٤/٨/ ١٤٢١هـ)
http://216.122.89.86/muntada/postings.cgi?action=newtopic&numb
er=1&forum.
٥٠. موقع وزارة التجارة (٢/٤/١٤٢٣هـ)
http://www.commerce.gov.sa/aboutus/leg1.asp?print=true
٥١. النشرة التعريفية عن مدينة الملك عبدالعزيز للعلوم والتقنية. (١٤١٩هـ). الرياض: الإدارة العامة للتوعية العلمية والنشر.
٥٢. اليوسف، عبدالله عبدالعزيز.(١٤٢٠هـ). التقنية والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية ، تونس، تونس (١٩٥- ٢٣٣)

ثانيا- المراجع الاجنبية:

Adsit, C. Kristin. (1999). Internet Pornography Addiction.[Online]. Available: http://www.chemistry.vt.edu/chem-dept/%20dessy/honors%20/papers99/adsit.htm [9.3.2001].

Highley, Reid. (1999). Viruses: The Internet's Illness.[Online]. Available: http://www.chemistry.vt.edu/chem-dept/dessy/honors%20/papers99/highleh.htm [9.3.2001].

Koerner, B. I. (1999,November 22). Only you can prevent computer intrusions. U.S. News and World Report, 127, pp. 50.

Morningstar, Steve. (1998). Internet Crime and Criminal Procedures. [Online]. Available: http://www.prevent-abuse-now.com/index.html [13.10.2001].

Nanoart. (2000) [Online]. Available: http://www.nanoart.f2s.com/hack/ [15.11.2000].

NUA Internet Surveys. (1998,June). How Many Online? [Online]. Available: http://www.nua.ie/surveys/howmayonline/index.html [26.10.2000].

Rapalus, P.(2000,May). Ninety percent of survey respondents detect cyber attacks. Computer Security Institute. [Online]. Available: http://www.gocsi.com/prelen_000321.htm [11.10.2001]

Reuvid, Jonathan. (1998). The Regulation and Prevention of Economic Crime, London: Kogan, 14.

Skinner, W. F., & Fream, A. M. (1997, November). A social learning theory analysis of computer crime among college students. Journal of research in Crime and Delinquency, 34 (4), 495-519.

Staff. (2000, April 2). The Business of Technology. Available:http://www.redherring.com/mag/issue7/news-security.html [11.10.2001].

Thomas, P. (2000, February 23). Insufficient computer security threatens doing business. [Online]. Available: http://www.cnn.com/2000/TECK/computing/02/23/credir.card.thefts [11.11.2001]. /index.html
Thompson, R. (1999, February). Chasing after petty computer crime. IEEE Potentials, 18 (1), 20-22.
Vacca, John. (1996). Internet Security Secrets.USA:IDG Book. Worldwide Inc.
Wilson, c. (2000) Holding management accountable: a new policy for protect against computer crime. Proceedings of the National Aerospace and Electronics Conference, USA 2000, 272-281.

* للمزيد ارجع إلى كتاب الإجرام المعاصر للدكتور محمد فتحي عيد، ص ٧٧-١٣١.
* للاستاذة يمكن الرجوع إلى كتاب الجريمة عبر الانترنت للدكتور ممدوح عبدالمطلب ص ٣٠

دراسة جرائم الانترنت

مقدمة الدراسة

الحمد لله الذي َخلَقَ الإنسانِ منْ عَدَمْ وعَلّمَهُ ما لم يعلم ورَغَّبَهُ في العِّلْمِ و التَّعَلُّمْ، والصلاة والسلام على هادي البشرية ومعلّمْ الإنسانية الذي أُمِرَ بالقراءة في أول آية أنزلت عليه والذي رغَّبَ في التعلّمْ وحثّ عليه ، أمَّا بعد :

الجريمة ظاهرة اجتماعية تتواجد بتواجد الإنسان والمجتمع وتتطور بتطورهما، ولا شك أن المجرمين - كما رجال الأمن - يحاولون الاستفادة من هذا التقدم التقني خاصة وأننا في عصر ثورة المعلومات وتقدم العلوم الحديثة والتكنولوجيا المتطورة، وتبعا لذلك فانه من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق، وهذا ليس قاصرا على أسباب التقدم التقني فقط بل يحدث دوما وبصفة مستمرة فالمجرم والجريمة في تقدم وتجدد مستمر، فمجرم الأمس ليس كمجرم اليوم وبالتالي فجريمة الأمس ليست كجريمة اليوم.

وقد تمخضت ثورة المعلومات والتكنولوجيا المتقدمة عن وسائل اتصالات متطورة جعلت العالم قرية إلكترونية مفتوحة للعموم، ألغت معها الحدود الجغرافية والسياسية للدول، وهذه التقنية الخاصة بنظام نقل المعلومات السريع أو ما يعرف بالإنترنت ليست سيئة في حد ذاتها بل هي سلاح ذو حدين فيمكن أن تسخَّر للخير والمنفعة كما يمكن أن تسخَّر للشَّرْ والمضرَة. وهذا ما أكده الفريق دكتور عباس أبو شامة وزير داخلية السودان الأسبق ورئيس قسم العلوم الشرطية بأكاديمية نايف للعلوم الأمنية في بحثه المقدم للندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها التي عقدت في تونس فيقول:

"ورغم الفوائد العديدة التي لا تحصى للاستفادة من شبكة المعلومات العالمية (الإنترنت) إلا انه في نفس الوقت فقد زادت أساليب إساءة الاستخدام لتلك الشبكة ومنها الاستخدام لارتكاب بعض الجرائم، وفي ذلك تطويع لهذه التقنية لرغبات بعض المجرمين، وسيستمر ذلك مادام المشترك في الشبكة (الإنترنت) يمكنه

الاطلاع على كل المعلومات التي تكون متاحة من المصدر. وبما انه حتى الآن ليس هناك ضوابط صارمة للحد من تلك الأضرار ولكن يحكم الأمر سلوك الأفراد المستعملين إلى حد كبير"(أبوشامة،١٤٢٠هـ : ٢١).

فهي سلاح ذو حدين و" من دون شك أن إستخدام الإنترنت كشبكة اتصالات متطورة ومعاصرة، يُضفي على الحضارة الإنسانية بعداً جديداً في تسهيل وسرعة إنجاز المعاملات للحصول على المعلومات والبيانات المطلوبة دون عناء. ولكن هذا الاستخدام الحضاري، دخل عليه الأشرار بتقنيات مضادة " (حبوش، ١٤٢٠هـ : ٢٥٣).

ومن سلبيات الإنترنت إستفادة المجرمون من هذا التطور حيث أن " هذه التقنيات شجعت وساعدت المجرمين على زيادة عدد وحجم جرائمهم دون زيادة في الجهد المبذول عما كانوا يبذلونه مع الوسائل التقليدية، بل مع انخفاض احتمالات انكشاف أمرهم " (داود، ١٤٢٠هـ : ٧٣).

نخلص مما تقدم إلى ظهور أنماط جديدة من الإجرام لم تكن مألوفة من السابق، بل أن الأمر تعدى أنماط الجرائم إلى ظهور أنماط جديدة من الحروب أيضا والتى تعرف بالحروب الالكترونية، ولا تزال الأيام القادمة حُبلى بكل جديد ولا نزال في بداية عصر الانفجار المعلوماتي، مما يعنى توقع ظهور المزيد والمزيد من هذه الأنماط الجديدة والذي يتوجب معها تحديث الأنظمة والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة.

وهذه الدراسة هي محاولة لإلقاء نظرة سريعة على المستجدات الإجرامية في عصر الإنترنت في المجتمع السعودي مع قصرها تحديدا على ما يعرف اصطلاحا بـ "جرائم الإنترنت" في محاولة لإلقاء الضوء على حجم ونمط أهم الجرائم الجديدة وتحديدها قدر الإمكان، وبالتالي المساهمة في وضع الخطوط العريضة للتعرف على كيفية مكافحتها والحد منها. مع التنويه سلفا بأنه لا يمكن بمكان حصر هذه الجرائم لسبب بسيط وبديهي هو أن الجريمة وأنماطها في تجدد مستمر ولا تقف إطلاقا عند أنماط محددة أو أشكال معينة بل هي ومنذ قديم الأزل في تطور مستمر، وهذا التجدد في أنماط الجريمة ليس قاصرا على عصر الانفجار المعلوماتي فقط بل انه ظاهرة قديمة قدم المجتمعات البشرية كما أنها ليست قاصرة على مجتمع دون أخر بل هي ظاهرة اجتماعية عالمية تتواجد في كل المجتمعات بصرف النظر عن تقدم أو تخلف تلك المجتمعات، إلا أن تطور أي مجتمع يصاحبه بالضرورة تطور أيضا في أنماط الجريمة.

مشكلة الدراسة

بالرغم من أن خدمة الإنترنت ليست بالخدمة الحديثة حيث بدأ استخدامها منذ عام (١٩٦٩م) إلا أن استخدامها كان أنذاك مقتصرا على الأغراض العسكرية وفي دولة واحدة هي أمريكا، ومنذ فترة ليست بالطويلة بدأ انتشار استخدام الإنترنت على المستوي العالمي وفي كل المجالات حيث غزت هذه الخدمة العالم بشكل سريع جدا وعلى كافة مستويات المجتمع. وقد قدرت إحدى الدراسات عدد مستخدمي شبكة الإنترنت عالميا في العام (١٩٩٨م) بحوالي (١٣٤) مليون مستخدم وتوقعت إزدياد

هائل في عدد المستخدمين للشبكة سنويا يمكن أن يصلوا في العام (٢٠٠٥ م) الى حوالي (٢٤٥) مليون مستخدم وستكون غالبية هذه الزيادة في خارج الولايات المتحدة الأمريكية، بمعنى أن انتشار الإنترنت لن يكون محصورا في أمريكا فقط بل سيشمل جميع دول العالم وهذا يوضح وبجلاء سرعة انتشار الإنترنت كظاهرة يتحول إليها الجميع بصورة سريعة وشبه حتمية حيث سيعتبر من يتخلف عن مواكبتها في عداد المتخلفين عن مواكبة تقنية العصر وبالتالي سَيُتَخَلَّفْ عن الركب (NUA , 1998 & 2000).

وحرصت المملكة العربية السعودية كغيرها من الدول بالأخذ بهذه الخدمة حيث بدأت في تقديم الخدمة بشكل رسمي للقطاعين الخاص والعام في عام (١٤١٩هـ)، وصاحب دخول هذه الخدمة إلى المملكة - كغيرها من الدول الأخرى - ظهور أنماط مختلفة وجديدة من الجرائم لم تكن مألوفة من قبل، وان كانت هذه الجرائم لا تمثل إلى الآن ظاهرة في حد ذاتها، وأصبحت الجهات الأمنية مطالبة بمواكبة هذه التقنية وبتحديث أساليب عملها بما يتوافق مع التقنية الحديثة وإفرازاتها وإلا تفشت هذه الجرائم وشَكَّلَتْ ظاهرة تقلق المجتمع وأمنه ووجدت الجهات الأمنية نفسها متخلفة عن المجرمين مِنْ مَنْ تسابقوا إلى استخدام هذه التقنية والأخذ بها بل واستغلالها في أنشطتهم الإجرامية وهو الأمر الذي يمثل خطرا محدقا يتربص بالمجتمع وأمنه مالم يسارع المجتمع والجهات الأمنية إلى المبادرة في التعرف عن قرب على هذه الأنماط الجديدة ليكونوا أقدر على مواجهتها والتعامل معها درءاً لخطرها.

وكان حرص الدولة على أمن الوطن والمواطنين بقدر حرصها على الأخذ بمستجدات التقنية ولذلك فقد تأخر تقديم خدمة الإنترنت في المملكة العربية السعودية نوعاً ما، ويعود ذلك لأسباب مختلفة لعل من أهمها حرص الدولة على التقليل من سلبيات هذه الخدمة، والتي نجحت في ذلك إلى حد ما حيث لا تمثل جرائم الانترنت ظاهرة في المجتمع الى الآن، ويعود الفضل في ذلك بعد الله إلى أن قوانين وتشريعات المملكة المستمدة من الشريعة الإسلامية قد تضع بعض الحواجز أمام من يرتكب مثل هذه الجرائم من داخل المملكة، إلا انه ومع ذلك فقد صاحب دخول الخدمة بالمملكة العربية السعودية ظهور أنماط جديدة من الإجرام - كغيرها من الدول التي أخذت بالتقنية الحديثة - فالطبيعة البشرية في كل مكان معرضة للضعف والنفس أمارة بالسوء، ولذلك يجب العمل على تفعيل وتطوير الأنظمة الرادعة دائما لتواكب مستجدات الجريمة المتطورة دوما.

وبالرغم من حداثة الإنترنت إلا أن الدراسات أظهرت أن حجم الخسائر المادية لجرائم الحاسب الآلي - همزة الوصل لشبكة الإنترنت – في المملكة العربية السعودية تقدر بحوالي ثلاثين مليون دولار امريكي (البداينة، ١٩٩٨م : ٩٨) وهذا مؤشر مهم يجب الأخذ به عند تصور حجم جرائم الإنترنت المتوقعة في المجتمع السعودي خاصة وان أي جريمة ترتكب في الإنترنت لا يمكن أن ترتكب إلا من خلال الحاسب الآلي.

لذا كان من الضرورة والأهمية بمكان العمل بداية على تحديد حجم وأنماط أهم الجرائم التي أفرزتها استخدامات الإنترنت في المجتمع السعودي مع العمل على

تحديد أهم سمات وخصائص مرتكبيها، حيث على ضوء ذلك يمكن للجهات الأمنية وضع خططها الحالية والمستقبلية لمواجهة هذه الأنماط غير التقليدية والجديدة.
ومن هنا فان مشكلة البحث تنحصر في تحديد حجم وأنماط أهم جرائم الإنترنت شيوعاً بين مستخدمي الانترنت في المجتمع السعودي وخاصة فيما يتعلق بالجرائم الجنسية، جرائم الاختراقات، جرائم التجارة الإلكترونية، جرائم إنشاء وارتياد المواقع المعادية، جرائم القرصنة والجرائم الأخرى. مع تحديد أهم سمات وخصائص مرتكبي تلك الجرائم من مستخدمي الانترنت في المجتمع السعودي.

اهمية الدراسة

الأهمية النظرية للدراسة:

انتشر الإنترنت في الآونة الأخيرة في جميع دول العالم ومنها الدول العربية ، وان كان الإنترنت كتقنية في حد ذاته غير حديث، وقد صاحب هذا الانتشار والاستخدام للشبكة سلبيات وإيجابيات سواء على المستوى الأمني (وهو ما يهمنا هنا) أو المستوى الثقافي أو الاجتماعي أو السياسي أو الاقتصادي .
ومن هنا تبرز أهمية هذه الدراسة كونها محاولة لتحديد حجم ونمط أهم جرائم الإنترنت المرتكبة في المملكة العربية السعودية وأهم سمات وخصائص مرتكبيها والتي يمكن الاستفادة من هذه الدراسة في مواجهة هذه الجرائم الحديثة والتعامل معها ومكافحتها، كما يمكن أن تساهم هذه الدراسة بطرح افتراضات تصورية وتلفت انتباه الباحثين في العلوم الشرطية والعلوم الاجتماعية والإنسانية بشكل عام إلى كثير من الظواهر السلوكية المتعلقة باستخدام الإنترنت والتي تتطلب البحث والدراسة.

الأهمية التطبيقية للدراسة:

من ناحية تطبيقية فإن الباحث يأمل من خلال هذه الدراسة أن يلفت انتباه الجهاز القضائي والقانوني إلى سلوكيات وأفعال جنائية ترتكب ضد الآخرين بواسطة الحاسب الآلي ومن خلال شبكة الانترنت، من أجل وضع ضوابط قانونية وقضائية في التعامل والحكم على مرتكبيها.
كما يأمل الباحث أيضاً من حصر أهم أنماط الجرائم الشائعة في المجتمع السعودي والتى ترتكب من خلال استخدام الحاسب الآلي وشبكة الإنترنت إلى لفت انتباه المعنيين والمسئولين عن الأجهزة والتنظيمات التربوية والإعلامية وخطباء المساجد والمؤسسات العلمية للمساهمة في مكافحتها والحد منها ولتحذير أولياء الأمور والشباب منها بشكل عام.

اهداف الدراسة

تهدف الدراسة إلى الآتي :

١. الكشف عن حجم ونمط الجرائم الجنسية التي يرتكبها مستخدمي الانترنت في المجتمع السعودي عبر الإنترنت وتحديد أهم سمات وخصائص مرتكبيها.
٢. التعرف على حجم ونمط جرائم الاختراقات التي يرتكبها مستخدمي الانترنت في المجتمع السعودي عبر الإنترنت وتحديد أهم سمات وخصائص مرتكبيها.

٣. الكشف عن حجم ونمط الجرائم المادية التي يرتكبها مستخدمي الانترنت في المجتمع السعودي وتحديد أهم سمات وخصائص مرتكبيها.
٤. الكشف عن حجم ونمط المواقع المعادية في شبكة الإنترنت وتحديد أهم سمات وخصائص منشئيها وزائريها من مستخدمي الانترنت في المجتمع السعودي.
٥. الكشف عن حجم ونمط جرائم القرصنة التي ترتكب في شبكة الإنترنت من مستخدمي الانترنت في المجتمع السعودي وتحديد أهم سمات وخصائص مرتكبيها.

اسئلة الدراسة

تحاول هذه الدراسة الإجابة على التساؤلات الآتية:
١. ما هو حجم الجرائم الجنسية التي يرتكبها أفراد المجتمع السعودي عبر الإنترنت وخاصة فيما يتعلق بارتياد المواقع الإباحية، الشراء منها، الاشتراك فيها، أو إنشائها، إنشاء القوائم الإباحية أو الاشتراك فيها، إنشاء المواقع أو الصفحات الخاصة بالقذف والتشهير بالأشخاص، استخدام البروكسي للدخول إلى المواقع المحجوبة، إخفاء الشخصية أثناء التصفح أو أثناء إرسال البريد الإلكتروني و انتحال شخصية الآخرين. وما هي أهم سمات وخصائص مرتكبيها؟
٢. ما هو حجم جرائم الاختراقات التي يرتكبها أفراد المجتمع السعودي على شبكة الإنترنت وخاصة فيما يتعلق بتدمير المواقع، اختراق المواقع الرسمية أو الشخصية، اختراق الأجهزة الشخصية، اختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه أو إغراقه، الاستيلاء على اشتراكات الآخرين وأرقامهم السرية و إرسال الفيروسات والتروجنات. وما هي أهم سمات وخصائص مرتكبيها ؟
٣. ما هو حجم الجرائم المالية التي يرتكبها أفراد المجتمع السعودي على شبكة الإنترنت وخاصة فيما يتعلق بجرائم السطو على أرقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمة المنظمة، المخدرات، غسيل الأموال. وما هي أهم سمات وخصائص مرتكبيها؟
٤. ما هو حجم جرائم إنشاء أو ارتياد أو الاشتراك في المواقع المعارضة أو المعادية التي يرتكبها أفراد المجتمع السعودي على شبكة الإنترنت وخاصة فيما يتعلق بالمواقع السياسية أو الدينية أو الشخصية المعادية. وما هي أهم سمات وخصائص مرتكبيها؟
٥. ما هو حجم جرائم القرصنة التي يرتكبها أفراد المجتمع السعودي على شبكة الإنترنت وخاصة فيما يتعلق بإنشاء مواقع للبرامج المقرصنة، استخدام البرامج المقرصنة وسرقة المواقع. وما هي أهم سمات وخصائص مرتكبيها؟

مفاهيم الدراسة

يركز الباحث على مصطلح رئيسي في البحث وهو جرائم الإنترنت ومع ذلك فسيتم التطرق إلى توضيح المفهوم الرئيسي في البحث إضافة إلى توضيح أهم المفاهيم التي ستتطرق إليها الدراسة :

الحاسب الآلي : يمكن أن يعرف بأنه " مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلة طبقا لبرنامج تم وضعه مسبقا للحصول على نتائج معينة " (قشقوش، ١٩٩٢م : ٦)
وهناك من يعرف الحاسب الآلي بأنه " جهاز آلي أو آلة تتولى معالجة المعطيات المخزونة في الذاكرة الرئيسية في صيغة معلومات تحت إشراف برنامج مخزون (سلفاً في الجهاز) " (عبدالرحمن، ١٩٩٢م : ١٦)
أما الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني فقد عرّفت الحاسب الآلي بتعريف مطول نذكر هنا ما يهمنا منه ومما جاء فيه أنه " جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات (Data Input) أو إخراج معلومات (Information Output) وإجراء عمليات حسابية أو منطقية، وهو يقوم بالكتابة على أجهزة الإخراج (Output Devices) أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الحاسب (Operator) عن طريق وحدات الإدخال " (فهمي وآخرون، ١٩٩١م : ١٠٨)

الإنترنت : " تعنى لغويا (ترابط بين شبكات) وبعبارة أخرى (شبكة الشبكات) حيث تتكون الإنترنت من عدد كبير من شبكات الحاسب المترابطة والمتناثرة في أنحاء كثيرة من العالم. ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى بروتوكول تراسل الإنترنت(TCP/IP)" (الفنتوخ، ١٤٢١هـ : ١١)
الشبكة النسيجية (WORLD WIDE WEB) وتسمي أيضا الويب (WEB) : " تمثل مدخلا ميسّراً للإنترنت وتمثل واجهة استخدام موحدة للعديد من أدوات الشبكة المتاحة وتعمل عن طريق تأسيس روابط نصّية متشعبة (Hypertextlink) بين الوثائق الموجودة في أي مكان على الشبكة "(الفنتوخ، ١٤٢١هـ : ١١)

المشترك : كل جهة أو شخص يستطيع الوصول إلى الإنترنت واستخدام الخدمات التى توفرها الشبكة أو الاستفادة منها.

المزود: جهة أو شركة تقدم الخدمة للمشترك مقابل اشتراك يدفعه المشترك، ويعتبر المزود كحارس لبوابة الإنترنت، ويوجد في المملكة العربية السعودية (٢٩) مزود خدمة معتمد من مدينة الملك عبدالعزيز للعلوم والتقنية لتقديم الخدمة، وان أتضح للباحث أثناء إجراء الدراسة اعتذار اثنين من هؤلاء المزودين المعتمدين عن تقديم خدمة الإنترنت.

المجتمع السعودي : يشمل مجتمع الدراسة جميع مستخدمي خدمة الإنترنت في المملكة العربية السعودية وذلك في زمن إجراء الدراسة عام ١٤٢٢هـ الموافق عام ٢٠٠٢م والبالغ عددهم حوالي (٥٧٠) ألف مستخدم حسب إحصائية موقع عجيب.

القرصنة : يقصد بالقرصنة هنا الاستخدام أو النسخ غير المشروع لنظم التشغيل أو/والبرامج الحاسوبية المختلفة والاستفادة منها شخصيا أو تجاريا.

الفيروسات الحاسوبية : هي إحدى أنواع البرامج الحاسوبية إلا أن الأوامر المكتوبة في هذه البرنامج تقتصر على أوامر تخريبية تلحق ضررا بنظام المعلومات أو البيانات، ولدى البرنامج القدرة على التضاعف والانتشار بحيث يزرع عند تشغيله نسخة منه في البرامج المصابة (داود، ١٤٢٠هـ) فيمكن عند كتابة كلمة أو أمر ما أو حتى مجرد فتح البرنامج الحامل لفيروس أو الرسالة البريدية المرسل معها الفيروس إصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به.

حصان طروادة (Trojan Horse) : هو برنامج صغير ظاهره النفع وباطنه الدمار وينتقل عبر الشبكات ويتم تشغيله داخل جهاز الحاسب لكي يقوم بأغراض التجسس على أعمال الشخص التي يقوم بها على حاسوبه الشخصي. (الفنتوخ، ١٤٢١هـ : ١٥)

المتسلل (Hacker) **:** شخص بارع في استخدام الحاسب وبرامجه ولديه فضول في استكشاف حاسبات الآخرين وبطرق غير مشروعة.

المقتحم : شخص مخالف للنظام يقوم بالتسلل إلى نظم الحاسب الآلي للإطلاع علي المعلومات المخزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها.

البروكسي : برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز واحد.

أما المصطلح الرئيسي الذي يركز الباحث عليه في البحث فهو **جرائم الإنترنت** وتعرَّفْ الجريمة كالأتي:

التعريف الشرعي للجريمة :

تُعَّرفْ الجريمة شرعاً بأنها " إتيان فعل محرّم معاقب على فعله، أو ترك فعل محرّم الترك معاقب على تركه، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه " (عوده، ١٤٠١هـ : ٦٦).

التعريف القانوني للجريمة :

يعرّف القانون الجريمة بأنها " إمّا عمل يجرِّمه القانون، أو امتناع عن عمل يقضى به القانون، ولا يعتبر الفعل أو الترك جريمة في نظر القوانين الوضعية إلا إذا كان معاقباً عليه طبقاً للتشريع الجنائي " (عوده، ١٤٠١هـ : ٦٧).

تعريف جرائم الحاسب الالي والانترنت :

تعرّف جرائم الحاسب الآلي والانترنت بأنها" ذلك النوع من الجرائم التي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها" (مندورة،١٤١٠هـ : ٢١).
كما يمكن تعريفها بأنها"الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني"(محمد، ١٩٩٥م : ٧٣).
وهناك من عرَفها بأنها " أي عمل غير قانوني يستخدم فيه الحاسب كأداة، أو موضوع للجريمة " (البداينة، ١٤٢٠هـ : ١٠٢)

التعريف الإجرائي لجريمة الإنترنت:

تُعَرِّفْ الدراسة جرائم الإنترنت بأنها : جميع الأفعال المخالفة للتشريع الإسلامي ولأنظمة المملكة العربية السعودية والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الإنترنت، ويشمل ذلك:

١. الجرائم الجنسية (ارتياد المواقع الإباحية، الشراء منها، الاشتراك فيها، أو إنشائها، إنشاء القوائم الإباحية أو الاشتراك فيها، إنشاء المواقع أو الصفحات الخاصة بالقذف والتشهير بالأشخاص، استخدام البروكسي لتجاوز المواقع المحجوبة، إخفاء الشخصية أثناء التصفح أو أثناء إرسال البريد الإلكتروني و انتحال شخصية الآخرين)
٢. جرائم الاختراقات (تدمير المواقع، اختراق المواقع الرسمية أو الشخصية، اختراق الأجهزة الشخصية، اختراق البريد الإلكتروني للآخرين، الاستيلاء على البريد الإلكتروني للآخرين، إغراق البريد الإلكتروني للآخرين، الاستيلاء على اشتراكات الآخرين وأرقامهم السرية و إرسال الفيروسات والتروجنات)
٣. جرائم الأموال (السطو على أرقام البطاقات الائتمانية ، لعب القمار، التزوير، الجريمة المنظمة، جرائم المخدرات وغسيل الأموال)
٤. جرائم إنشاء أو ارتياد المواقع المعارضة أو المعادية (إنشاء، ارتياد أو الاشتراك في المواقع السياسية أو الدينية أو الشخصية المعادية)
٥. جرائم القرصنة (إنشاء مواقع للبرامج المقرصنة، استخدام البرامج المقرصنة وسرقة المواقع)

مجتمع الدراسة :

يشمل مجتمع الدراسة جميع مستخدمي خدمة الإنترنت في المملكة وذلك في زمن إجراء الدراسة عام (١٤٢٢هـ) الموافق عام (٢٠٠٢م) والبالغ عددهم (١٥٠) ألف مستخدم حسب الاحصائية التي صدرت وقت اختيار الباحث لمجتمع البحث، في حين ارتفع العدد ليبلغ (٥٧٠) ألف مستخدم تقريبا حسب أخر الإحصائيات حين تم البدء في تنفيذ الدراسة الميدانية.

المجال البشري : جميع مستخدمي الإنترنت في المجتمع السعودي في زمن إجراء الدراسة من الذكور والإناث ومن جميع الجنسيات العربية والأجنبية ولجميع الديانات السماوية وغير السماوية ويبلغ عددهم تقريبا (٥٧٠) ألف مستخدم حسب أخر الإحصائيات

المجال المكاني : جميع مناطق المجتمع السعودي ويشمل ذلك المنطقة الغربية والجنوبية والوسطى والشرقية والشمالية في المملكة العربية السعودية.

عينة الدراسة:

تمّ اختيار المجتمع الكلي للدراسة وهم جميع مستخدمي الإنترنت في المجتمع السعودي، والبالغ عددهم تقريباً (١٥٠) مائة وخمسين ألف مستخدم حسب إحصائية مدينة الملك عبدالعزيز للعلوم والتقنية صدرت وقت اختيار الباحث لمجتمع البحث، ووزعت الاستبانة بطريقة تضمن الوصول إلى جميع مستخدمي الإنترنت في المجتمع السعودي، ووصل عدد الاستبانات المجاب عليها (١٠,١٣٨) استمارة، تمّ استبعاد (٢٤٧) استبانة منها للنقص في بعض إجاباتها، حيث وُضع معيار لاستبعاد أيّ استبانة لم يتم الإجابة على (٤٠) سؤال على أقلّ تقدير من الأسئلة الكلية للاستبانة والبالغ عددها (٦٢) سؤالاً، ليصبح العدد الكلي للاستبانات الداخلة في تحليل الدراسة الميدانية (٩٨٩١) استبانة، أي ما نسبته (٦,٥٩٪) من المجموع الكلي لمجتمع البحث وهي نسبة مقبولة منهجياً.

خصائص مجتمع الدراسة

سيتمّ التطرّق هنا إلى وصف خصائص المشاركين في الدراسة الميدانية، بحسب ترتيب متغيّرات الدراسة ،التي سيتم التطرّق لها بشكل مفصّل لاحقاً، وهي :

١. الفئة العمرية: كانت أكبر نسبة مشاركة لفئة أواسط العمر، حيث بلغ (٤٩٠٩) مستخدم، أي ما نسبته (٤٩,٦٪) من مجموع المشاركين، ويوضح الجدول التالي ذلك مفصلاً:

جدول رقم (١)يوضّح خصائص مجتمع الدراسة بحسب الفئة العمرية

الفئة العمرية	التكرار (ك)	النسبة (٪)
طفل (أقلّ من ١٢ سنة)	٥٤	٠,٥٪
مراهق (١٣-١٧ سنة)	٥٥١	٥,٦٪
شباب (١٨-٢٥ سنة)	٤٢٤٤	٤٢,٩٪
أواسط العمر ٢٦-٥٠ سنة)	٤٩٠٩	٤٩,٦٪
كهولة (٥١-٦٥ سنة)	٨١	٠,٨٪
شيخوخة (أكبر من ٦٥ سنة)	٣٤	٠,٣٪
الفاقد من إجابات هذا السؤال	١٨	٠,٢٪
المجموع	٩٨٩١	١٠٠٪

٢. الجنس: بلغت نسبة الذكور المشاركين في الدراسة (٧٦,٧٪)، ويوضّحه الجدول التالي:

جدول رقم (٢)يوضّح خصائص مجتمع الدراسة بحسب الجنس

الجنس	التكرار (ك)	النسبة (٪)
ذكر	٧٥٨٤	٪٧٦,٧
أنثى	٢١٨٣	٪٢٢,١
الفاقد من إجابات هذا السؤال	١٢٤	٪١,٣
المجموع	٩٨٩١	٪١٠٠

٣. الدخل الشهري: كان دخل غالبية المشاركين في الدراسة أقلّ من خمسة ألاف ريال.

جدول رقم (٣)

يوضّح خصائص مجتمع الدراسة بحسب الدخل الشهري

الدخل الشهري	التكرار (ك)	النسبة (٪)
منخفض (أقلّ من ٥,٠٠٠ ألاف)	٣٨٤٨	٪٣٨,٩
متوسط (من ٥,٠٠٠ – ١٠,٠٠٠)	٣٠٨٦	٪٣١,٢
مرتفع (أكثر من ١٠,٠٠٠)	٢٨٦٩	٪٢٩,٠
الفاقد من إجابات هذا السؤال	٨٨	٪٠,٩
المجموع	٩٨٩١	٪١٠٠

٤. الجنسيّة: شكّل السعوديين الغالبية العظمى من المشاركين بنسبة (٨٣,٢٪).

جدول رقم (٤)

يوضّح خصائص مجتمع الدراسة بحسب الجنسيّة

الجنسيّة	التكرار (ك)	النسبة (٪)
سعودي	٨٢٣٠	٪٨٣,٢
دول الخليج العربي	٤٨٦	٪٤,٩
الدول العربية الأخرى	٩٩٣	٪١٠,٠
دول آسيا غير العربية	٧٤	٪٠,٧
دول أفريقيا غير العربية	١٤	٪٠,١
الدول الأوروبية	٣٢	٪٠,٣

دول أمريكا الجنوبية	٧	٠,١٪
الولايات المتحدة الأمريكية وكندا	٣٧	٠,٤٪
الفاقد من إجابات هذا السؤال	١٨	٠,٢٪
المجموع	٩٨٩١	١٠٠٪

٥. المنطقة الأصلية للسعوديين: النسبة الأكبر من المشاركين السعوديين كانوا من المنطقة الوسطى حيث بلغت النسبة (٣٢,٣٪). ويوضح الجدول التالي ذلك:

جدول رقم (٥)يوضّح خصائص مجتمع الدراسة بحسب المنطقة الأصلية للسعوديين

المنطقة	التكرار (ك)	النسبة (٪)
المنطقة الغربية	٢٢٧٦	٢٣,٠٪
المنطقة الجنوبية	١٣١٧	١٣,٣٪
المنطقة الوسطى	٣١٩٦	٣٢,٣٪
المنطقة الشرقية	١١١٧	١١,٣٪
المنطقة الشمالية	٤٩٩	٥,٠٪
الفاقد من إجابات هذا السؤال	١٤٨٦	١٥,٠٪
المجموع	٩٨٩١	١٠٠٪

٦. المستوى التعليمي: أكثر من نصف المشاركين يحملون المؤهل الجامعي بنسبة (٥٧,٨٪).

جدول رقم (٦) يوضّح خصائص مجتمع الدراسة بحسب مستوى التعليم

مستوى التعليم	التكرار (ك)	النسبة (٪)
أقل من الثانوية	٧٢٤	٧,٣٪
ثانوي أو معهد	٢٥٥٥	٢٥,٥٪
جامعي	٥٧١٦	٥٧,٨٪

٧. نوع التخصص: النسبة الأكبر من المشاركين متخصصين في العلوم التطبيقية (٢٦,٣٪).

جدول رقم (٧) يوضّح خصائص مجتمع الدراسة بحسب نوع التخصص

نوع التخصص	التكرار (ك)	النسبة (٪)
تعليم عام	١٥٤٤	١٥,٦٪
علوم إدارية	١٢٩٦	١٣,١٪
علوم إنسانية	١٠٣٧	١٠,٥٪
علوم تطبيقية	٢٦٠٣	٢٦,٣٪
علوم شرعية	٨٩١	٩,٠٪
علوم أمنية وعسكرية	٤٦٩	٤,٧٪
حاسب آلي	١٩٠٨	١٩,٣٪
الفاقد من إجابات هذا السؤال	١٤٣	١,٤٪
المجموع	٩٨٩١	١٠٠٪

٨. الحالة الاجتماعية: يمثّل العزّاب أكثر من نصف مجتمع الدراسة (٥٣,٠٪)

جدول رقم (٨) يوضّح خصائص مجتمع الدراسة بحسب الحالة الاجتماعية

الحالة الاجتماعية	التكرار (ك)	النسبة (٪)
أعزب	٥٢٤٠	٥٣,٠٪
متزوج	٤٤٥٦	٤٥,١٪
مطلق	١٥٠	١,٥٪
أرمل	٢١	٠,٢٪
الفاقد من إجابات هذا السؤال	٢٤	٠,٢٪
المجموع	٩٨٩١	١٠٠٪

٩. الديانة:
الدين الإسلامي هو الدين الرسمي والوحيد للمملكة العربية السعودية، لذا فيمكن الجزم بأنّه لا يوجد أي مواطن سعودي غير مسلم، خاصة وأنّ مجتمعنا من المجتمعات المحافظة دينيا ولله الحمد والمنّة، إلاّ أنّ الانفتاح الاقتصادي للدولة، والتطور في جميع مرافقها، جعلها مقصداً للعمالة الأجنبية من جميع الجنسيات والأديان، ونظراً لأنّ الدراسة تشمل جميع مستخدمي شبكة الإنترنت في المجتمع السعودي، ومنهم ولا شك العمالة الوافدة بكل مستوياتها وجنسياتها ومعتقداتها، لذا فقد استلزم الأمر شمولية الدراسة لجميع الأديان والمعتقدات سواء السماوية أو غير السماوية، وقد كانت غالبية المشاركين في الدراسة من المسلمين، حيث بلغت نسبتهم (٩٨,٢٪) من مجموع المشاركين في الدراسة الميدانية.
ويوضح الجدول التالي ذلك وبشكل مفصل:
جدول رقم (٩)يوضّح خصائص مجتمع الدراسة بحسب نوع الديانة

نوع الديانة	التكرار (ك)	النسبة (٪)
مسلم	٩٧١٥	٪٩٨,٢٢
نصراني	١٠٧	٪١,٠٨
يهودي	١٢	٪٠,١٢
بوذي	٥	٪٠,٠٥
هندوسي	٤	٪٠,٠٤
لا ديني	٢٠	٪٠,٢٠
الفاقد من إجابات هذا السؤال	٢٨	٪٠,٢٨
المجموع	٩٨٩١	٪١٠٠

١٠. الحالة الوظيفية: كانت نسبة الطلاب المشاركين في الدراسة الميدانية أكثر من بقية الفئات الأخرى، حيث بلغت النسبة (٣٣,٧٪) من مجموع المشاركين في الدراسة الميدانية، يليهم الموظفين بنسبة (٣١,٢٪).
ويوضّح الجدول التالي ذلك مفصلاً:
جدول رقم (١٠)
يوضّح خصائص مجتمع الدراسة بحسب الحالة الوظيفية

الحالة الوظيفية	التكرار (ك)	النسبة (٪)
طالب	٣٣٣٦	٪٣٣,٧
عاطل	٣٨٩	٪٣,٩
عامل	١٦١	٪١,٦
موظف	٣٠٨٢	٪٣١,٢

عسكري	٦٧٢	٪٦,٣
مدرس	١٢٩٩	٪١٣,١
أستاذ جامعي	٢٠٣	٪٢,١
طبيب وصيدلي	١٩١	١,٩
رجال أعمال	٣٠٦	٣,١
ربة منزل	٢٧٥	٪٢,٨
الفاقد من إجابات هذا السؤال	٢٢	٪٠,٢
المجموع	٩٨٩١	٪١٠٠

١١. مستوى إجادة استخدام الحاسب الآلي: حوالي نصف مجتمع الدراسة يحسن استخدام الحاسب الآلي بشكل متوسط (٥٠,٣٪). ويوضح الجدول التالي ذلك:
جدول رقم (١١) يوضّح خصائص مجتمع الدراسة بحسب مستوى إجادة استخدام الحاسب الآلي

مستوى إجادة استخدام الحاسب الآلي	التكرار (ك)	النسبة (٪)
لا يجيد	١٢٧	٪١,٣
متوسط	٤٩٧٤	٪٥٠,٣
متقدم بالخبرة	٣٥٦٨	٪٣٦,١
متخصص بالحاسب الآلي	١١٩٤	٪١٢,١
الفاقد من إجابات هذا السؤال	٢٨	٪٠,٣
المجموع	٩٨٩١	٪١٠٠

١٢. مستوى إجادة استخدام الإنترنت: غالبية المشاركين في الدراسة يجيدون استخدام الإنترنت بشكل متوسط (٤٨,٩٪). ويوضح ذلك الجدول التالي:
جدول رقم (١٢) يوضّح خصائص مجتمع الدراسة بحسب مستوى إجادة استخدام الإنترنت

مستوى إجادة استخدام الإنترنت	التكرار (ك)	النسبة (٪)
لا يجيد	٦٦	٪٠,٧
متوسط	٤٨٣٩	٪٤٨,٩
متقدم بالخبرة	٤٠١٦	٪٤٠,٦
متخصص بالحاسب الآلي	٩٢٦	٪٩,٤
الفاقد من إجابات هذا السؤال	٤٤	٪٠,٤

المجموع	٩٨٩١	٪١٠٠

١٣. مستوى إجادة اللغة الإنجليزية: أكثر من نصف المشاركين في الدراسة الميدانية لديهم إلمام
متوسط باللغة الإنجليزية، حيث كانت نسبتهم (٥٩,٢٪) من مجموع المشاركين في الدراسة.

جدول رقم (١٣)يوضّح خصائص مجتمع الدراسة بحسب مستوى إجادة اللغة الإنجليزية

مستوى إجادة استخدام اللغة الإنجليزية	التكرار (ك)	النسبة (٪)
لا يجيد	١٤٥٧	٪١٤,٧
متوسط	٥٨٥٩	٪٥٩,٢
متمكّن	٢٤٥٧	٪٢٤,٨
لغته الأم الإنجليزية	٩١	٪٠,٩
الفاقد من إجابات هذا السؤال	٢٧	٪٠,٣
المجموع	٩٨٩١	٪١٠٠

مجال الزمنى للدراسة

تمّ تجميع البيانات الميدانية خلال فترة إثنى عشر شهراً قمرياً، أي سنة هجرية كاملة اعتباراً من ١٤٢٢/٩/١٥هـ الموافق ٢٠٠١/١١/٣٠م، إلى ١٤٢٣/٩/١٥هـ الموافق ٢٠٠٢/١١/٢٠م، وتعتبر هذه المدة كافية لجمع البيانات الميدانية اللازمة لأغراض الدراسة.

متغيرات الدراسة
يركّزْ الباحث على إثني عشر متغيراً أساسياً يساهموا في تحليل الدراسة الميدانية وهي :
يركز الباحث على اثني عشر متغيراً أساسياً يساهموا في تحليل الدراسة الميدانية وهي :
١. المستوى ألعمري (أخذ بتقسيم علم النفس حيث قسمت مراحل العمر التى يهمنا التعامل معها الى مرحلة الطفولة (٣-١٢) سنة، المراهقة (١٣-١٧) سنة، الشباب

(١٨-٢٥) سنة، أواسط العمر (٢٦-٥٠) سنة، الكهولة (٥١-٦٥) سنة، ومرحلة الشيخوخة (أكبر من ٦٥) سنة. (الهاشمي، ١٩٨٦م : ٧٣)

٢. الجنس (ذكر ، أنثى)

٣. المستوى الاقتصادي.

٤. الجنسية (سعودي، دول الخليج العربي، الدول العربية الأخرى، دول أسيا غير العربية، دول إفريقيا غير العربية، الدول الأوروبية، دول أمريكا الجنوبية والولايات المتحدة وكندا)

٥. المنطقة الأصلية للسعوديين (المنطقة الغربية، الجنوبية، الوسطى، الشرقية، الشمالية)

٦. المستوى التعليمي (أقل من الثانوي، ثانوي أو معهد، جامعي و دراسات عليا).

٧. الحالة الاجتماعية (أعزب، متزوج، مطلق و أرمل).

٨. نوع التخصص العلمي أو الفني (تعليم عام غير متخصص، علوم إدارية، علوم إنسانية، علوم تطبيقية وفنية، علوم شرعية، علوم أمنية وعسكرية، وعلوم الحاسب الآلي).

٩. الديانة (مسلم، نصراني، يهودي، بوذي، هندوسي، شيوعي، لا ديني)

١٠. الوظيفة (طالب، عاطل، عامل، موظف، عسكري، مدرس، أستاذ جامعة، طبيب وصيدلي في مستشفيات، أعمال حرة، وربة منزل).

١١. الخبرة في استخدام الحاسب الآلي (لا يجيد، منخفض، متوسط، متقدم بالخبرة، متخصص).

١٢. الخبرة في استخدام الإنترنت (لا يجيد، منخفض، متوسط، متقدم بالخبرة، متخصص).

١٣. الإلمام باللغة الإنجليزية (لا يجيد، نسبيا، بطلاقة، و لغته الأم).

اسلوب المعالجة الاحصائى

استخدم الباحث عدداً من الاختبارات والمقاييس الإحصائية، لتحليل البيانات الميدانية والإجابة عن التساؤلات الرئيسة في البحث. ومن أهم هذه الاختبارات الإحصائية:

١. معدل النسبة المئوية، لمنح مزيد من الإيضاح للظواهر المتصلة بجرائم الإنترنت.

٢. معامل ارتباط ألفا كرونباخ لتحديد معامل ثبات أداة الدراسة.

٣. اختبار كاي٢ لقياس العلاقة بين الخصائص والسمات الاجتماعية، لمستخدمي الإنترنت في المجتمع السعودي وميلهم نحو نمط معين من الجريمة عبر الإنترنت.

٤. اختبار جاما واختبار كرايمر (التوافق) لقياس قوة الارتباط بين الخصائص الاجتماعية والثقافية لمستخدمي الإنترنت في المجتمع السعودي وميلهم نحو نمط معين من الجريمة.

٥. اختبار الرجْوَل (stander Residual) لمعرفة قيمة البواقي المعيارية وتحديد قوة العلاقة والارتباط بين الخلايا الداخلية عند قياس المتغيّرات.

٦. اختبار لوقلنير (Log linear) وإخراج قيمة (Z) لمعرفة العلاقة بين المتغيّرات المستقلة والتابعة.
٧. اختبار الانحدار اللوجستيكي (logistic) لتوضيح أثر متغيرات الدراسة على احتمال ميل مستخدمي شبكة الإنترنت لارتكاب الجرائم.
٨. اختبار العامل التحليلي (Factor Analysis) لتوضيح أكثر جرائم الإنترنت انتشارا.

اداة الدراسة

تمّ استخدام أداة الاستبانة لجمع المعلومات الميدانية لهذه الدراسة، والتي تمّ تطويرها خصيصاً لأغراض هذه الدراسة، بعد الأخذ بالشروط العلمية اللازمة لتصميم الاستبانة، وبعد الرجوع إلى الكتب المنهجية المتخصصة في ذلك.
وتشمل الاستبانة سبعة محاور أساسية وزّعت على (٦٢) سؤالاً:
المحور الأول: يركّز على المتغيّرات الديموغرافية لأفراد الدراسة ويقيسها القسم الأول من الاستبانة أي الأسئلة من (١) إلى (١٣).
المحور الثاني: يعالج أنماط أكثر الجرائم الجنسيّة والممارسات غير الأخلاقية شيوعاً عبر الإنترنت، وتقيسها أسئلة القسم الثاني من الاستبانة أي من السؤال (١٤) إلى (٢٥).
المحور الثالث: يتناول أكثر أنماط جرائم الاختراقات شيوعاً، وخصّص لقياسه القسم الثالث من الأسئلة، أي من السؤال (٢٦) إلى (٤٤).
المحور الرابع: يحدد أنماط أكثر الجرائم المالية شيوعاً، ويقيسه القسم الرابع من أسئلة الاستبانة، أي السؤال (٤٥) إلى (٥٢).
المحور الخامس: يركّز على تحديد أنماط أكثر جرائم المواقع المعادية شيوعاً، والتي يتم إنشاؤها عبر الإنترنت، أو الاشتراك فيها، وتقيسها أسئلة القسم الخامس من الاستبانة من السؤال (٥٣) إلى (٥٨).
المحور السادس: يحدد أنماط أكثر جرائم القرصنة شيوعاً والتي تتمّ عبر الإنترنت، وتقيسها أسئلة القسم السادس من الاستبانة أي من السؤال (٥٩) إلى (٦٢).

صدق الأداة:

تمّ التأكّد من صدق المحتوى لأداة الدراسة بعرض الاستبانة بعد تصميمها على المشرف على الدراسة لأنّه من المتخصصين في المنهج العلمي، ومن ثَمَّ تَمَّ تحكيمها علمياً من قبل المتخصصين والخبراء في مجال العلوم الشرطية والاجتماعية والمهتمين بمناهج البحث العلمي، كما قام الباحث بالإجراءات المنهجية المطلوبة للتحقق من صدق وصحة صياغة عبارات الاستبانة، وذلك بتجريبها على عيّنة عشوائية من مستخدمي الإنترنت بلغت (٧٥) خمسة وسبعين مستخدماً، ومن ثَمَّ تَمَّ إخراج استبانة الدراسة في صورتها النهائية بعد إجراء التعديلات التي استلزم الأمر إجراءها من إضافة أو حذف أو تعديل.

ثبات الأداة:

اتّبَعَ الباحث القياس الإحصائي لقياس ثبات الاستبانة، وسلامة بناء الفقرات الخاصة بجرائم الإنترنت (الجرائم الجنسيّة والممارسات غير الأخلاقية، جرائم

الاختراقات، الجرائم المالية، الجرائم الخاصة بالمواقع المعادية، وجرائم القرصنة) والبالغ عددها (٤٩) تسع وأربعون فقرة، وذلك باستخدام الاتّساق الذاتي، وهي طريقة كرونباخ ألفا (Cronbach's Alpha)، لقياس مدى ثبات أداة الدراسة، وكان معامل الثبات (٠,٩٢) وهو قيمة ثبات عالية ومقبولة لغايات هذه الدراسة.

إجراءات الدراسة:

أ- تمّ عمل دراسة استطلاعية لمزودي خدمة الإنترنت في المملكة لتحديد أكثر جرائم الإنترنت شيوعاً في المجتمع السعودي.

ب- تمّ تصميم استبانة الدراسة وتوزيعها عبر كل الوسائل المتاحة لتصل إلى جميع مستخدمي الإنترنت في المجتمع السعودي، واتخذ لذلك الخطوات الآتية:

١. إنشاء موقع خاص لوضع استبانة الدراسة به ، وليَسْهُل على مستخدمي الإنترنت الوصول إليه، والإجابة على استبانة الدراسة.

٢. التعاقد مع مبرمج محترف لكتابة الاستبانة بلغة تسمح بنشرها في شبكة الإنترنت، مع وضع الضوابط اللازمة لمنع تكرار إجابة الشخص الواحد.

٣. ترجمة الاستبانة إلى اللغة الإنجليزية ليسهل على من لا يجيد اللغة العربية من غير السعوديين المقيمين في المملكة الإجابة على أسئلة الدراسة.

٤. كتابة نسخة من الاستبيان بصيغة الوورد (Microsoft Word)، مع استخدام النماذج الإلكترونية لتسهيل وتسريع اختيار الإجابة المناسبة من قبل المستخدمين.

٥. وضع إعلانات تشجيعية في عدّة مواقع مشهورة بشبكة الإنترنت لطلب المساهمة في هذه الدراسة من قبل مستخدمي الإنترنت في السعودية فقط.

٦. الاشتراك في عدد من القوائم البريدية ونشرها هناك.

٧. الاشتراك في عدد من ساحات الحوار والمنتديات ونشرها هناك.

٨. الدخول على مواقع المحادثات (chat) ونشر رابط الاستبيان هناك وطلب المساهمة في الدراسة.

٩. بعث الاستبانة بواسطة البريد الإلكتروني لعدد كبير جداً من العناوين البريدية الخاصة بمشتركين داخل المملكة بعد أن تمّ تجميع تلك العناوين على مدى سنتين.

١٠. تمّت الاستعانة بالمواقع التي لديها قاعدة بيانات لعناوين بريد الكترونية، وبعث الاستبيان إلى تلك العناوين مع التنويه إلى أنّ الدراسة قاصرة فقط على مواطني السعودية والمقيمين فيها من غير السعوديين.

١١. تمّ حصر عناوين البريد الإلكترونية لمدارس إدارات التعليم المختلفة بكافة أنحاء المملكة وبعث الاستبيان لهم.

١٢. وضع رابط الاستبانة في عدد من المواقع الشخصية المختلفة في الإنترنت، وطلب من أصحاب تلك المواقع بعث الرابط على مشتركي قائمتهم البريدية إن وجدت.

١٣. الاستعانة بمزودي خدمة الإنترنت لنشر رابط الاستبانة في مواقعهم، وكذلك توزيع الرابط على مشتركي الخدمة لديهم بواسطة البريد الإلكتروني.

١٤. مخاطبة مديري المواقع الحكومية بشبكة الإنترنت، كإدارات التعليم، لوضع رابط الاستبانة في مواقعهم وتوزيع الرابط على منسوبيهم.
١٥. التنسيق مع أصحاب المواقع شبه الحكومية، كنادي الحاسب الآلي، وشبكة المدينة المنورة، لوضع رابط الاستبيان في مواقعهم ونشر الرابط على مشتركي القائمة البريدية بموقعهم.
١٦. الاستعانة ببعض المشاركين في الدراسة وطلب المساهمة بنشر رابط الاستبانة على أكبر قدر ممكن من مستخدمي الإنترنت في السعودية، وقد حظيت الدراسة – بفضل الله- بقبول كبير بين أوساط مستخدمي الإنترنت، حيث تفاعلوا وبشكل غير متوقع في نشر الاستبيان في الكثير من المواقع والمنتديات، وعلى كثير من الأشخاص بإرسال الاستبيان على بريدهم الإلكتروني.
١٧. ساهمت وسائل الإعلام المقروءة -بعد ترحيبها بموضوع الدراسة- وبمساهمة ذاتية من قبل مندوبي الصحف المختلفة بنشر أخبار ومقالات ومقابلات تدور حول توضيح أهمية الدارسة وتشجع المشاركة فيها.
١٨. مخاطبة الشركات الكبرى المعروفة باستخدامها للشبكة الحاسوبية كأرامكو، وطلب توزيع استبانة الدراسة على منسوبيها.
١٩. حصر سفارات وقنصليات المملكة التي لها مواقع على شبكة الإنترنت، أو لهم بريد إلكتروني وبعث الاستبيان لهم.
٢٠. حصر السفارات والقنصليات العاملة بالمملكة وبعث الاستبيان على بريدهم الإلكتروني.
٢١. حصر الملحقيات والأكاديميات التعليمية السعودية بالخارج وبعث الاستبيان على بريدهم الإلكتروني.

منهج الدراسة

المنهج الذي تمّ استخدامه في هذه الدراسة، هو المسح الاجتماعي لجميع مستخدمي الإنترنت في المملكة العربية السعودية، والاستبانة هي أداة جمع معلومات الدراسة.

ويبدو أنّ استخدام أسلوب المسح الاجتماعي هو المنهج الملائم لمثل هذا الموضوع، باعتبار أنّه سيفيد في جمع معلومات وبيانات واقعية ومعاصرة من شرائح اجتماعية متعددة وكثيرة وغير متجانسة عن الظاهرة محل الدراسة.

مراجع الدراسة

أولا المراجع العربية :

ابن كثير (١٤٠٨هـ). تفسير القرآن الكريم. بيروت: دار الفكر.
ابن ماجة، أبي عبدالله محمد بن يزيد القزويني (١٣٩٥هـ). سنن ابن ماجة. (بدون): دار إحياء التراث العربي.
ابن منظور، أبو الفضل جمال الدين محمد بن مكرم (بدون). لسان العرب . بيروت: دار صادر.
أبو الحجاج، أسامة (١٩٩٨م). دليلك الشخصي إلى عالم الإنترنت. القاهرة : نهضة مصر.
أبو شامة، عباس (١٤٢٠هـ). التعريف بالظواهر الإجرامية المستحدثة، حجمها، أبعادها ونشاطها في الدول العربية، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية ، تونس، تونس، (٩-٣٩).
أبوزهرة، محمد (١٩٧٦م). الجريمة والعقوبة في الفقه الإسلامي. القاهرة: دار الفكر العربي.
أحمد، هلالي عبداله (٢٠٠٠م). تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي. عابدين : النسر الذهبي للطباعة.

بحر، عبدالرحمن محمد (١٤٢٠هـ). معوقات التحقيق في جرائم الإنترنت : دراسة مسحية على ضباط الشرطة في دولة البحرين. رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.
البخاري، أبي عبدالله محمد بن اسماعيل بن المغيرة (بدون). صحيح البخاري. (بدون): دار مطابع الشعب.
البداينة، ذياب (١٤٢٠هـ). جرائم الحاسب والإنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (٩٣-١٢٤).
البداينة، ذياب (١٩٩٩م). التطبيقات الاجتماعية للإنترنت، ورقة قُدّمت في الدورة التدريبية حول شبكة الإنترنت من منظور أمنى، أكاديمية نايف العربية للعلوم الأمنية، بيروت، لبنان.
البداينة، ذياب (١٩٨٨م). الأمن الوطني في عصر المعلومات. الجزيرة، ٩٤٢١.
البداينة، ذياب (١٩٩٧م). جرائم الحاسب الدولية، ورقة قُدّمت في ندوة جرائم الحاسب. معهد التدريب : أكاديمية نايف العربية للعلوم الأمنية ، الرياض، المملكة العربية السعودية.
البغوي، ابي محمد الحسين بن مسعود (١٤٠٩هـ). معالم التنزيل ((تفسير البغوي)). الرياض : دار طيبة للنشر والتوزيع.
البشري، محمد الأمين (١٤٢١هـ). التحقيق في جرائم الحاسب الآلي والإنترنت. المجلة العربية للدراسات الأمنية والتدريب دار الكتب العربية.
الترمذي، أبي عيسى بن عيسى بن سورة (١٣٩٨هـ). سنن الترمذي ((الجامع الصحيح)). (ط٣)، (بدون): دار الفكر.
تمّام، أحمد حسام طه (٢٠٠٠م). الجرائم الناشئة عن استخدام الحاسب الآلي. القاهرة : دار النهضة العربية.
الجنيدي، ماهر(أ) (١٩٩٩م). النصر للأقوى والأذكى والقذر، مجلة إنترنت العالم العربي، (نوفمبر ١٥(٣٠)، ٣١٧-٣٨٠.
بن أبي شيبة، أبو بكر عبدالله بن محمد (١٣٨٦هـ). المصنّف في الأحاديث والآثار. حيدر اباد: المطبعة العزيزية
بن همّام، عبدالرزاق (بدون). المصنّف. بيروت: المكتب الاسلامي.
البيضاوي، ناصر الدين عبدالله (بدون). تفسير البيضاوي ((أنوار التنزيل وأسرار التأويل)). (بدون) :)، ٣٦.

الجنيدي، ماهر(ب) (١٩٩٩م). رائحة الماريجوانا تنبعث من أوكار إنترنت ، مجلة إنترنت العالم العربي ، (نوفمبر)، ٣٩ – ٤٠.

الحازمي، خليل عبيد سالم (١٤٢٠هـ). أثر استخدام الحاسب الآلي في أداء الأجهزة الأمنية : دراسة مسحية على حرس الحدود بمدينة الرياض. رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

حبوش، طاهر عبدالجليل (١٤٢٠هـ). الوقاية والتأهيل والمكافحة للجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية ، تونس، تونس (٢٣٧-٣٠٧).

الحجي، خالد راشد (١٤٢١هـ). أمن الإنترنت. الرياض: مجلة الأمن (ع٥١).

الخليفة، عبدالله حسين (١٤٢٠هـ). البناء الاجتماعي والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية ، تونس، تونس (١٢٧-١٦٦).

الخليفة، عبدالله حسين (١٤١٣هـ). المحددات الاجتماعية لتوزيع الجريمة على أحياء مدينة الرياض. الرياض: مركز أبحاث مكافحة الجريمة.

داود، حسن طاهر (١٤٢١هـ). الحاسب وامن المعلومات. الرياض: معهد الإدارة العامة.
داود، حسن طاهر (١٤٢٠هـ). جرائم نظم المعلومات. الرياض : أكاديمية نايف العربية للعلوم الأمنية.

الدميني، مسفر غرم الله (١٤٠٢هـ). الجناية بين الفقه الإسلامي والقانون الوضعي. (ط.٢) الرياض : دار طيبة للنشر والتوزيع.

الدوري، عدنان (١٩٨٤م). أسباب الجريمة وطبيعة السلوك الإجرامي. (ط.٣) الكويت: ذات السلاسل.

الرازي، محمد بن أبي بكر بن عبد القادر (١٩٧٨ م). مختار الصحاح . بيروت : المكتبة الأموية.

رمضان، مدحت (٢٠٠٠م). جرائم الاعتداء على الأشخاص والإنترنت. القاهرة : دار النهضة العربية.

الزغاليل، أحمد سليمان (١٤٢٠هـ). الاتجار بالنساء والأطفال، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (٤٣-٩٠).

سالم، فادي (١٩٩٩م). عالم إنترنت السفلي، مجلة إنترنت العالم العربي ، (نوفمبر)، ٢٨ – ٣٥.

السجستاني، أبي داود سليمان الاشعث (بدون). سنن أبي داود. راجعه: محمد محي الدين عبدالحميد، (بدون) ، دار إحياء السنة النبوية.

سليم، طارق عبدالوهاب (١٩٩٧م). الجرائم المرتكبة بواسطة الإنترنت وسبل مكافحتها. بحث مقدم إلى الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة، مجلس وزراء الداخلية العرب، تونس، تونس، ٧-٩ يوليو ١٩٩٧م.

السمالوطي، نبيل محمد (١٤١١هـ). الدراسات العلمية للسلوك الإجرامي. جدة : دار الشروق.

سنن النسائي. (بدون). بشرح الحافظ جلال الدين السيوطي وحاشية السندي، بيروت: دار إحياء التراث العربي.
السيد، سمير (١٩٩٧م). محاضرات في شبكة المعلومات العالمية . القاهرة : مكتبة عين شمس.

السيف، محمد إبراهيم (١٤١٧هـ). الظاهرة الإجرامية في ثقافة وبناء المجتمع السعودي : بين التصور الاجتماعي وحقائق الاتجاه الإسلامي. الرياض : مكتبة العبيكان.

السيف، محمد إبراهيم (١٤١٤هـ). العوامل الاجتماعية المرتبطة بنمط الجريمة الجنسيّة. رسالة دكتوراة غير منشورة، قسم الاجتماع، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية.

شتا، محمد محمد (٢٠٠١م). فكرة الحماية الجنائية لبرامج الحاسب الآلي. الإسكندرية: دار الجامعة الجديدة للنشر.

الشنيفي، عبدالرحمن عبدالعزيز (١٤١٤هـ). أمن المعلومات وجرائم الحاسب الآلي. (ط١) الرياض : بدون.

الشهاوي، قدري عبدالفتاح (١٩٩٩م). أساليب البحث العلمي الجنائي والتقنية المتقدمة. الإسكندرية :منشأة المعارف.

الشهري، عبدالله محمد صالح (١٤٢٢هـ). المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي : دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض، المملكة العربية السعودية.

الشهري، فايز عبدالله (١٤٢٢هـ). استخدامات شبكة الإنترنت في مجال الإعلام الأمني العربي. مجلة البحوث الأمنية ، ١٠(١٩)، ١٦٥-٢١٤.

صحيفة عكاظ، العدد ١٢٧٨٩، ١٤٢٢/٦/١٣هـ، الصفحة الأولى.

الصليفيح، حمد (١٤٠٧هـ). حقوق الإنسان في الإسلام والوقاية من انحراف الأحداث. الرياض : المركز العربي للدراسات الأمنية والتدريب (أكاديمية نايف العربية للعلوم الأمنية).

طالب، أحسن (١٩٩٨م). الجريمة والعقوبة والمؤسسات الإصلاحية. الرياض : دار الزهراء.

عبدالرحمن، خالد حمدي (١٩٩٢م)، الحماية القانونية للكيانات المنطقية. رسالة دكتوراه غير منشورة، جامعة عين شمس، القاهرة، جمهورية مصر العربية.

عبدالمطلب، ممدوح عبدالحميد (٢٠٠١ م). جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية : الجريمة عبر الإنترنت. الشارقة: مكتبة دار الحقوق.

عجب نور، أسامة محمد (١٤١٧هـ). جريمة الرشوة في النظام السعودي. الرياض : معهد الإدارة العامة.

عزالدين، أحمد جلال (١٤١٤هـ). أساليب التعاون العربي في مجال التخطيط لمواجهة جرائم الإرهاب. الرياض : أكاديمية نايف العربية للعلوم الأمنية.

العسال، أحمد محمد (١٤٠٧هـ). التكافل الاجتماعي في الإسلام ودوره في الوقاية من انحراف الإحداث. الرياض : المركز العربي للدراسات الأمنية والتدريب (أكاديمية نايف العربية للعلوم الأمنية).

عودة، عبدالقادر (١٤٠١هـ). التشريع الجنائي الإسلامي. بيروت : مؤسسة الرسالة، (المجلد الأول).

عيد، محمد فتحي (١٤٢٢هـ). الاتجار غير المشروع بالمخدرات والمؤثرات العقلية. الرياض : أكاديمية نايف العربية للعلوم الأمنية.
عيد، محمد فتحي (١٤١٩هـ). الإجرام المعاصر. الرياض : أكاديمية نايف العربية للعلوم الأمنية.

الفرج، عبدالرحمن، والمصري، أيمن (١٤١٩هـ). المملكة العربية السعودية على الإنترنت. الرياض، مجلة مكتبة الملك فهد الوطنية، م ٤(١)، ٦٢-٦٨.

فرحات، محمد نعيم (١٤٠٤هـ). التشريع الجنائي الإسلامي. جدة : مكتبة الخدمات الحديثة.

الفرم، خالد فيصل عبدالمحسن (١٤٢٢هـ). شبكة الإنترنت وجمهورها في مدينة الرياض : دراسة تطبيقية في ضوء نظرية الاستخدامات والإشباعات، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض، المملكة العربية السعودية.

الفنتوخ، عبدالقادر (١٤٢١هـ). الإنترنت للمستخدم العربي. الرياض: مكتبة العبيكان.
فهمي، علاء الدين، وآخرون (١٩٩١م). الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني. موسوعة دلتا كمبيوتر ٢ : مطابع المكتب المصري الحديث.

الفيروزآبادي، مجد الدين محمد بن يعقوب (١٩٨٧م). القاموس المحيط. (ط٢). بيروت: مؤسسة الرسالة.

القدهي، مشعل عبدالله (١٤٢٢هـ). المواقع الإباحية على شبكة الإنترنت وأثرها على الفرد والمجتمع. [١٤٢٢/٧/٢٩هـ] http://www.minshawi.com/gadhi.htm

القرطبي، محمد أحمد الانصاري (١٩٨٦م). الجامع لاحكام القرآن. (ط٣). القاهرة: دار القلم.

كاره، مصطفى عبدالمجيد (١٩٨٥م). مقدمة في الانحراف الاجتماعي. بيروت : معهد الإنماء العربي

الماوردي، محمد حبيب (١٤٠٧هـ). الأحكام السلطانية. القاهرة : دار التراث العربي.

مجلة آفاق الإنترنت (١٩٩٧)، إنترنت ٢، المؤلف، السنة ١ (٣)، ٣٨-٤١.

مجلة المجلة (٢٠٠٠م)، سعودي يخترق موقع (ياهو) ويعطله لمدة سبع دقائق، مجلة المجلة، (١٠٦٣)، ٤٢-٤٣.

مجلس وزراء الداخلية العرب (١٤١٨هـ). وثائق الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة. الأمانة العامة : تونس.

محمد، عادل ريان (١٩٩٥م)، جرائم الحاسب الآلي وأمن البيانات، العربي ، (٤٤٠)، ٧٣ – ٧٧ .

مراد، عبدالفتاح (١٩٩١م). موسوعة القضاء والفقه للدول العربية. الإسكندرية : المكتب الجامعي الحديث.

المسالمة، هشام أحمد (٢٠٠١م). جرائم نظم المعلومات والإنترنت. بحث علمي قانوني مقدّم لنيل لقب أستاذ في المحاماة، درعة : مكتب الخنساء.

مسند الإمام أحمد بن حنبل (١٣٩٨هـ). (ط٢)، بيروت: دار الفكر.

المسند، صالح محمد، و المهيني، عبدالرحمن راشد (١٤٢١هـ). التحقيق في جرائم الحاسب الآلي والإنترنت . المجلة العربية للدراسات الأمنية والتدريب ١٥(٢٩)، ١٤٧-٢٠٧.
مندورة، محمد محمود (١٤١٠هـ). جرائم الحاسب الآلية، دورة فيروس الحاسب الآلي، مكتب الأفاق المتحدة : الرياض ، ١٩ – ٢٦.

منصور، عبدالمجيد سيد أحمد (١٤١٠هـ). السلوك الإجرامي والتفسير الإسلامي. الرياض : مركز أبحاث الجريمة.

موقع صحيفة الجزيرة - القرية الإلكترونية (١٤٢١/٢/٢) http://www.al-jazirah.com/2000/may/6/ev.htm#evt3

موقع أرابيا (٢٠٠١/٦/١٠م)
http://www.arabia.com/tech/article/arabic/0,4884,48801,00.html

موقع إسلام أون لاين (٢٠٠٠/١٠/٢٩)
http://www.islamonline.net/Arabic/news/10/29/2000-rticle9
موقع السوق الخليجي (١٤٢٣/٤/١هـ)
http://www.gulfforum.com/ksa1/20/1.html
موقع المركز السعودي لمعلومات الشبكة (١٤٢٣/٢/٨هـ)
http://www.saudinils.net.sa/too.htm/estimating%20thenumber%20.htm

موقع بوابة عجيب (٢٠٠١/٣/٢٥م)
http://it.ajeeb.com/viewarticle=1662&category=34

موقع بوابة عجيب (٢٠٠١/٨/٨م)
http://it.ajeeb.com/viewarticle.asp?article=1976&category=17

موقع صحيفة البي بي سي (٢٠٠١)
http://news.bbc.co.uk/hi/arabic/news/newsid_1550000/1550726.stm

موقع صحيفة البي بي سي (٢٠٠٠/٦/١٢م)
http://news.bbc.co.uk/hi/arabic/news/newsid_1382000/1382266.stm

موقع صحيفة البي بي سي (٢٠٠٠م)
http://news.bbc.co.uk/hi/arabic/news/newsid_989000/989047

موقع صحيفة البي بي سي (٢٠٠٠م)
http://news.bbc.co.uk/hi/arabic/news/newsid_993000/993502

موقع صحيفة البيان (٢٠٠٠/٥/١٩)
http://www.albayan.co.ae/albayan/2000/05/19/mhl/2.htm

موقع صحيفة الجزيرة (٢٠٠٠) http://www.al-jazirah.com/

موقع صحيفة الرياض (١٤٢٣/١٠/١٣هـ)
http://www.alriyadh.com.sa/Contents/17-12002/RiyadhNet/COV_941.php

موقع صحيفة الرياض (١٤٢٣/١٠/١٠هـ)
http://www.alriyadh.com.sa/Contents/14-12-002/RiyadhNet/News_1414.php

موقع صحيفة الشرق الأوسط (٢٠٠٠)
http://www.asharqalawsat.com/aaasumframe/pc/technology/technology.html

موقع مجلة الأمن الإلكترونية (١٤٢١/٧/٢٢هـ)
http://safola.com/security.chtml

موقع مجلس التعاون لدول الخليج العربية (١٤٢٣/٤/٢هـ) http://www.gcc-sg.org/index.html

موقع محامو المملكة (١٤٢٣/٤/٢هـ)
http://www.mohamoon-ksa.com/dir.asp?DirID=1&Status=1

موقع منتدى الفوائد (١٤٢١ /٨/١٤هـ)
http://216.122.89.86/muntada/postings.cgi?action=newtopic&number=1&forum

موقع وحدة خدمات الإنترنت(١٤٢٣/٢/٨هـ)http://www.isu.net.sa/ar/faqs.html

موقع وزارة التجارة (١٤٢٣/٤/٢هـ)
http://www.commerce.gov.sa/aboutus/leg1.asp?print=true

النحلاوي، عبدالرحمن (١٤٠٣هـ). أصول التربية الإسلامية وأساليبها : في البيت والمدرسة والمجتمع. دمشق: دار الفكر.

نشرة تعريفية عن مدينة الملك عبدالعزيز للعلوم والتقنية (١٤١٩هـ). الرياض: الإدارة العامة للتوعية العلمية والنشر.

النيسابوري، أبي الحسين مسلم بن الحجاج القشيري (١٣٧٥هـ). صحيح مسلم. (ط١)، (بدون): دار إحياء التراث العربي.

الهاشمي، عبدالحميد محمد (١٩٨٦م). علم النفس التكويني: أسسه وتطبيقه من الولادة إلى الشيخوخة، (الطبعة الثانية). القاهرة: مكتبة الخانجي.

اليامي، محمد (١٩٩٨م). رجال الأعمال ينطلقون إلى الاستفادة من فرص التجارة الإلكترونية. الحياة ، الملحق ، (٩٤- ١٢٩).
اليوسف، عبدالله عبدالعزيز (١٤٢٠هـ). التقنية والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (١٩٥- ٢٣٣).

ثانيا: المراجع الأجنبية:

Adsit,, C. Kristin. (1999). Internet Pornography Addiction. http://www.chemistry.vt.edu/chem-[Online]. Available: [9.3.2001].dept/ dessy/honors /papers99/adsit.htm

Glabosky,PN,&Smith. Russell G.(1998). Crime in the Digital Age. Australia: Transaction Publishers & The Federation Press.

Highley, Reid. (1999). Viruses: The Internet's Illness.[Online]. Available: http://www.chemistry.vt.edu/chem-dept/dessy/honors [9.3.2001]./papers99/highleh.htm

Koerner, B. I. (1999,November 22). Only you can prevent computer intrusions. U.S. News and World Report, 127, pp. 50.

Morningstar, Steve. (1998). Internet Crime and Criminal Procedures.[Online]. http://www.prevent-abuse-now.com/index.htmlAvailable: [13.10.2001].

Nanoart. (2000) [Online].
[15.11.2000].http://www.nanoart.f2s.com/hack/Available:

NUA Internet Surveys. (1998,June). How Many Online? [Online].
Available:
http://www.nua.ie/surveys/howmayonline/index.html
[26.10.2000].

NUA Internet Surveys. (1998,June). How Many Online? [Online].
Available:
http://www.nua.ie/surveys/howmayonline/index.html
[6.11.2000].

NUA Internet Surveys.(1998,June). How Many Online? [Online].
Available:
http://www.nua.ie/surveys/howmayonline/index.html
[10.7.2000].
Rapalus, P.(2000,May). Ninety percent of survey respondents detect cyber attacks. Computer Security Institute. [Online]. Available:
[11.10.2001].http://www.gocsi.com/prelen_000321.htm

Reuvid, Jonathan. (1998). The Regulation and Prevention of Economic Crime, London: Kogan, 14.
Skinner, W. F., & Fream, A. M. (1997, November). A social learning theory analysis of computer crime among college students. Journal of research in Crime and Delinquency, 34 (4), 495-519.

Staff. (2000, April 2). The Business of Technology.
www.redherring.com/mag/issue7/news-Available:http://
[11.10.2001]. security.html

Staff. (2000, February 17). Information Assurance Capabilities Brief : ACS Defense, Inc.

Sweeny, Paul. (Jul/Aug 1999). Cyber-crime's Looming Threat. Banking Strategies, 75, 54-59.

Thomas, P. (2000, February 23). Insufficient computer security threatens doing business. [Online]. Available: http://www.cnn.com/2000/TECK/computing/02/23/credir.c [11.11.2001].ard.thefts/index.html

Thompson, R. (1999, February). Chasing after petty computer crime. IEEE Potentials, 18 (1), 20-22.

Tim, W. (1998) Profits Embolden Hackers. Internet week (March: 23) P. P1-12.

Vacca, John. (1996). Internet Security Secrets.USA:IDG Book. Worldwide Inc.

Wilson, c. (2000) Holding management accountable: a new policy for protect against computer crime. Proceedings of the National Aerospace and Electronics Conference, USA 2000, 272-281.

نتائج الدراسة

أهم النتائج:

اولاً: حجم جرائم الانترنت وهي:

١. أنّ حجم الجرائم الجنسيّة والممارسات غير الأخلاقية التي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: ارتياد المواقع الجنسيّة ويرتكبها (٥٣٤١) مستخدم، أو ما نسبته (٥٤,٣٪) من مجموع المشاركين في الدراسة الميدانية، (١٦٧٥) مستخدم أو ما نسبته (١٩,٢٪) طلبوا مواد إباحية منها، (١٧٩١) مستخدم أو ما نسبته (١٨,٣٪) اشتركوا في القوائم البريدية الجنسيّة، (٢٣٥) مستخدم أو ما نسبته (٢,٤٪) أنشئوا موقعاً جنسياً، (٤١٠) مستخدم أو ما نسبته (٤,٢٪) قاموا بإنشاء قوائم بريدية جنسيّة، (٢٨٣) مستخدم أو ما نسبته (٢,٩٪) قاموا بالتشهير بالآخرين ، (٢٧٨) مستخدم أو ما نسبته (٢,٨٪) شُهّرَ بهم، (٤٢٨)

مستخدم أو ما نسبته (٤,٤٪) شُهّرَ بأقارب لهم، (٤٠٥٥) مستخدم أو ما نسبته (٤١,٢٪) استخدموا البروكسي لتجاوز المواقع المحجوبة، (١٦٦٠) مستخدم أو ما نسبته (١٦,٩) استخدموا برامج إخفاء الشخصية أثناء تصفح الإنترنت، (١١٥٦) مستخدم أو ما نسبته (١١,٨٪) استخدموا برامج إخفاء الشخصية لإرسال البريد الالكتروني، (١١٥٣) مستخدم أو ما نسبته (١١,٧٪) انتحلوا شخصية الآخرين أثناء التصفح أو استخدام البريد.

٢. أنّ حجم أكثر جرائم الاختراقات شيوعاً التي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: (١٣٤٨) مستخدم أو ما نسبته (١٣,٧٪) من مجموع المشاركين في الدراسة الميدانية قاموا بتدمير المواقع، (٣٨١) مستخدم أو ما نسبته (٣,٩٪) دُمّرَتْ مواقعهم، (٥٤٨) مستخدم أو ما نسبته (٥,٦٪) اخترقوا مواقع حكومية، (٥٢٩) مستخدم أو ما نسبته (٥,٣٪) اخترقوا مواقع تجارية، (٨٦٩) مستخدم أو ما نسبته (٨,٩٪) اخترقوا مواقع شخصية، (٣٧٦) مستخدم أو ما نسبته (١٣,٢٪) اخترقوا مواقع محلية، (١٤٠) مستخدم أو ما نسبته (٥,٠٪) اخترقوا مواقع خليجية، (٨٣) مستخدم أو ما نسبته (٢,٩٪) اخترقوا مواقع عربية غير خليجية، (٨٨) مستخدم أو ما نسبته (٣,١٪) اخترقوا مواقع آسيوية غير عربية، (٩) مستخدم أو ما نسبته (٠,٣٪) اخترقوا مواقع أفريقية غير عربية، (٥١) مستخدم أو ما نسبته (١,٨٪) اخترقوا مواقع أوروبية، (١٤) مستخدم أو ما نسبته (٠,٥٪) اخترقوا مواقع أمريكية جنوبية، (٢٢١) مستخدم أو ما نسبته (٧,٨٪) اخترقوا مواقع في الولايات المتحدة الأمريكية وكندا، (١٨٦٠) مستخدم أو ما نسبته (٦٥,٤٪) لا يذكرون المواقع التي اخترقوها، (٤٥٦) مستخدم أو ما نسبته (٤,٧٪) تعرّضت مواقعهم للاختراق، (١٦٨٨) مستخدم أو ما نسبته (١٧,٣٪) اخترقوا أجهزة شخصية، (٣٢٧٨) مستخدم أو ما نسبته (٣٣,٣٪) تعرضت أجهزتهم الشخصية للاختراق، (١٤٧٩) مستخدم أو ما نسبته (١٥,١٪) قاموا باختراق البريد الإلكتروني، (١٥٣١) مستخدم أو ما نسبته (١٥,٦٪) تعرّض بريدهم الإلكتروني للاختراق، (١٥٧٠) مستخدم أو ما نسبته (١٦,٠٪) قاموا بالاستيلاء على البريد الإلكتروني، (١٠٨٤) مستخدم أو ما نسبته (١١,٠٪) تم الاستيلاء على بريدهم الإلكتروني، (١٠١٧) مستخدم أو ما نسبته (١٠,٣٪) قاموا بإغراق البريد الإلكتروني، (١٨٣٢) مستخدم أو ما نسبته (١٨,٦٪) تعرّض بريدهم الإلكتروني للإغراق، (١٦٩٧) مستخدم أو ما نسبته (١٧,٣٪) استولوا على اشتراك الآخرين، (١٥٣١) مستخدم أو ما نسبته (١٥,٦٪) تم الاستيلاء على اشتراكهم، (١٢١١) مستخدم أو ما نسبته (١٢,٣٪) قاموا بإرسال فيروسات أو تروجنات، (٥١٣٨) مستخدم أو ما نسبته (٥٢,٢٪) تضرروا من الفيروسات.

٣. أنّ حجم الجرائم والممارسات المالية التي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: (٤٣٥) مستخدم أو ما نسبته (٤,٤٪) قاموا بالاستيلاء على البطاقات الائتمانية، (١٢٦) مستخدم أو ما نسبته (١,٣٪) تم الاستيلاء على بطائقهم الائتمانية، (٥٠٠) مستخدم أو ما نسبته (٥,١٪) لعبوا القمار، (٤٤٤) مستخدم أو ما نسبته (٤,٥٪) قاموا بالتزوير عبر الإنترنت، (٤١٤) مستخدم أو ما نسبته (٤,٢٪)

ارتادوا مواقع الجريمة المنظمة، (٢٩٠) مستخدم أو ما نسبته (٣,٠٪) ارتادوا مواقع المخدرات، (١٧٧) مستخدم أو ما نسبته (١,٨٪) ارتادوا مواقع غسيل الأموال، (٧٩١) مستخدم أو ما نسبته (٤٢,٢٪) من مرتادي مواقع الجريمة المنظمة أو المخدرات أو غسيل الأموال كان هدفهم الاستفادة العلمية من هذه المواقع، (٨٣٩) مستخدم أو ما نسبته (٤٤,٧٪) كان هدفهم الفضول أو من باب المصادفة، (١٠٦) مستخدم أو ما نسبته (٥,٧٪) كان هدفهم تنفيذ الأفكار الإجرامية التي تنشرها تلك المواقع، (١٣٩) مستخدم أو ما نسبته (٧,٤٪) كان هدفهم الانضمام إلى تلك المنظمات الإجرامية.

٤. أنّ حجم جرائم وممارسات إنشاء المواقع المعادية أو الاشتراك فيها والتي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: (٢٦١) مستخدم أو ما نسبته (٢,٦٪) قاموا بإنشاء مواقع سياسية معادية، (١٣٣٦) مستخدم أو ما نسبته (١٣,٦٪) اشتركوا طوعاً في المواقع السياسية المعادية، (٧٣٦) مستخدم أو ما نسبته (٧,٥٪) تعرضوا للاشتراك القهري في المواقع السياسية المعادية، (٥٦١) مستخدم أو ما نسبته (٥,٧٥٪) قاموا بإنشاء مواقع دينية، منهم (٥٠٠) مستخدم أو ما نسبته (٥,١١٪) أنشئوا مواقع سنية، (٤٣) مستخدم أو ما نسبته (٠,٤٣٪) أنشئوا مواقع شيعية ، (٥) مستخدم أو ما نسبته أنشئوا (٠,٠٥٪) مواقع نصرانية، (٣) مستخدم أو ما نسبته (٠,٠٣٪) أنشئوا مواقع يهودية، (٢) مستخدم أو ما نسبته (٠,٠٢٪) أنشئوا مواقع بوذية، (٣) مستخدم أو ما نسبته (٠,٠٣٪) أنشئوا مواقع هندوسية، (٥) مستخدم أو ما نسبته (٠,٠٥٪) أنشئوا مواقع لا دينية.

(٣٧٢٨) مستخدم أو ما نسبته (٣٨,٠٦٪) اشتركوا في القوائم الدينية، منهم (٣٤٥٥) مستخدم أو ما نسبته (٣٥,٣٠٪) اشتركوا في المواقع السنية، (١٩٠) مستخدم أو ما نسبته (١,٩٣٪) اشتركوا في المواقع الشيعية، (٢٩) مستخدم أو ما نسبته (٠,٢٩٪) اشتركوا في المواقع النصرانية، (١٠) مستخدم أو ما نسبته (٠,١٠٪) اشتركوا في المواقع اليهودية، (٦) مستخدم أو ما نسبته (٠,٠٦٪) اشتركوا في المواقع البوذية، (١٢) مستخدم أو ما نسبته (٠,١٢٪) اشتركوا في المواقع الهندوسية، (٢٦) مستخدم أو ما نسبته (٠,٢٦٪) اشتركوا في المواقع اللا دينية.

(٢٩٢) مستخدم أو ما نسبته (٣,٠٪) قاموا بإنشاء مواقع معادية للأشخاص أو الجهات.

٥. أنّ حجم أكثر جرائم القرصنة شيوعاً والتي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: (٣٩٥) مستخدم أو ما نسبته (٤,٠٪) قاموا بإنشاء مواقع للبرامج المقرصنة، (٣٠٩١) مستخدم أو ما نسبته (٣١,٥٪) قاموا بتحميل برامج مقرصنة، (٣١٨٢) مستخدم أو ما نسبته (٣٢,٤٪) استخدموا برامج تشغيل البرامج المقرصنة، (٥٧٧) مستخدم أو ما نسبته (٥,٩٪) قاموا بإنشاء مواقع مقرصنة.

ثانياً: سمات وخصائص مرتكبي جرائم الإنترنت في المجتمع السعودي:

يمكن تلخيصها وبحسب متغيرات الدراسة في النقاط الآتية: أولاً: الفئة العمرية:

١. الأطفال (١٢ سنة فأقل): يقوى احتمال ميلهم لارتياد مواقع غسيل الأموال

(٧,٥٤)، ارتياد مواقع المخدرات (٧,١٢)، التزوير (٥,٨٠)، ارتياد مواقع الجريمة المنظمة (٥,٥١)، لعب القمار (٤,٠٣)، الاستيلاء على البطاقات الائتمانية (٣,٦٨)، إنشاء المواقع السياسية المعادية (٣,٢٥)، انتحال الشخصية (٢,٨٤)، تدمير المواقع (٢,٣٧)، إنشاء المواقع الجنسيّة (٢,٢٠)، اختراق المواقع (٢,١١)، الاشتراك في المواقع السياسية المعادية (١,٨٥)، اختراق الأجهزة الشخصية (١,٣٥)، الاعتداء على البريد الالكتروني (١,١٨)، وأخيراً استخدام البروكسي (١,٠٧).

٢.المراهقة (١٣-١٧سنة): يقوى احتمال ميلهم لارتياد مواقع الجريمة المنظمة (١,٨٨)، إنشاء المواقع السياسية المعادية (١,٨٧)، لعب القمار (١,٥٠)، الاستيلاء على البطاقات الائتمانية (١,٤٧)، الاعتداء على البريد الالكتروني (١,٤٤)، التزوير (١,٣٩)، اختراق الأجهزة الشخصية (١,٣١)، إنشاء المواقع الجنسيّة (١,٢٣)، انتحال الشخصية (١,١٩)، إنشاء المواقع المقرصنة (١,١٨)، تدمير المواقع (١,١٤)، ارتياد مواقع غسيل الأموال (١,٠٩)، ارتياد المواقع الجنسيّة (١,٠٨)، وأخيراً إنشاء مواقع للتشهير بالآخرين (١,٠٦).

٣. الشباب (١٨-٢٥سنة): يقوى احتمال ميلهم لارتياد المواقع الجنسيّة (١,٧٥)، إنشاء المواقع السياسية المعادية (١,٦٠)، الاستيلاء على البطاقات الائتمانية (١,٤٤)، ارتياد مواقع الجريمة المنظمة (١,٤٢)، التزوير (١,٣٨)، اختراق الأجهزة الشخصية (١,٣١)، استخدام البروكسي (١,١٩)، الاعتداء على البريد (١,١٠)، لعب القمار (١,١٠)، ارتياد مواقع المخدرات (١,٠٦)، وأخيراً انتحال الشخصية (١,٠٣).

٤. أواسط العمر (٢٦-٥٠ سنة): يقوى احتمال ميلهم لارتياد المواقع الجنسيّة (١,٥٥)، استخدام البروكسي (١,٣٧)، وأخيراً لعب القمار (١,٢٧).

٥. الكهولة (٥١-٦٥ سنة): يقوى احتمال ميلهم لإنشاء مواقع للتشهير بالآخرين (١,٣٨)، وإنشاء مواقع للبرامج المقرصنة (١,٢٥).

٦. الشيخوخة (أكبر من ٦٥ سنة): انعدم احتمال ميلهم لارتكاب أي جريمة.

ثانياً: الجنس (ذكر– أنثى): يقوى احتمال ميل الذكور لارتكاب جميع الجرائم والأفعال التي تطرقت إليها الدراسة، في حين ينعدم احتمال ميل الإناث لذلك.

ثالثاً: مستوى الدخل الشهري: (منخفض – متوسط – مرتفع)لم يكن هذا المتغيّر مؤثراً في احتمال الميل لارتكاب أي جريمة أو فعل من التي تطرقت إليها الدراسة.

رابعاً: الجنسيّة:

١. السعوديين: يقوى احتمال ميلهم فقط لإنشاء المواقع المقرصنة (١,١٥).

٢. مواطني الدول الخليجية الأخرى: يقوى احتمال ميلهم لإنشاء المواقع المقرصنة (٣,٤٩)، إنشاء مواقع البرامج المقرصنة (٢,٧٣)، و الاشتراك في المواقع السياسية المعادية (١,٩٥).

٣. الدول العربية الأخرى: يَقِلّ احتمال ميلهم لارتكاب الجرائم والأفعال التي شملتها الدراسة.

٤. دول آسيا غير العربية: يقوى احتمال ميلهم فقط لإنشاء مواقع البرامج المقرصنة

(١,١٠).
٥. دول أفريقيا غير العربية: يقوى احتمال ميلهم لإنشاء مواقع التشهير بالأشخاص (٩,٩٣)، التزوير (٩,٧٢)، إنشاء المواقع المقرصنة (٩,١٧)، إنشاء المواقع الجنسيّة (٨,٩٨)، إنشاء مواقع البرامج المقرصنة (٨,٨٤)، ارتياد مواقع المخدرات (٨,٤٨)، استخدام ما يساعد على تشغيل البرامج المقرصنة (٧,٦٦)، الاستيلاء على البطاقات الائتمانية (٧,٥٦)، انتحال الشخصية (٧,٠١)، تحميل البرامج المقرصنة (٦,٨٣)، اختراق الأجهزة (٦,٧٤)، إنشاء المواقع السياسية المعادية (٦,٠٣)، اختراق المواقع (٥,٧٦)، إنشاء المواقع المعادية للأشخاص أو الجهات (٥,٧١)، لعب القمار (٥,٦٧)، الاعتداء على البريد (٤,٦٢)، الاشتراك في المواقع السياسية المعادية (٤,٠٣)، استخدام البروكسي (٤,٠٢)، وأخيراً استخدام برامج إخفاء الشخصية (٣,٧١).
٦. مواطني الدول الأوروبية: يَقِلّ احتمال ميلهم لارتكاب الجرائم والأفعال التي شملتها الدراسة.
٧. مواطني دول أمريكا الجنوبية: يقوى احتمال ميلهم لإنشاء مواقع البرامج المقرصنة (٨,٧٥)، إنشاء مواقع للتشهير بالأشخاص (٦,٣٦)، إنشاء المواقع الجنسيّة (٥,٨٤)، استخدام ما يساعد على تشغيل البرامج المقرصنة (٥,٧٤)، تحميل البرامج المقرصنة (٤,٤٩)، إنشاء المواقع المقرصنة (٤,٤٨)، التزوير (٣,٦٣)، اختراق المواقع (٣,٢٣)، إنشاء المواقع السياسية المعادية (٣,١٣)، اختراق الأجهزة الشخصية (٢,٩٣)، استخدام البروكسي (٢,٦٨)، إنشاء المواقع المعادية للأشخاص أو الجهات (٢,٥١)، انتحال الشخصية (٢,٥٠)، الاعتداء على البريد (١,١٨)، الاشتراك في المواقع السياسية المعادية (١,٣٦)، وأخيراً استخدام برامج إخفاء الشخصية (١,٠١).
٨. مواطني الولايات المتحدة الأمريكية وكندا: ينعدم احتمال ميلهم لارتكاب الجرائم والأفعال التي تطرقت إليها الدراسة.

خامساً: المنطقة الأصلية للسعوديين:

١. المنطقة الغربية: يقوى احتمال ميلهم للعب القمار (١,١٧)، اختراق الأجهزة (١,١٥)، استخدام البروكسي (١,٠٦)، استخدام ما يساعد على تشغيل البرامج المقرصنة (١,٠٣)، وأخيراً استخدام برامج إخفاء الشخصية (١,٠٠).
٢. المنطقة الجنوبية: يقوى احتمال ميلهم فقط للاشتراك في المواقع السياسية المعادية (١,٠٣).
٣. المنطقة الوسطى: يقوى احتمال ميلهم للاشتراك في المواقع السياسية المعادية (١,١٨)، استخدام ما يساعد على تشغيل البرامج المقرصنة (١,١٥)، استخدام البروكسي (١,١٣)، وأخيراً اختراق الأجهزة الشخصية (١,٠١).
٤. المنطقة الشرقية: يقوى احتمال ميلهم للعب القمار (١,٢٧)، استخدام ما يساعد على تشغيل البرامج المقرصنة (١,٠٥)، وأخيراً استخدام برامج إخفاء الشخصية (١,٠٢).
٥. المنطقة الشمالية: ينعدم احتمال ميلهم لارتكاب الجرائم والأفعال التي شملتها

الدراسة.

سادساً المستوى التعليمي:
١. اقل من الثانوي: يقوى احتمال ميلهم لإنشاء المواقع المعادية للأشخاص أو الجهات (١,٥٩)، تدمير المواقع (١,٣٥)، ارتياد مواقع الجريمة المنظمة (١,٢٦)، استخدام برامج إخفاء الشخصية (١,٢٤)، انتحال الشخصية (١,٢٣)، اختراق المواقع (١,١٩)، إنشاء مواقع التشهير بالأشخاص (١,١٦)، إنشاء المواقع السياسية المعادية (١,١٣)، التزوير (١,١٢)، إنشاء مواقع البرامج المقرصنة (١,١١)، استخدام البروكسي (١,٠٧)، وأخيراً الاستيلاء على البطاقات الائتمانية (١,٠٣).
٢. ثانوي أو معهد: يقوى احتمال ميلهم إنشاء مواقع التشهير بالأشخاص (١,٤٢)، ارتياد مواقع غسيل الأموال (١,٣٥)، الاستيلاء على البطاقات الائتمانية (١,٣١)، إنشاء مواقع البرامج المقرصنة (١,٢١)، ارتياد المواقع الجنسيّة (١,١٨)، ارتياد مواقع الجريمة المنظمة (١,١٧)، استخدام البروكسي (١,١٢)، انتحال الشخصية (١,١٠)، تدمير المواقع (١,٠٩)، التزوير (١,٠٤)، اختراق المواقع (١,٠٢)، استخدام برامج إخفاء الشخصية (١,٠١)، إنشاء المواقع السياسية المعادية (١,٠٠)، وأخيراً إنشاء المواقع المعادية للأشخاص أو الجهات (١,٠٠).
٣. جامعي: يقوى احتمال ميلهم لارتياد المواقع الجنسيّة (١,٢٠)، استخدام البروكسي (١,٠٩)، وأخيراً الاشتراك في المواقع السياسية المعادية (١,٠٤).
٤. دراسات عليا: ينعدم احتمال ميلهم لارتكاب الجرائم والأفعال التي شملتها الدراسة.

سابعاً: نوع التخصص:
١. تعليم عام : يقوى احتمال ميلهم لإنشاء المواقع المقرصنة (١,٢٠)، ارتياد مواقع غسيل الأموال (١,١٦)، اختراق الأجهزة الشخصية (١,١٠)، وأخيراً الاعتداء على البريد (١,٠٥).
٢. علوم إدارية: يقوى احتمال ميلهم لارتياد مواقع غسيل الأموال (١,٤٥)، لعب القمار (١,٤٤)، وأخيراً ارتياد المواقع الجنسيّة (١,١٧).
٣. علوم إنسانية: يقوى احتمال ميلهم لارتياد مواقع غسيل الأموال (١,٨٠)، الاستيلاء على البطاقات الائتمانية (١,٣٨)، إنشاء المواقع المقرصنة (١,٢٢)، ارتياد المواقع الجنسيّة (١,٠٩)، وأخيراً اختراق المواقع (١,٠٦).
٤. علوم تطبيقية: يقوى احتمال ميلهم لارتياد مواقع غسيل الأموال (١,٩٣)، استخدام ما يساعد على تشغيل البرامج المقرصنة (١,١٩)، ارتياد المواقع الجنسيّة (١,١٧)، لعب القمار (١,١٥)، تحميل البرامج المقرصنة (١,٠٥)، اختراق المواقع (١,٠٢)، وأخيراً تدمير المواقع (١,٠١).
٥. علوم شرعية: يقوى احتمال ميلهم فقط لتدمير المواقع (١,١٥).
٦. علوم عسكرية: يقوى احتمال ميلهم للاستيلاء على البطاقات الائتمانية (٢,٤٢)، لعب القمار (١,٧٠)، اختراق الأجهزة الشخصية (١,٢٥)، اختراق المواقع (١,٢٤)، إنشاء المواقع المقرصنة (١,٢٤)، تحميل البرامج المقرصنة (١,٢٠)،

ارتياد مواقع غسيل الأموال (١,١٨)، تدمير المواقع (١,١٤)، الاعتداء على البريد (١,١٤)، استخدام ما يساعد على تشغيل البرامج المقرصنة (١,١٤)، وأخيراً ارتياد المواقع الجنسيّة (١,٠٢).

٧. حاسب آلي: ينعدم احتمال ميلهم لارتكاب الجرائم والأفعال التي شملتها الدراسة.

ثامناً: الحالة الاجتماعية (أعزب – متزوج – مطلق – أرمل)

١. العزاب: يقوى احتمال ميلهم للتزوير (٤,٠٧)، إنشاء مواقع للبرامج المقرصنة (٣,٤٢)، الاستيلاء على البطاقات الائتمانية (٣,٢٥)، استخدام البرامج المقرصنة (٣,٠٩)، استخدام البروكسي (٢,٨٨)، استخدام ما يساعد على تشغيل البرامج المقرصنة (٢,٦٨)، استخدام برامج إخفاء الشخصية (٢,٦٤)، تدمير المواقع (٢,٥١)، ارتياد مواقع غسيل الأموال (٢,١٩)، انتحال الشخصية (٢,١٦)، إنشاء المواقع المعادية للأشخاص أو الجهات (٢,٠٢)، الاعتداء على البريد (٢,٠٠)، الاشتراك في المواقع السياسية المعادية (١,٨٦)، إنشاء المواقع السياسية المعادية (١,٧٧)، ارتياد مواقع المخدرات (١,٦٧)، إنشاء المواقع المقرصنة (١,٦١)، ارتياد مواقع الجريمة المنظمة (١,٥٢)، اختراق المواقع (١,١٦).

٢. المتزوجون: يقوى احتمال ميلهم لتحميل البرامج المقرصنة (١,٧٦)، استخدام البروكسي (١,٧٣)، استخدام برامج إخفاء الشخصية (١,٦٨)، استخدام ما يساعد على تشغيل البرامج المقرصنة (١,٦٦)، تدمير المواقع (١,٤٣)، التزوير (١,٣٧)، انتحال الشخصية (١,٣٤)، الاشتراك في المواقع السياسية المعادية (١,٢٠)، إنشاء مواقع للبرامج المقرصنة (١,١٣)، إنشاء المواقع السياسية المعادية (١,٠٦)، الاعتداء على البريد (١,٠٢).

٣. المطلقون: يقوى احتمال ميلهم للتزوير (٩,١٥)، الاستيلاء على البطاقات الائتمانية (٨,٧٥)، إنشاء المواقع السياسية المعادية (٨,٣٢)، ارتياد مواقع المخدرات (٨,٢٠)، إنشاء مواقع للبرامج المقرصنة (٨,١٥)، ارتياد مواقع غسيل الأموال (٧,٢٤)، إنشاء المواقع المعادية للأشخاص أو الجهات (٦,٩٥)، إنشاء المواقع المقرصنة (٦,٧٧)، ارتياد مواقع الجريمة المنظمة (٥,٩٣)، تدمير المواقع (٥,٣٦)، انتحال الشخصية (٤,٩٢)، استخدام برامج إخفاء الشخصية (٤,٠٩)، الاشتراك في المواقع السياسية المعادية (٣,٨٩)، تحميل البرامج المقرصنة(٣,٨٦)، استخدام ما يساعد على تشغيل البرامج المقرصنة (٣,١٧)، استخدام البروكسي (٣,٦٠)، إنشاء مواقع للتشهير بالآخرين (١,٩٠)، الاعتداء على البريد (١,٨٧)، اختراق المواقع (١,٧٤)، إنشاء المواقع الجنسيّة (١,٥٢)، ارتياد المواقع الجنسيّة (١,٤٧)، ارتياد مواقع القمار (١,٢٧).

٤. الأرامل: يقوى احتمال ميلهم لارتياد مواقع غسيل الأموال (٨,٦٣)، ارتياد مواقع المخدرات (٦,٥٨)، ارتياد مواقع الجريمة المنظمة (٤,٦٤)، إنشاء المواقع المقرصنة (٤,٢٢)، استخدام البروكسي (٣,٥٤)، الاستيلاء على البطاقات الائتمانية (٣,٢٠)، إنشاء المواقع المعادية للأشخاص أو الجهات (٢,٧٢)، الاعتداء على البريد (٢,٥٢)، انتحال الشخصية (٢,٣٧)، تحميل البرامج المقرصنة (٢,٠٥)، إنشاء مواقع للبرامج المقرصنة (١,٩٩)، التزوير (١,٩٧)، الاشتراك في

المواقع السياسية المعادية (١,٩٥)، استخدام ما يساعد على تشغيل البرامج المقرصنة (١,٥٢)، إنشاء المواقع الجنسيّة (١,٥٠)، تدمير المواقع (١,١٢)، لعب القمار (١,١٢)، وأخيراً استخدام برامج إخفاء الشخصية (١,٠٥).

تاسعا: الديانة

١. المسلمون: يَقِلّ احتمال ميلهم لارتكاب الجرائم والأفعال التي شملتها الدراسة.

٢. النصارى: يقوى احتمال ميلهم لإنشاء مواقع البرامج المقرصنة (٦,٣٥)، إنشاء المواقع المقرصنة (٦,٠٢)، إنشاء المواقع المعادية للأشخاص أو الجهات (٤,٢٩)، تحميل البرامج المقرصنة (٣,٢٧)، انتحال الشخصية (٣,١١)، اختراق الأجهزة الشخصية (٢,٨٢)، اختراق المواقع (٢,٣٥)، تدمير المواقع (٢,٣٣)، إنشاء مواقع للتشهير بالأشخاص (٢,٢١)، إنشاء المواقع الجنسيّة (٢,١٦)، إنشاء المواقع السياسية المعادية (٢,٠٥)، استخدام برامج إخفاء الشخصية (١,٨١)، ارتياد مواقع المخدرات (١,٦٨)، استخدام ما يساعد على تشغيل البرامج المقرصنة (١,٦٨)، الاستيلاء على البطاقات الائتمانية (١,٥٨)، لعب القمار (١,٤٣)، الاشتراك في المواقع السياسية المعادية (١,٤٢)، الاعتداء على البريد (١,٣٦)، وأخيراً ارتياد المواقع الجنسيّة (١,٠٤).

٣. اليهود: يقوى احتمال ميلهم لاستخدام ما يساعد على تشغيل البرامج المقرصنة (٥,٢٣)، إنشاء مواقع البرامج المقرصنة (٤,٧٩)ارتياد مواقع غسيل الأموال (٣,٦٠)، إنشاء المواقع المعادية للأشخاص أو الجهات (٢,٦٦)، استخدام البروكسي (١,٩٤)، انتحال الشخصية (١,٩٢)، الاشتراك في المواقع السياسية المعادية (١,٧٨)، وأخيراً ارتياد مواقع الجريمة المنظمة (١,٢٥).

٤. البوذيين: يقوى احتمال ميلهم للتزوير (٩,٦٩)، الاعتداء على البريد (٧,٧١)، تحميل البرامج المقرصنة (٧,٦٣)، إنشاء المواقع الجنسيّة (٧,٠٤)، اختراق الأجهزة الشخصية (٥,٧٦)، الاستيلاء على البطاقات الائتمانية (٥,٨٩)، الاشتراك في المواقع السياسية المعادية (٥,٥٦)، ارتياد مواقع المخدرات (٥,٣٢)، استخدام البروكسي (٤,٨٨)، استخدام برامج إخفاء الشخصية (٤,٢٨)، إنشاء المواقع المعادية للأشخاص أو الجهات (٣,٨٢)، اختراق المواقع (٣,٦٨)، ارتياد المواقع الجنسيّة (٣,٢٩)، لعب القمار (٣,٢٦)، تدمير المواقع (٣,١٠)، وأخيراً ارتياد مواقع الجريمة المنظمة (١,٧٤).

٥. الهندوس: يقوى احتمال ميلهم لتدمير المواقع (٩,٩٠)، إنشاء مواقع للتشهير بالأشخاص (٩,٢٩)، إنشاء المواقع المقرصنة (٩,١٠)، الاستيلاء على البطاقات الائتمانية (٨,٨٣)، اختراق المواقع (٨,٥٦)، إنشاء المواقع الجنسيّة (٨,٤٢)، استخدام ما يساعد على تشغيل البرامج المقرصنة (٨,٠٥)، التزوير (٦,٩٧)، الاعتداء على البريد (٦,٤٤)، إنشاء المواقع السياسية المعادية (٦,٣٥)، ارتياد مواقع المخدرات (٦,٢٨)، استخدام برامج إخفاء الشخصية (٦,٢٦)، استخدام البروكسي (٥,٤٩)، لعب القمار (٥,١٨)، ارتياد المواقع الجنسيّة (٥,١٦)، إنشاء مواقع للبرامج المقرصنة (٤,٤٠)، ارتياد مواقع غسيل الأموال (٤,٣٢)، اختراق الأجهزة الشخصية (٤,٢٦)، ارتياد مواقع الجريمة المنظمة (٢,٣٧)، انتحال

الشخصية (١,٥٠)، وأخيراً تحميل البرامج المقرصنة (١,٠٧).
٦. اللادينيين: ينعدم احتمال ميلهم لارتكاب الجرائم والأفعال التي شملتها الدراسة.
عاشرا: الحالة الوظيفية:
١. الطلبة: يقوى احتمال ميلهم لانتحال الشخصية (١,٤٠)، تحميل البرامج المقرصنة (١,٢٦)، الاعتداء على البريد (١,٢١)، التزوير (١,١٢)، إنشاء المواقع المعادية للأشخاص أو الجهات (١,١٠)، تدمير المواقع (١,٠٥)، وأخيراً اختراق الأجهزة الشخصية (١,٠٤).
٢. العاطلين: يقوى احتمال ميلهم للعب القمار (١,٧٧)، إنشاء المواقع الجنسيّة (١,٧٣)، التزوير (١,٦٤)، إنشاء مواقع للتشهير بالأشخاص (١,٣٥)، تحميل البرامج المقرصنة (١,٣٢)، انتحال الشخصية (١,٢٩)، إنشاء المواقع المعادية للأشخاص أو الجهات (١,٢٣)، الاعتداء على البريد (١,١١)، تدمير المواقع (١,١٠)، وأخيراً اختراق المواقع (١,١٠).
٣. العمال: يقوى احتمال ميلهم لإنشاء المواقع الجنسيّة (٢,٦٥)، إنشاء مواقع البرامج المقرصنة (١,٩٣)، الاستيلاء على البطاقات الائتمانية (١,٨٠)، ارتياد المواقع الجنسيّة (١,٦١)، تحميل البرامج المقرصنة (١,٣٥)، تدمير المواقع (١,٢٩)، وأخيراً اختراق الأجهزة الشخصية (١,٠٥).
٤. الموظفين: يقوى احتمال ميلهم لارتياد المواقع الجنسيّة (١,١٣)، ولعب القمار (١,٠٥).
٥. العسكريين: يقوى احتمال ميلهم لإنشاء المواقع المعادية للأشخاص أو الجهات (١,٣٧)، إنشاء المواقع الجنسيّة (١,٢٢)، التزوير (١,١٩)، اختراق المواقع (١,١٧)، تدمير المواقع (١,١٣)، اختراق الأجهزة الشخصية (١,٠٩)، الاعتداء على البريد (١,٠٦)، وأخيراً إنشاء مواقع للبرامج المقرصنة (١,٠٤).
٦. المدرسين: يقوى احتمال ميلهم للتزوير (١,٣٧)، إنشاء مواقع للبرامج المقرصنة (١,٢٧)، وأخيراً انتحال الشخصية (١,٠٠).
٧. أساتذة الجامعة: يقوى احتمال ميلهم لإنشاء مواقع للتشهير بالأشخاص (١,٣٠)، انتحال الشخصية (١,١٧)، وأخيراً إنشاء المواقع المعادية للأشخاص أو الجهات (١,٠٣).
٨. الأطباء والصيادلة: يقوى احتمال ميلهم للتزوير (٢,٧٨)، إنشاء مواقع التشهير بالأشخاص (٢,٥٣)، الاستيلاء على البطاقات الائتمانية (١,٨٤)، إنشاء المواقع المعادية للأشخاص أو الجهات (١,٦٨)، إنشاء المواقع الجنسيّة (١,٤٨)، لعب القمار (١,٤٣)، إنشاء مواقع للبرامج المقرصنة (١,٣٣)، انتحال الشخصية (١,٢٨)، تدمير المواقع (١,١٠)، وأخيراً تحميل البرامج المقرصنة (١,١٠).
٩. رجال الأعمال: يقوى احتمال ميلهم لإنشاء المواقع المعادية للأشخاص أو الجهات (٣,٤٨)، الاستيلاء على البطاقات الائتمانية (٢,٤٢)، إنشاء مواقع للتشهير بالأشخاص (٢,٣٧)، التزوير (٢,١٢)، لعب القمار (٢,٠٧)، اختراق المواقع (١,٨٤)، إنشاء مواقع للبرامج المقرصنة (١,٨٤)، تدمير المواقع (١,٦٨)، الاعتداء على البريد (١,٤٣)، إنشاء المواقع الجنسيّة (١,٤٠)، اختراق

الأجهزة الشخصية (١,٢٥)، انتحال الشخصية (١,١٦)، تحميل البرامج المقرصنة (١,١١)، وأخيراً ارتياد المواقع الجنسيّة (١,٠٨).

١٠. ربات المنازل: ينعدم احتمال ميلهم لارتكاب الجرائم والأفعال التي شملتها الدراسة.

حادي عشر: مستوى إجادة استخدام الحاسب الآلي:

١. لا يجيد استخدام الحاسب الآلي: يقوى احتمال ميلهم للتزوير (٣,٠٩)، إنشاء المواقع المقرصنة (٢,٨٧)، إنشاء المواقع الجنسيّة (٢,٧٧)، الاستيلاء على البطاقات الائتمانية (٢,٤٨)، ارتياد مواقع غسيل الأموال (٢,٣٨)، اختراق المواقع (١,٧٢)، إنشاء مواقع للبرامج المقرصنة (١,٤٥)، استخدام برامج إخفاء الشخصية (١,٠٧)، وأخيراً الاعتداء على البريد (١,٠٢).

٢. يجيد استخدام الحاسب بشكل متوسط: يقوى احتمال ميلهم فقط لإنشاء المواقع الجنسيّة (١,٠٦).

٣. مُتقدّم في استخدام الحاسب بالخبرة: يقوى احتمال ميلهم لاستخدام البروكسي (١,٠٢)، اختراق الأجهزة الشخصية (١,٠٠)، وأخيراً تحميل البرامج المقرصنة (١,٠٠).

٤. متخصص بالحاسب الآلي: يقوى احتمال ميلهم لاستخدام ما يساعد على تشغيل البرامج المقرصنة (١,٩٤)، تحميل البرامج المقرصنة (١,٨٨)، اختراق الأجهزة الشخصية (١,٧٤)، إنشاء مواقع للبرامج المقرصنة (١,٤٩)، تدمير المواقع (١,٤٦)، استخدام البروكسي (١,٤٢)، إنشاء المواقع المقرصنة (١,٣٦)، الاستيلاء على البطاقات الائتمانية (١,٣٥)، الاعتداء على البريد (١,٢٢)، اختراق المواقع (١,١٨)، وأخيراً استخدام برامج إخفاء الشخصية (١,١٦).

ثاني عشر: مستوى إجادة استخدام الإنترنت:

١. لا يجيد استخدام الإنترنت: يقوى احتمال ميلهم فقط لإنشاء مواقع البرامج المقرصنة (١,٠٠).

٢. يجيد استخدام الإنترنت بشكل متوسط: يقوى احتمال ميلهم للتزوير (١,٧٥)، وإنشاء المواقع السياسية المعادية (١,٥٠).

٣. مُتقدّم في استخدام الإنترنت بالخبرة: يقوى احتمال ميلهم لارتياد المواقع الجنسيّة (١,١٨)، إنشاء المواقع السياسية المعادية (١,١٥)، الاعتداء على البريد (١,١٠)، إنشاء المواقع الجنسيّة (١,٠٩)، وأخيراً الاشتراك في المواقع السياسية المعادية (١,٠٦).

٤. متخصص بالحاسب الآلي: يقوى احتمال ميلهم للاعتداء على البريد (٢,١٣)، الاشتراك في المواقع السياسية المعادية (٢,٠٧)، إنشاء المواقع الجنسيّة (١,٩٨)، استخدام ما يساعد على تشغيل البرامج المقرصنة (١,٩٤)، ارتياد المواقع الجنسيّة (١,٨٧)، استخدام البروكسي (١,٨٤)، ارتياد مواقع غسيل الأموال (١,٨٤)، اختراق الأجهزة الشخصية (١,٧٦)، إنشاء مواقع للتشهير بالأشخاص (١,٧٤)، تدمير المواقع (١,٦٥)، تحميل البرامج المقرصنة (١,٦٤)، التزوير (١,٦٠)، اختراق المواقع (١,٥٧)، استخدام برامج إخفاء الشخصية (١,٤٦)،

ارتياد مواقع الجريمة المنظمة (١,٤٢)، انتحال الشخصية (١,٣٦)، إنشاء المواقع السياسية المعادية (١,٣٥)، إنشاء المواقع المقرصنة (١,٣٤)، وأخيراً إنشاء المواقع المعادية للأشخاص أو الجهات (١,٠١).

ثالث عشر: مستوى إجادة اللغة الإنجليزية:

١. لا يجيد اللغة الإنجليزية: يقوى احتمال ميلهم لارتياد مواقع غسيل الأموال (١,٠٩)، و إنشاء المواقع السياسية المعادية (١,٠٠).

٢. يجيد اللغة الإنجليزية بشكل متوسط: يَقِلّ احتمال ميلهم لارتكاب الجرائم والأفعال التي شملتها الدراسة.

٣. متمكّن من اللغة الإنجليزية: يقوى احتمال ميلهم فقط لارتياد مواقع الجريمة المنظمة (١,٢٦)

ثالثا: أكثر الجرائم والممارسات انتشاراً:

يستخدم الباحث هنا اختباراً إحصائيا أكثر تقدماً وهو اختبار (Factor Analysis)
أو ما يعرف باختبار التحليل العاملي، وذلك لترتيب الجرائم والممارسات بحسب أكثرها شيوعاً، فالمتوسطة الشيوع، ومن ثم الأقلّ شيوعاً، وحرصاً على الخروج بنتائج دقيقة وغير مضللة فقد تم استبعاد الأسئلة المتعلقة بمتغيرات الدراسة، وهي أسئلة القسم الأول من استبانة الدراسة والتي تحدد معلومات ديمغرافية للمبحوث، ويمثلها الأسئلة رقم (١-١٣)، وكذلك تم استبعاد الأسئلة التي تعبر عن الجرائم والممارسات التي يكون المستخدم فيها ضحية وهي الأسئلة (٢٠،٢١، ٢٧، ٣٢، ٣٤، ٣٦، ٣٨، ٤٠، ٤٢، ٤٤، ٤٦، ٥٥)،
كما تم أيضاً استبعاد الأسئلة التوضيحية التي تفيد فقط في توضيح إجابة سابقة وهي :
سؤال (٣١) كونه يحدد مستوى الاختراق الذي قام بها المستخدم.
وسؤال (٥٢) كونه يوضّح سبب ارتياد المستخدم لمواقع الجريمة المنظمة، المواقع الخاصة بالمخدرات، ومواقع غسيل الأموال.

أمّا باقي أسئلة الاستبانة وعددها (٣٥) سؤال فقد دخلت في اختبار التحليل العاملي (Factor Analysis)، ونتج عن ذلك الجدول التالي والذي يوضّح فيه تقسيم الجرائم والممارسات التي يرتكبها مستخدم الإنترنت في المجتمع السعودي بحسب شيوعها، والتي أتضح منها:

١. أنّ أكثر جرائم وممارسات الإنترنت شيوعاً في المجتمع السعودي هي جرائم الاختراقات.

٢. يليها الجرائم المالية وجرائم المواقع المعادية كجرائم وممارسات متوسطة الشيوع.

٣. وأخيراً اظهر الاختبار الجرائم والممارسات الأقلّ شيوعاً وهي الجرائم الجنسيّة وممارسة الأفعال غير الأخلاقية.

ويوضّح الجدول التالي ذلك مفصلا:

جدول رقم (٩٦)

اختبار التحليل العاملي (Factor Analysis)

يوضّح أكثر الجرائم شيوعاً عند مستخدمي شبكة الإنترنت في المجتمع السعودي

التسلسل	الجرائم الرئيسة الشائعة	الارتباط	الجرائم المتوسطة الشيوع	الارتباط	الجرائم الأقلّ شيوعاً	الارتباط
١	اختراق الأجهزة الشخصية	٠,٧٧	ارتياد مواقع المخدرات	٠,٧٣	ارتياد المواقع الجنسيّة	٠,٧١
٢	اختراق البريد الالكتروني	٠,٧٤	إنشاء المواقع الجنسيّة	٠,٧١	الاشتراك في القوائم الجنسيّة	٠,٧٠
٣	إرسال الفيروسات/التروجنات	٠,٧٣	إنشاء المواقع السياسية المعادية	٠,٧٠	طلب مواد إباحية	٠,٦٦
٤	اختراق المواقع الشخصية	٠,٦٩	إنشاء المواقع المعادية للأشخاص أو الجهات	٠,٦٩	استخدام البروكسي	٠,٥٥
٥	تدمير المواقع	٠,٦٩	إنشاء مواقع للتشهير بالأشخاص	٠,٦٣	الاشتراك في المواقع السياسية المعادية	٠,٣٥
٦	إغراق البريد الالكتروني	٠,٦٥	ارتياد مواقع غسيل الأموال	٠,٥٦		
٧	الاستيلاء على الاشتراك	٠,٥٩	لعب القمار	٠,٥٦		
٨	اختراق المواقع التجارية	٠,٥٧	التزوير	٠,٥٤		
٩	الاستيلاء على البريد	٠,٥٥	إنشاء قائمة	٠,٥٤		

			بريدية جنسيّة			
١٠	تحميل البرامج المقرصنة	٠,٥٤	الاستيلاء على البطاقات الائتمانية	٠,٥٣		
١١	استخدام برامج إخفاء الشخصية أثناء إرسال البريد	٠,٥٢	إنشاء مواقع للبرامج المقرصنة	٠,٥٢		
١٢	تشغيل البرامج المقرصنة	٠,٥٢	إنشاء المواقع الدينية	٠,٥١		
١٣	اختراق المواقع الحكومية	٠,٥١	ارتياد مواقع الجريمة المنظمة	٠,٤٨		
١٤	انتحال الشخصية	٠,٥٠	إنشاء مواقع مقرصنة	٠,٤٥		
١٥	استخدام برامج إخفاء الشخصية أثناء التصفح	٠,٤٩	الاشترا ك في القوائم الدينية	٠,٣١		
	قيمة ايجن = ٦,٧٤ التباين المفسر = ١٩,٢٦		قيمة ايجن = ٦,٠٩ التباين المفسر = ١٧,٤٠		قيمة ايجن = ٢,٧٢ التباين المفسر= ٧,٧٩	

k.m.o = ٠,٩٤ صفر = (sig)

يلاحظ من قِيَمْ الجدول السابق أنّ قيمة اختبار k.m.o والتي تساوي (٠,٩٤)، تعنى أنّ هناك كفاية بالعيّنة، وأنّ حجم المتغيرات قابل للتعامل مع اختبار التحليل العاملي

(Factor Analysis). كما يلاحظ من قيمة ايجنت (الجزء الكامن) والتباين المفسر الآتي:

١. الجرائم الرئيسة الشائعة عند مستخدمي شبكة الانترنت في المجتمع السعودي تنحصر في عدد (١٥) جريمة أو فعل ممارس والتي يمكن أنْ تُدْرج تحت تصنيف جرائم الاختراقات وهي:

١. اختراق الأجهزة الشخصية (٠,٧٧).
٢. اختراق البريد الالكتروني (٠,٧٤).
٣. إرسال الفيروسات أو التروجنات (٠,٧٣).
٤. اختراق المواقع الشخصية (٠,٦٩).
٥. تدمير المواقع (٠,٦٩).
٦. إغراق البريد الالكتروني (٠,٦٥).
٧. الاستيلاء على الاشتراك (٠,٥٩).
٨. اختراق المواقع التجارية (٠,٥٧).
٩. الاستيلاء على البريد الالكتروني (٠,٥٥).
١٠. تحميل البرامج المقرصنة (٠,٥٤).
١١. استخدام برامج إخفاء الشخصية أثناء إرسال البريد (٠,٥٢).
١٢. استخدام ما يساعد على تشغيل البرامج المقرصنة (٠,٥٢).
١٣. اختراق المواقع الحكومية (٠,٥١).
١٤. انتحال الشخصية أثناء التصفح أو إرسال البريد الالكتروني (٠,٥٠).
١٥. استخدام برامج إخفاء الشخصية أثناء التصفح (٠,٤٩).

يلاحظ أنّ قيمة ايجنت (الجزء الكامن) للجرائم الأكثر شيوعا بين مستخدمي شبكة الإنترنت في المجتمع السعودي هي (٦,٧٤)، وان التباين المفسر (١٩,٢٦).

٢. الجرائم المتوسطة الشيوع عند مستخدمي شبكة الإنترنت في المجتمع السعودي تنحصر أيضاً في (١٥) جريمة أو فعل ممارس والتي يمكن أنْ تُدْرج تحت تصنيف الجرائم المالية وجرائم المواقع المعادية وهي:

١. ارتياد مواقع المخدرات (٠,٧٣).
٢. إنشاء المواقع الجنسيّة (٠,٧١).
٣. إنشاء المواقع السياسية المعادية (٠,٧٠).
٤. إنشاء المواقع المعادية للأشخاص أو الجهات (٠,٦٩.).
٥. إنشاء مواقع للتشهير بالأشخاص (٠,٦٣).
٦. ارتياد مواقع غسيل الأموال (٠,٥٦).
٧. لعب القمار (٠,٥٦).
٨. التزوير (٠,٥٤).
٩. إنشاء قائمة بريدية جنسيّة (٠,٥٤).
١٠. الاستيلاء على البطاقات الائتمانية (٠,٥٣).
١١. إنشاء مواقع للبرامج المقرصنة (٠,٥٢).
١٢. إنشاء المواقع الدينية (٠,٥١).

١٣. ارتياد مواقع الجريمة المنظمة (٠,٤٨).
١٤. إنشاء المواقع المقرصنة (٠,٤٥).
١٥. الاشتراك في القوائم الدينية (٠,٣١).
يلاحظ أنّ قيمة ايجنت (الجزء الكامن) للجرائم المتوسطة الشيوع بين مستخدمي شبكة الإنترنت في المجتمع السعودي هي (٦,٠٩)، وان التباين المفسر (١٧,٤٠).

٣. الجرائم الأقلّ شيوعاً بين مستخدمي شبكة الإنترنت في المجتمع السعودي
تنحصر في (٥) جرائم أو فعل ممارس والتي يمكن أنْ تُدْرج تحت تصنيف الجرائم الجنسيّة وممارسة الأفعال غير الأخلاقية، وهي:
١. ارتياد المواقع الجنسيّة (٠,٧١).
٢. الاشتراك في القوائم الجنسيّة (٠,٧٠).
٣. طلب مواد إباحية (٠,٦٦).
٤. استخدام البروكسي (٠,٥٥).
٥. الاشتراك في المواقع السياسية المعادية (٠,٣٥).
يلاحظ أنّ قيمة ايجنت (الجزء الكامن) للجرائم الأقلّ شيوعا بين مستخدمي شبكة الإنترنت في المجتمع السعودي هي (٢,٧٢)، وان التباين المفسر (٧,٧٩).

توصيات البحث:

من نتائج الدراسة الميدانية يمكن صياغة بعض التوصيات ذات العلاقة بنتائج الدراسة ومن أهمّها:

.1أظهرت نتائج الدراسة أنّ هناك الكثير من الجرائم والممارسات غير الأخلاقية التي يرتكبها مستخدمو شبكة الإنترنت في المجتمع السعودي. وعليه توصي هذه الدراسة بوضع ضوابط واضحة وصريحة وصالحة للتعامل مع هذه الجرائم والممارسات غير الأخلاقية، وبما يحدّ من خطورة هذه الأفعال وردع مرتكبيها، مع تفعيل ما هو موجود من أوامر وتعليمات لترتقي إلى الحدّ الذي يُمَكّنُ الجهة ذات العلاقة من استخدامها وقايةً وردعاً.

.2اتّضح من خلال إجراءات البحث الميداني، ومن نتائج الدراسة عدم وجود جهة أمنية متخصّصة للتعامل مع جرائم وسلبيات الإنترنت. ولذا توصى هذه الدراسة بإيجاد جهة متخصصة للتعامل مع جرائم الإنترنت وقايةً، وتحقيقاً، وضبطاً، وردعاً، بحيث تتلقي الشكاوى الخاصة بجرائم الإنترنت أو الممارسات غير الأخلاقية أثناء تصفّح الإنترنت، وتتمكن في الوقت نفسه من ملاحقة مرتكبيها والتحقيق معهم وتقديمهم للقضاء للبَتِّ في مجازاتهم شرعاً، مع قيام تلك الجهات بدورها الوقائي بتوعية المواطنين والمقيمين بمخاطر مثل هذه الأفعال وكيفية الوقاية منها، وكذلك لإعلام وتعريف الجمهور بوجود مثل هذه الجهة المتخصّصة للتعامل مع جرائم الإنترنت، حيث يجهل الكثير من مستخدمي الإنترنت الجهة التي يمكن أنْ يتقدموا لها بشكواهم في مخالفات وجرائم الإنترنت، ويمكن أنْ تكون هذه الجهة فرعاً من الأمن العام، وتسمي مثلاً شرطة الإنترنت، أو أي مسمى آخر يوضّح مهمتها ويُعْرَفُ منه أنّها أنشئت خصيصاً مِنْ أجل التعامل مع جرائم ومخالفات

الإنترنت.

3.العمل على تدريب العاملين بالجهة التي سيتّم إنشاؤها للتعامل مع جرائم ومخالفات الإنترنت، بما يكفل لهم القدرة الفنّية والتحقيقيّة لممارسة أعمالهم بكفاءة وفاعليّة، ويقترح أنْ يستعان بضباط الشرطة العاملين في التحقيق الجنائي الملمّين بالحاسب الآلي لتشكيل نواة هذه الجهة الجديدة،على أنْ يَتِمّ الاهتمام بالجانب التدريبي المستمّر لرفع كفاءات ومهارات العاملين بهذه الجهة، كالابتعاث في دورات إلى الدول المتقدمة والتي سبقتنا في هذا المجال، وذلك لاكتساب الخبرة الكافية لبدء العمل بأسرع وقت ممكن.

4.نظراً لأنّه ثبت بأنّ الإعلان عن العقوبة عامل رادع للآخرين، فإنّ الباحث يوصي بدراسة نشر بعض العقوبات التي تُتَّخذ بحَقّ بعض المخالفين، على أنْ يسبق ذلك دراسة الأمر من جميع جوانبه لتلافي أيّ سلبية قد تنتج عن الإعلان عن العقوبة أو الأشخاص.

5.توصلت الدراسة الميدانية إلى أنّ نسبة19.2) ٪ (من مستخدمي الإنترنت في المجتمع السعودي طلبوا موادّ إباحية من المواقع الجنسيّة، ومن البديهي أنّ أغلب هذه المواد - إن لم يكن كلّها - تصل لطالبيها بواسطة البريد العادي، وبأشكالها المختلفة كمطبوعات، أو أفلام فيديو ،أو مواد متنّوعة، ولذا توصى الدراسة بتشديد الرقابة على المطبوعات والطرود البريدية، والمواد التي تصل من خارج البلاد خشية تسلل المواد المحظورة.

6.أثبتت نتائج الدراسة أنّ (٤١,٢٪) من مستخدمي شبكة الإنترنت في المجتمع السعودي يستخدمون البروكسي للدخول إلى المواقع المحجوبة، لذا فإنّ هذه الدراسة توصي بإعادة النظر في آلية حجب المواقع غير المرغوبة فيها من قبل مدينة الملك عبدالعزيز للعلوم والتقنية، بما يكفل معه الحجب الفعلي للمواقع الممنوعة فقط، وبما يمنع ارتياد تلك المواقع .

7.ثبت من نتائج الدراسة أنّ احتمال ميل فئة الأطفال، والمراهقين، والشباب قوي لارتكاب حوالي نصف الجرائم والممارسات التي شملتها الدراسة، لذا فإنّ الدراسة توصي بتكثيف الاهتمام التربوي بالنشء، من قبل مؤسسات المجتمع المختلفة، وبخاصة المؤسسات التعليمية، وذلك لتوعيتهم بالمخاطر الأمنية لشبكة الإنترنت، ولتوضيح العقوبات التي ستوضع لمعاقبة مرتكبي تلك الجرائم والممارسات أثناء استخدام شبكة الإنترنت.

8.أثبتت الدراسة الميدانية انعدام احتمال ميل الإناث، وكذلك انعدام احتمال ميل ربات المنازل من مستخدمي شبكة الإنترنت في المجتمع السعودي لارتكاب الجرائم والممارسات التي شملتها الدراسة، بالرغم من أنّ مجموع المشاركين في الدراسة من النساء (٢١٨٣ (مستخدمة، أو ما نسبته (٢٢,٤٪) من مجموع من شارك في الدراسة، وعليه فإنّ الدراسة توصي بالاستمرار في النهج التعليمي المحافظ في مدارس البنات، مع تطويره بما يتوافق وتعاليم ديننا الحنيف والتطوّر التقني الحديث، لأنّ المنهج الذي ينجح في تنمية الرادع الذاتي، وفي غرس الفضيلة الواقية من الانحراف، جدير بالمحافظة عليه.

9. أثبتت نتائج الدراسة أنّ نسبة ميل الأجانب لارتكاب جرائم الإنترنت، يفوق نسبة السعوديين، لذا فإنّ الدراسة توصي بتطبيق نظام السعودة في كلّ المجالات الوظيفية، والعمل على الاستغناء التدريجي والسريع للعمالة الأجنبية، وبخاصة الجنسيات التي أثبتت الدراسة الميدانية احتمال ميلهم القوي لارتكاب الجرائم والممارسات التي شملتها الدراسة.

10. توصلّت الدراسة إلى أنّ عدداً غير قليل من العسكريين قاموا بارتكاب جرائم وممارسات غير أخلاقية أثناء استخدامهم لشبكة الإنترنت، لذا فإنّ الدراسة توصي الجامعات والكليات المدنية والعسكرية بتكثيف البرامج التعليمية والتربوية المتنوعة والكفيلة بزيادة الوزاع الديني، وتنمية الحس الوطني والوعي الأمني، بمخاطر الجرائم والممارسات التي ترتكب من قبل مستخدمي شبكة الإنترنت في المجتمع السعودي، وعدم التساهل في ممارستها لأنّها جرائم يُعَاقَبُ على ارتكابها بعقوبات صارمة، وبخاصة على منسوبي الجهات الأمنية والعسكرية.

11. أوضحت الدراسة الميدانية الاحتمال القوي لميل فئة الشباب، والمراهقين، وفئة المطلقين، والأرامل، لارتكاب معظم الجرائم والممارسات التي شملتها الدراسة والتي يرتكبها مستخدمو شبكة الإنترنت في المجتمع السعودي. لذا فإنّ الدراسة توصي المؤسسات الدينية، والثقافية، والاجتماعية، والرياضية بتكثيف برامجها الهادفة والبنّاءة لجذب مختلف فئات المجتمع وشغل أوقاتهم بما يفيد، وبخاصة من قد يَشْعُر بفراغ عاطفي أو اجتماعي، ولعلنا نتمثل قول الشاعر أبو العتاهية:

إنّ الشبابَ والفراغَ والجدةَ مفسدةٌ للمرءِ أيّ مفسدة

12. ثبت من الدراسة الميدانية أنّ الاحتمال قويُ في ميل العمالة غير المسلمة لارتكاب الجرائم والممارسات التي ترتكب من خلال شبكة الإنترنت، لذا فإنّ الدراسة توصي بتكثيف البرامج الدعوية للجاليات غير المسلمة في مجتمعنا، لدعوتهم إلى الإسلام أولاً، ولتوعيتهم بعقوبة الجرائم والممارسات التي ترتكب من خلال شبكة الإنترنت ثانياً.

13. أثبتت الدراسة الميدانية أنّ هناك إقبالاً كبيراً للاشتراك في المواقع الدينية، فقد وصل مجموع المشتركين في المواقع الدينية (٣٧٢٨) مستخدماً، وهو ما يمثّل نسبة (٣٨٪) من مجموع المشاركين في الدراسة. لذا فإنّ الدراسة توصي بالاهتمام بالمجال الدعوي على شبكة الإنترنت، سواء للمسلمين بإيجاد مواقع هادفة وبديلة عن المواقع الهابطة المنتشرة في شبكة الإنترنت، أو لغير المسلمين لدعوتهم للإسلام الذي هو أتمّ الأديان السماوية وخاتمها .

كلية الدراسات العليا

قسم : العلوم الشرطية

تخصص : القيادة الأمــينة

ملخص رسالة ماجستير

عنوان الرسالة : جرائم الإنترنت في المجتمع السعودي

إعداد الطالب: محمد بن عبدالله بن علي المنشاوي
إشـــراف: عقيد دكتور/ محمد بن إبراهيم السيف
لجنة مناقشة الرسالة:
١. عقيد دكتور: محمد بن إبراهيم السيف مشرفاً ومقرراً.
٢. أ. دكتور: عبدالرحمن إبراهيم الشاعر مناقشاً.
٣. د. علي عبدالكريم المسلّم مناقشاً.
تاريخ المناقشة: ١٤٢٤/٢/٢٧هـ الموافق ٢٠٠٣/٤/٢٩م.
مشكلة البحث: تنحصر مشكلة البحث في تحديد حجم ونمط أكثر جرائم الإنترنت شيوعاً بين مستخدمي الإنترنت في المجتمع السعودي، وخاصة فيما يتعلق بالجرائم الجنسيّة، وجرائم الاختراقات، والجرائم المالية، وجرائم إنشاء أو ارتياد المواقع المعادية، وجرائم القرصنة. مع تحديد أهم سمات وخصائص مرتكبي تلك الجرائم.
أهمية البحث: يمكن الاستفادة من هذه الدراسة في مواجهة جرائم الإنترنت والتعامل معها ومكافحتها، كما يمكن أن تساهم هذه الدراسة بطرح افتراضات تصورية، وتلفت انتباه الباحثين في العلوم الشرطية والعلوم الاجتماعية والعلوم الإنسانية، بشكل عام إلى كثير من الظواهر السلوكية المتعلقة باستخدام الإنترنت، والتي تتطلب البحث والدراسة، وإلى لفت انتباه الجهاز القضائي والقانوني إلى سلوكيات وأفعال جنائية ترتكب ضد الآخرين بواسطة الحاسب الآلي ومن خلال شبكة الإنترنت، من أجل وضع ضوابط قانونية وقضائية في التعامل والحكم على مرتكبيها. كما يأمل الباحث أيضاً إلى لفت انتباه المعنيين والمسؤولين عن الأجهزة والتنظيمات التربوية، والإعلامية، وخطباء المساجد، والمؤسسات العلمية، للمساهمة في مكافحتها والحد منها، ولتحذير أولياء الأمور وكافة شرائح المجتمع من التعامل معها، ولبيان عظيم خطرها بشكل عام.
أهداف البحث: هدفت هذه الدراسة إلى الكشف عن حجم ونمط أكثر الجرائم الجنسيّة والممارسات غير الأخلاقية، وجرائم الاختراقات، والجرائم المالية، وجرائم المواقع المعادية، و جرائم القرصنة الأكثر شيوعاً، والتي يرتكبها مستخدمو الإنترنت في المجتمع السعودي، وتحديد أهم سمات وخصائص مرتكبيها.
تساؤلات البحث: ما حجم الجرائم الجنسيّة والممارسات غير الأخلاقية، و جرائم الاختراقات، والجرائم المالية، وجرائم إنشاء، أو الاشتراك، في المواقع المعارضة، أو المعادية، وجرائم القرصنة التي يرتكبها أفراد المجتمع السعودي عبر الإنترنت؟ وما أهم سمات وخصائص مرتكبيها؟
منهج البحث وأدواته: المنهج الذي تمّ استخدامه في هذه الدراسة، هو المسح الاجتماعي لجميع مستخدمي الإنترنت في المملكة العربية السعودية، واستخدمت أداة الاستبانة لجمع المعلومات الميدانية لهذه الدراسة، والتي تمّ تطويرها خصيصاً لأغراض هذه الدراسة، بعد الأخذ بالشروط العلمية اللازمة لتصميم الاستبانة، وبعد الرجوع إلى الكتب المنهجية المتخصصة في ذلك. وشملت الاستبانة سبعة محاور أساسية وزّعت على (٦٢) سؤالاً والاستبانة هي أداة جمع معلومات الدراسة. وتمّ اختيار المجتمع الكلي للدراسة - وهم جميع مستخدمي الإنترنت في المجتمع

السعودي- والبالغ عددهم تقريباً (١٥٠) مائة وخمسين ألف مستخدم حسب إحصائية مدينة الملك عبدالعزيز للعلوم والتقنية والتي صدرت وقت اختيار الباحث لمجتمع البحث، ووزعت الاستبانة بطريقة تضمن الوصول إلى جميع مستخدمي الإنترنت في المجتمع السعودي، ووصل عدد الاستبانات المجاب عليها (١٠,١٣٨) استمارة، تمّ استبعاد (٢٤٧) استبانة منها للنقص في بعض إجاباتها، حيث وُضع معيار لاستبعاد أيّ استبانة لم يتم الإجابة على (٤٠) سؤال - على أقلّ تقدير- من الأسئلة الكلية للاستبانة والبالغ عددها (٦٢) سؤالاً، ليصبح العدد الكلي للاستبانات الداخلة في تحليل الدراسة الميدانية (٩٨٩١) استبانة، أي ما نسبته (٦,٥٩٪) من المجموع الكلي لمجتمع البحث وهي نسبة مقبولة منهجياً.

أهم النتائج:

١. أنّ حجم الجرائم الجنسيّة والممارسات غير الأخلاقية التي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: ارتياد المواقع الجنسيّة ويرتكبها (٥٣٤١) مستخدم، أو ما نسبته (٥٤,٣٪) من مجموع المشاركين في الدراسة الميدانية، (١٦٧٥) مستخدم أو ما نسبته (١٩,٢٪) طلبوا مواد إباحية منها، (١٧٩١) مستخدم أو ما نسبته (١٨,٣٪) اشتركوا في القوائم البريدية الجنسيّة، (٢٣٥) مستخدم أو ما نسبته (٢,٤٪) أنشئوا موقعاً جنسياً، (٤١٠) مستخدم أو ما نسبته (٤,٢٪) قاموا بإنشاء قوائم بريدية جنسيّة، (٢٨٣) مستخدم أو ما نسبته (٢,٩٪) قاموا بالتشهير بالآخرين ، (٢٧٨) مستخدم أو ما نسبته (٢,٨٪) شُهّرَ بهم، (٤٢٨) مستخدم أو ما نسبته (٤,٤٪) شُهّرَ بأقارب لهم، (٤٠٥٥) مستخدم أو ما نسبته (٤١,٢٪) استخدموا البروكسي لتجاوز المواقع المحجوبة، (١٦٦٠) مستخدم أو ما نسبته (١٦,٩) استخدموا برامج إخفاء الشخصية أثناء تصفح الإنترنت، (١١٥٦) مستخدم أو ما نسبته (١١,٨٪) استخدموا برامج إخفاء الشخصية لإرسال البريد الالكتروني، (١١٥٣) مستخدم أو ما نسبته (١١,٧٪) انتحلوا شخصية الآخرين أثناء التصفح أو استخدام البريد.

٢. أنّ حجم أكثر جرائم الاختراقات شيوعاً التي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: (١٣٤٨) مستخدم أو ما نسبته (١٣,٧٪) من مجموع المشاركين في الدراسة الميدانية قاموا بتدمير المواقع، (٣٨١) مستخدم أو ما نسبته (٣,٩٪) دُمّرَتْ مواقعهم، (٥٤٨) مستخدم أو ما نسبته (٥,٦٪) اخترقوا مواقع حكومية، (٥٢٩) مستخدم أو ما نسبته (٥,٣٪) اخترقوا مواقع تجارية، (٨٦٩) مستخدم أو ما نسبته (٨,٩٪) اخترقوا مواقع شخصية، (٣٧٦) مستخدم أو ما نسبته (١٣,٢٪) اخترقوا مواقع محلية، (١٤٠) مستخدم أو ما نسبته (٥,٠٪) اخترقوا مواقع خليجية، (٨٣) مستخدم أو ما نسبته (٢,٩٪) اخترقوا مواقع عربية غير خليجية، (٨٨) مستخدم أو ما نسبته (٣,١٪) اخترقوا مواقع آسيوية غير عربية، (٩) مستخدم أو ما نسبته (٠,٣٪) اخترقوا مواقع أفريقية غير عربية، (٥١) مستخدم أو ما نسبته (١,٨٪) اخترقوا مواقع أوروبية، (١٤) مستخدم أو ما نسبته (٠,٥٪) اخترقوا مواقع أمريكية جنوبية، (٢٢١) مستخدم أو ما نسبته (٧,٨٪) اخترقوا مواقع في الولايات المتحدة الأمريكية وكندا، (١٨٦٠) مستخدم أو ما نسبته

(٦٥,٤٪) لا يذكرون المواقع التي اخترقوها، (٤٥٦) مستخدم أو ما نسبته (٤,٧٪) تعرّضت مواقعهم للاختراق، (١٦٨٨) مستخدم أو ما نسبته (١٧,٣٪) اخترقوا أجهزة شخصية، (٣٢٧٨) مستخدم أو ما نسبته (٣٣,٣٪) تعرضت أجهزتهم الشخصية للاختراق، (١٤٧٩) مستخدم أو ما نسبته (١٥,١٪) قاموا باختراق البريد الإلكتروني، (١٥٣١) مستخدم أو ما نسبته (١٥,٦٪) تعرّض بريدهم الإلكتروني للاختراق، (١٥٧٠) مستخدم أو ما نسبته (١٦,٠٪) قاموا بالاستيلاء على البريد الإلكتروني، (١٠٨٤) مستخدم أو ما نسبته (١١,٠٪) تم الاستيلاء على بريدهم الإلكتروني، (١٠١٧) مستخدم أو ما نسبته (١٠,٣٪) قاموا بإغراق البريد الإلكتروني، (١٨٣٢) مستخدم أو ما نسبته (١٨,٦٪) تعرّض بريدهم الإلكتروني للإغراق، (١٦٩٧) مستخدم أو ما نسبته (١٧,٣٪) استولوا على اشتراك الآخرين، (١٥٣١) مستخدم أو ما نسبته (١٥,٦٪) تم الاستيلاء على اشتراكهم، (١٢١١) مستخدم أو ما نسبته (١٢,٣٪) قاموا بإرسال فيروسات أو تروجنات، (٥١٣٨) مستخدم أو ما نسبته (٥٢,٢٪) تضرروا من الفيروسات.

٣. أنّ حجم الجرائم والممارسات المالية التي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: (٤٣٥) مستخدم أو ما نسبته (٤,٤٪) قاموا بالاستيلاء على البطاقات الائتمانية، (١٢٦) مستخدم أو ما نسبته (١,٣٪) تم الاستيلاء على بطائقهم الائتمانية، (٥٠٠) مستخدم أو ما نسبته (٥,١٪) لعبوا القمار، (٤٤٤) مستخدم أو ما نسبته (٤,٥٪) قاموا بالتزوير عبر الإنترنت، (٤١٤) مستخدم أو ما نسبته (٤,٢٪) ارتادوا مواقع الجريمة المنظمة، (٢٩٠) مستخدم أو ما نسبته (٣,٠٪) ارتادوا مواقع المخدرات، (١٧٧) مستخدم أو ما نسبته (١,٨٪) ارتادوا مواقع غسيل الأموال، (٧٩١) مستخدم أو ما نسبته (٤٢,٢٪) من مرتادي مواقع الجريمة المنظمة أو المخدرات أو غسيل الأموال كان هدفهم الاستفادة العلمية من هذه المواقع، (٨٣٩) مستخدم أو ما نسبته (٤٤,٧٪) كان هدفهم الفضول أو من باب المصادفة، (١٠٦) مستخدم أو ما نسبته (٥,٧٪) كان هدفهم تنفيذ الأفكار الإجرامية التي تنشرها تلك المواقع، (١٣٩) مستخدم أو ما نسبته (٧,٤٪) كان هدفهم الانضمام إلى تلك المنظمات الإجرامية.

٤. أنّ حجم جرائم وممارسات إنشاء المواقع المعادية أو الاشتراك فيها والتي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: (٢٦١) مستخدم أو ما نسبته (٢,٦٪) قاموا بإنشاء مواقع سياسية معادية، (١٣٣٦) مستخدم أو ما نسبته (١٣,٦٪) اشتركوا طوعاً في المواقع السياسية المعادية، (٧٣٦) مستخدم أو ما نسبته (٧,٥٪) تعرضوا للاشتراك القهري في المواقع السياسية المعادية، (٥٦١) مستخدم أو ما نسبته (٥,٧٥٪) قاموا بإنشاء مواقع دينية، منهم (٥٠٠) مستخدم أو ما نسبته (٥,١١٪) أنشئوا مواقع سنية، (٤٣) مستخدم أو ما نسبته (٠,٤٣٪) أنشئوا مواقع شيعية ، (٥) مستخدم أو ما نسبته أنشئوا (٠,٠٥٪) مواقع نصرانية، (٣) مستخدم أو ما نسبته (٠,٠٣٪) أنشئوا مواقع يهودية، (٢) مستخدم أو ما نسبته (٠,٠٢٪) أنشئوا مواقع بوذية، (٣) مستخدم أو ما نسبته (٠,٠٣٪) أنشئوا مواقع هندوسية، (٥) مستخدم أو ما نسبته (٠,٠٥٪) أنشئوا مواقع لا دينية.

(٣٧٢٨) مستخدم أو ما نسبته (٣٨,٠٦٪) اشتركوا في القوائم الدينية، منهم (٣٤٥٥) مستخدم أو ما نسبته (٣٥,٣٠٪) اشتركوا في المواقع السنية، (١٩٠) مستخدم أو ما نسبته (١,٩٣٪) اشتركوا في المواقع الشيعية، (٢٩) مستخدم أو ما نسبته (٠,٢٩٪) اشتركوا في المواقع النصرانية، (١٠) مستخدم أو ما نسبته (٠,١٠٪) اشتركوا في المواقع اليهودية، (٦) مستخدم أو ما نسبته (٠,٠٦٪) اشتركوا في المواقع البوذية، (١٢) مستخدم أو ما نسبته (٠,١٢٪) اشتركوا في المواقع الهندوسية، (٢٦) مستخدم أو ما نسبته (٠,٢٦٪) اشتركوا في المواقع اللا دينية.

(٢٩٢) مستخدم أو ما نسبته (٣,٠٪) قاموا بإنشاء مواقع معادية للأشخاص أو الجهات.

٥. أنّ حجم أكثر جرائم القرصنة شيوعاً والتي يرتكبها مستخدمي الإنترنت في المجتمع السعودي هي: (٣٩٥) مستخدم أو ما نسبته (٤,٠٪) قاموا بإنشاء مواقع للبرامج المقرصنة، (٣٠٩١) مستخدم أو ما نسبته (٣١,٥٪) قاموا بتحميل برامج مقرصنة، (٣١٨٢) مستخدم أو ما نسبته (٣٢,٤٪) استخدموا برامج تشغيل البرامج المقرصنة، (٥٧٧) مستخدم أو ما نسبته (٥,٩٪) قاموا بإنشاء مواقع مقرصنة.

كما تم التوصل إلى سمات وخصائص مرتكبي تلك الجرائم والممارسات غير الأخلاقية وبشكل مفصل.

وأخيرا أتضح أنّ أكثر جرائم وممارسات الإنترنت شيوعاً في المجتمع السعودي هي جرائم الاختراقات، يليها الجرائم المالية وجرائم المواقع المعادية كجرائم وممارسات متوسطة الشيوع، أمّا الجرائم والممارسات الأقلّ شيوعاً فأتضح أنّها الجرائم الجنسيّة وممارسة الأفعال غير الأخلاقية.

Institute of Graduate Studies
Department : Police Science
Specialization : Security Command
Master Thesis Abstract

Thesis Title: Internet Crimes in the Saudi Soci
Prepared By: Mohammad A. A. Alminshawi
Supervisor: Colonel Dr. Mohammad I Alsaif.
Thesis Defence Committee:

1. Colonel Dr. Muhammad I Alsaif (supervisor and reporter)
2. Professor Ibrahim Alsha'ir (discussant)
3. Dr. Ali A. Almusallam (discussant)

Defence Date: 27/2/1424 H – 29/4/2003 AD *Research Problem:* Specifying and determining the most recurrent internet crimes in the Saudi society, specially those that pertain to sex, hacking, finance, creating or surfing opponent websites, and piracy. And also characterizing those who commit those crimes.

Research Importance: The study can be utilized to face, deal with, and control internet crimes. It might also help researchers in human, social, and police sciences in creating useful concepts on explaining behavioral phenomena that pertain to internet usage, which needs be thoroughly studied and researched, and also to draw the attention of the judicial and legal systems to such criminal acts committed by PC and internet users in order to set judicial and legal standards for treating and judging such cases. The researcher also hopes to draw the attention of education and press officials, masjid public speakers, technological organizations, and parents as to control and limit those crimes. The dangers of such acts and crimes are also made subject to clarification and manifestation in this study.

Research Objectives: The purpose of this study is to uncover the most recurrent internet crimes of any nature such as sexual abuse, immorality, hacking, financial crimes, opponent websites, and piracy. The subject of this study is the internet users in the Saudi society. It also tries to characterize those who commit such crimes.

Research Questions: How recurrent are sexual, immoral, hacking, financial, opponent websites' surfing and managing, and piracy crimes that are committed by internet users in the

Saudi society? And what are their main characteristics?
Research Methodology & Tools: the method used in this study is social surveys. The whole community targeted in the study is all of the internet users in the Saudi society who reach about 150.000 users according to KACST's (King AbdulAziz City for Science and Technology) census issued at the time of determining the study community.
The questionnaire was distributed in a manner that assures that all of the study community members get the chance to answer it. A total of 10.138 questionnaires were answered, 274 questionnaires were discarded for being incompletely answered. Any questionnaire that contains at least 40 unanswered questions out of the total 62 questions is always ignored. Thus the total number of questionnaires used in the study is 9.891, a ratio of 6.59% of the total study community, which is methodically accepted.
The questionnaire is utilized to get the necessary data from the study field. It was designed specially for this study after having it methodically standardized. The questionnaire contains 62 questions allotted to seven main axes.
. *Important findings:*
1. The recurrences of sexual and immoral practices done by internet users in the Saudi society is as follows:
- visiting websites of sexual contents: 5341 users (54.3% of the total users).
- 1675 users (19.2%) searched for pornographic contents in these websites.
- 1791 users (18.3%) subscribed to mailing lists of sexual nature.
- 235 users (2.4%) constructed website(s) of sexual contents.
- 410 users (4.2%) established mailing lists of sexual contents.
- 283 users (2.9%) defamed others.
- 278 users (2.8%) were subjected to defamation.
- 428 users (4.4%) had their relatives subjected to defamation.
- 4055 users (41.2%) used a proxy to visit blocked websites.
- 1660 users (16.9%) used special software to surf anonymously.

- 1156 users (11.8%) used special software to send email messages anonymously.
- 1153 users (11.7%) disguised in other users' identities in surfing or using email.

2. The recurrences of hacking crimes committed by internet users in the Saudi society is as follows:

- 1348 users (13.7%) destroyed websites.
- 381 users (3.9%) had their websites destroyed.
- 548 users (5.6%) hacked websites of governmental nature.
- 529 users (5.3%) hacked commercial websites.
- 869 users (8.9%) hacked personal websites.
- 376 users (13.2%) hacked local websites.
- 140 users (5.0%) hacked GCC (Gulf states) websites.
- 83 users (2.9%) hacked other Arab (non-GCC) websites.
- 88 users (3.1%) hacked Asian (non-Arab) websites.
- 9 users (0.3%) hacked African (non-Arab) websites.
- 51 users (1.8%) hacked European websites.
- 14 users (0.5%) hacked South American websites.
- 221 users (7.8%) hacked USA and Canadian websites.
- 1860 users (65.4%) do not recall the websites they hacked.
- 456 users (4.7%) had their websites hacked.
- 1688 users (17.3%) hacked PCs.
- 3278 users (33.3%) had their PCs hacked.
- 1479 users (15.1%) hacked email accounts.
- 1531 users (15.6%) had their email account(s) hacked.
- 1570 users (16.0%) occupied email accounts.
- 1084 users (11.0%) had their email account(s) occupied.
- 1017 users (10.3%) flooded (bombed) email accounts.
- 1832 users (18.6%) had their email account(s) flooded (bombed).
- 1697 users (17.3%) stole others' ISP accounts.
- 1531 users (15.6%) had their ISP accounts stolen.
- 1211 users (12.3%) sent viruses and trojans.
- 5138 users (52.2%) had their PCs infected by viruses.

3. The recurrences of financial crimes committed by internet users in the Saudi society is as follows:

- 435 users (4.4%) stole Credit Cards accounts.
- 126 users (1.3%) had their Credit Cards accounts stolen.
- 500 users (5.1%) gambled.

- 444 users (4.5%) committed forgery through the internet.
- 414 users (4.2%) visited websites of organized crimes.
- 290 users (3.0%) visited drugs' websites.
- 177 users (1.8%) visited money laundering websites.
- 791 users of those who visited websites of organized crime, drugs, and money laundering (42.2%) surfed them for scientific reasons.
- 839 users of those who visited websites of organized crime, drugs, and money laundering (44.7%) surfed them out of curiosity or by chance.
- 106 users of those who visited websites of organized crime, drugs, and money laundering (5.7%) surfed them to use their contents in committing crimes.
- 139 users of those who visited websites of organized crime, drugs, and money laundering (7.4%) surfed them to become members in those criminal organizations.

4. The recurrences of establishing or cooperating with opponent websites by internet users in the Saudi society is as follows:

- 261 users (2.6%) established politically opponent websites.
- 1336 users (13.6%) subscribed voluntarily in politically opponent websites.
- 736 users (7.5%) were subject to compulsory subscription in politically opponent websites.
- 561 users (5.75%) established religious websites, out of whom 500 users (5.11%) established Sunni websites, 43 users (0.43%) established Shiite websites, 5 users (0.05%) established Christian websites, 3 users (0.03%) established Jewish websites, 2 users (0.02%) established Buddhist websites, 3 users (0.03%) established Hindu websites, and 5 users (0.05%) established Atheistic websites.
- 3728 users (38.06%) subscribed in religious mailing lists, out of whom 3455 users (35.30%) subscribed in Sunni lists, 190 users (1.93%) subscribed in Shiite lists, 29 users (0.29%) subscribed in Christian lists, 10 users (0.10%) subscribed in Jewish lists, 6 users (0.06%) subscribed in Buddhist lists,12 users (0.12%) subscribed in Hindu lists, and 26 users (0.26%) subscribed in Atheistic lists.
- 292 users (3.0%) established hostile websites against

organizations or persons.

5. The recurrences of piracy crimes by internet users in the Saudi society is as follows:

- 395 users (4.0%) established pirated software websites.
- 3091 users (31.5%) downloaded pirated software.
- 3182 users (32.4%) used downloading software to download pirated software.
- 577 users (5.9%) established pirated websites.

The personal characteristics of those who committed such crimes and immoral practices were also uncovered and manifested in details.

It is clear from the study that the most frequent of internet crimes in the Saudi society are (in order) hacking, then financial crimes, and lastly, the least frequent are crimes and practices of sexual and immoral nature.

دور الأسرة في أمن المجتمع

ورقة عمل مقدمة لندوة المجتمع والأمن المنعقدة بكلية الملك فهد الأمنية بالرياض من ٢/٢١ حتى ٢/٢٤ من عام ١٤٢٥هـ :
د . إدريس بن حامد محمد
جامعة الملك سعود – الرياض
الجلسة الثانية/ الاثنين ١٤٢٥/٢/٢٢هـ الساعة ٦,٣٠ مساء
الدور الأمني للأسرة
رئيـــس الجلســـــة
معالي الدكتور/ أحمد بن علي المباركي
عضو هيئة كبار العلماء وعضو اللجنة الدائمة للبحوث العلمية والإفتاء
الورقة الرابعة

مقدمة البحث :

الأسرة هي النواة الأولى للمجتمع، وتمثل الأساس الاجتماعي في تشكيل وبناء شخصيات أفراد المجتمع حيث تضفي على أبنائها خصائصها ووظيفتها. والمجتمع بوجه عام يتكون من أسر ولم يوجد مجتمع عبر التاريخ أقام بناءه على غير الأسر وبذلك تعدّ الأسرة عنوان قوة تماسك المجتمع أو ضعفه لأنها مأخوذة من الأسر وهو القوة والشدة ، فهي تمثل الدرع الحصين لأفرادها ، باعتبار أن كلا من الزوجين يعتبر درعا للآخر .

إن المهام المنوطة بالأسرة منذ نشأتها عديدة منها ما هو تربوي أو اجتماعي أو اقتصادي أو سياسي وقد أكدت مجريات الأحداث التي تشهده المجتمعات البشرية دور الأسرة الكبير في عملية استتباب الأمن وبسط الطمأنينة التي تنعكس آثارها على الأفراد والمجتمعات سلباً أو إيجابا . وهذا ما يؤكد الحقيقة التي تقول إنّ قوة الأسرة هي قوة للمجتمع وضعفها ضعف له .

إن الأمن والأسرة يكمل أحدهم الآخر ويوجد بينهما الترابط الوثيق ، وذلك أنه لا حياة للأسرة إلا باستتباب الأمن ، ولا يمكن للأمن أن يتحقق إلا في بيئة أسرية مترابطة ، وجو اجتماعي نظيف ، يسوده التعاطف والتآلف ، والعمل على حب الخير بين أفراده ، كل ذلك ضمن عقيدة إيمانية راسخة ، واتباع منهج نبوي سديد ، هذا الإيمان هو الكفيل بتحقيق الأمن الشامل والدائم ، الذي يحمي المجتمع من المخاوف ، ويبعده عن الانحراف ، وارتكاب الجرائم .

إن هذا الدور لا يتحقق إلا في ظل أسرة واعية تحقق في أبنائها الأمن النفسي ، والجسدي ، والغذائي ، والعقدي ، والاقتصادي ، والصحي بما يشبع حاجاتهم النفسية والتي ستنعكس بالرغبة الأكيدة في بث الطمأنينة في كيان المجتمع كله وهذا ما سيعود على الجميع بالخير الوفير.

وقد تناولت الدراسة موضوع البحث في النقاط الآتية :

• المقدمة في بيان أهمية الموضوع ، ومشكلة البحث ، وأهدافه ، وحدوده .

- بيان مفهوم الأسرة .
- بيان مفهوم الأمن .
- أهمية الأسرة .
- بناء الأسرة وتكوينها .
- الدور المنشود منها لتحقيق الأمن .
- أهداف تكوين الأسرة .
- أهمية الأمن ، والحاجة إليه ، وأقسامه .
- مكانة الأمن في الكتاب والسنة .
- وسائل الأسرة في تحقيق الأمن .
- تحقيق الأمن النفسي والجسدي .
- تحقيق الأمن الغذائي .
- تحقيق الأمن العقدي .
- تحقيق الأمن الاقتصادي .
- تحقيق الأمن الصحي .
- الأسرة وأمن المجتمع .
- الخاتمة وفيها نتائج البحث .
- التوصيات .
- مصادر البحث .

مشكلة البحث

تقصير الأسرة عن دورها الأساسي، أو تخليها عنه، إما جهلاً أو استخدامها وسائل وأساليب خاطئة في التربية كاستخدام أساليب التخويف والإذلال والتسلط، أو فرض الطاعة العمياء، أو استخدام أساليب التدليل والإفراط في التساهل والاتكالية، مما نتج عنه جنوح الأولاد وانحلالهم وتشردهم وضياعهم، مما أدى إلى تمرد الأبناء على الآباء والأسر والمتجمعات

ويجيب عن التساؤل الآتي :

ماهي العواقب السيئة التي تترتب عن تخلي الأسرة عن دورها التربوي ؟.

أهداف البحث

١- بيان الوظائف الحقيقية للأسرة .

٢- تكوين الوعي بخطورة وإهمال الأسرة لدورها التربوي المحقق للكفاية والأمن .

٣- تحقيق الأمن في حياة الناس من أهداف الإسلام الكبرى التي تقوم الأسرة بنشره .

أهمية البحث

١- بيان أهمية الأمن ودور الأسرة في بسطه بين أفرادها.

٢- الدعوة إلى تنمية وعي الأسرة المسلمة .

حدود البحث

اقتصرت هذه الدراسة على بيان دور الأسرة في الأمن والكفاية، مع بيان أهمية

الأمن وضرورته والحاجة إليه للجميع.
معنى الأسرة لغة واصطلاحا
الأسرة في اللغة :
الأسرة مأخوذة من الأسر في أصلها ، والأسر لغة الدرع الحصين ، والأسرة : الخلقَ ، الأسر أيضا القوة والصبر وفي المعجم الوسيط : الأسر يعني القيد يقال أسره – أسرا – وإساراً: قيده .
والأسرة عشيرة الرجل وأهل بيته ، وأسرة الرجل عشيرته ورهطه الأدنون .
تشير الأسرة إلى القوة والشدة لأن أعضاءها يشدّ بعضهم بعضا كما تطلق على الأهل والعشيرة ، وتطلق على الجماعة الذي يضمهم هدف واحد كأسرة الآباء ، أو المحامين لكن لم يرد إن[لفظ الأسرة في القرآن ، وإنما ورد الأهل والعشيرة قال تعالى على لسان نوح : وأنذر[، وقوله :] وأمر أهلك بالصلاة واصطبر عليها [، وقوله :]ابني من أهلي]عشيرتك الأقربين
معنى الأسرة اصطلاحا :
إن مصطلح الأسرة اكتنفه بعض الغموض لأن مدلوله لم يرد في القرآن بالرغم من أنه معروف لدى جميع الناس، ومع ذلك فقد عرّفه أهل الاختصاص فقالوا : الأسرة هي الجماعة التي ارتبط ركناها بالزواج الشرعي والتزمت بالحقوق والواجبات بين طرفيها ومانتج عنهما من ذرية وما اتصل بهما من أقارب .
كما عرفها محمد عقله بأنها : (الوحدة الأولى للمجتمع ، وأولى مؤسساته التي تكون العلاقة فيها في الغالب مباشرة ، ويتم داخلها تنشئة الفرد اجتماعيا ، ويكتسب منها الكثير من معارفه ومهاراته وعواطفه واتجاهاته في الحياة ، ويجد فيها أمنه وسكينته) .
ومن هنا نعلم أن الأسرة هي الخلية الأولى في بناء المجتمع حيث يتكون كل مجتمع من العديد من الأسر التي تنظم حياته وتسير أموره وتحقق حاجاته وميوله وعاداته وتقاليده .
معنى الأمن لغة واصطلاحا
معنى الأمن لغة :
وردت كلمة الأمن وما يشتق منها في القرآن في مواضع عديدة وبالمعنى الذي نقصده وهو يعني السلامة والاطمئنان النفسي مع انتفاء الخوف على حياة الإنسان .
الأمن لغة : تقيض الخوف قاله ابن سيده، وقال الجوهري : الأمن ضد الخوف .
وهذا الاختلاف بين ابن سيده والجوهري بأنه ضد أو النقيض يدل حسب مراد علماء اللغة على أن الأمن لا يجتمع مع الخوف وأن وجود أحدهما يرفع وجود الآخر فالإنسان إما أن يكون آمنا وإما أن يكون خائفا.
فالأمن مصدر أمن يأمن ، أي اطمأنّ وزال خوفه ، وسكن قلبه ، وأمن إن المتقين في مقام أمين[البلد اطمئن به أهله ، فهو آمن وأمين قال تعالى: .]
أي آمن من أمن الرجل أمانة فهو أمين وهو ضد الخائن ، فوصف به المكان استعارة . قال ابن فارس : (الهمزة والميم والنون أصلا متقاربا :إحداهما : الأمانة التي هي ضد الخيانة ومعناها سكون القلب . والآخر : التصديق . والمعنيان

متقاربان ٠ قال الخليل الأمنة من الأمن ٠والأمان إعطاء الأمنة ٠والأمانة ضد الخيانة ٠٠٠ وبيت آمن ٠ وبهذا يتضح أن معنى الأمن في] رب اجعل هذا البلد آمنا [ذو أمن قال تعالى : اللغة الاطمئنان وسكون القلب وطمأنينة النفس وزوال الخوف، والسلامة،والسكن ،والأمن والأمانة والأمان .
كما أن مادة أمن ومشتقاتها جاءت في القرآن الكريم في أكثر من ثمانمائة مرة فالمؤمنون، والإيمان ،والأمانة، والذين آمنوا ٠ كلها من الأمور المرتبطة حساً ومعنى بالإيمان ونتائجه .
الأمن في الاصطلاح :
إن تعريف الأمن الاصطلاحي لا يخرج كثيراً عن معناه اللغوي حسب فهم السلف لذلك حيث تعددت عباراتهم اللغوية له من حيث مدلوله لثرائه اللغوي ٠
فيرجع مفهومه عندهم إلى عدم الخيانة، والتصديق ، والحفظ٠ الطمأنينة ، الدين ، الثقة، القوة، السلم ،الإجارة وطلب الحماية ومع ذلك حاول الجرجاني تعريفه بقوله: (الأمن: عدم توقع مكروه في الزمان الآتي) ومن تعريفات الأمن (اطمئنان الفرد والأسرة والمجتمع على أن يحيوا حياة طيبة في الدنيا ولا يخافون على أنفسهم وأموالهم وأعراضهم ودينهم وعقولهم ونسلهم من أن يعتدى عليها٠٠٠) .
كما عرف بأنه:(الشعور بالطمأنينة الذي يتحقق بحفظ مصالح الناس الدينية والبدنية والعقلية والاجتماعية والمالية وذلك من خلال الوسائل التربوية والوقائية والزجرية التي شرعها الإسلام لذلك) لكن الملاحظ في هذه التعريفات أنها عبارة عن شروح وتفصيلات للموضوع المعرف، ومن شرط التعريف أن يكون جامعاً مانعاً مختصراً، كأن يعرف (السكينة التي يشعر بها الفرد نتيجة لإشباع دوافعه العضوية والنفسية) ويرى الباحث أن اقرب تعريف للأمن هو (الشعور بالسلامة والاطمئنان للفرد والمجتمع وتحقيق مصالح الخلق ومتطلباتهم بحفظ الضرورات الخمس عبر وسائل الشرع)٠ من هذه التعريفات يتبيّن أن حقيقة الأمن هو طمأنينة النفس وسكينة القلب وزوال الخوف وبالتالي يصبح للأمن مفهوم شمولي متكامل يحيط بكل جوانب الأمن المختلفة وصوره المتعددة بما يحققه الحفاظ على مصالح كل الناس التي يخافون عليها ، ويحرصون على حفظها ورعايتها ،بجلب النفع وتحقيقه ،ودفع الضر وإزالته٠
إن أي وسيلة زجرية أو وقائية قد توصل إلى الأمن ، لكنه يبقى محصوراً في مظهره مما يتطلب أن تكون الوسيلة التربوية مما شرعه الله تعالى لعباده لأنه سبحانه أعلم بما يصلح الخلق ويحقق لهم .] ألا يعلم من خلق وهو الطيف الخبير[الأمن
ولذا كانت أول وسيلة وأعظمها في الذين أمنوا ولم[تحقيقه هي وسيلة الحفاظ على التوحيد ونبذ الشرك كما قال تعالى: .]يلبسوا إيمانهم بظلم أولئك لهم الأمن وهم مهتدون
ومن مصطلحات البحث كلمة (دور) وتعني :عود الشيء إلى ما كان عليه كما تعني النوبة والمرة والحركة .
ويقصد بدور الأسرة في الدراسة بيان الحقوق والواجبات والإرتباطات التي تقوم بها

الأسرة داخل أفرادها لإحداث تغيير في بناء شخصية الفرد المسلم.
أهمية الأسرة
تعتبر الأسرة أهم خلية يتكون منها جسم المجتمع البشري إذا صلحت صلح المجتمع كله ، وإذا فسدة فسد المجتمع كله، في كنفها يتعلم النوع الإنساني أفضل أخلاقه .
إذ فيها ينشأ الفرد وفيها ، تنطبع سلوكياته ،وتبقى أثارها منفوشة فيه ، يحملها معه ، ويورثها ذريته من بعده
وتكمن أهميتها في الأمور الآتية:
١- هي أول لبنة في بناء المجتمع ،لأن الأسرة السوية الصالحة هي أساس الحياة الاجتماعية ، بل هي أساس المجتمع المتكامل، لأنه عبارة عن مجموعة من الأسر المتفاعلة٠
٢- تحقيق وظائف الإنسان الفطرية مثل غريزة البقاء، والتوازن في الدوافع الجنسية وتوثيق العلاقات والعواطف الاجتماعية بين أفراد الأسرة الواحدة .
٣- تكسب الفرد اتجاهاته، وتكّون ميوله، وتميز شخصيته، وتحدد تصرفاته، بتعريفه بدنيه ، وعادات مجتمعه ولغته ، فيكون لها الأثر الذاتي ،والتكوين النفسي في تقويم السلوك وبعث الطمأنينة في نفس الطفل .
٤- تعلم أفرادها كيفية التفاعل الاجتماعي بما تكسبهم من حرف تمكنهم من العيش في أمان مع المجتمع الذي ينتموا إليه ٠
وبهذا نعلم أن الأسرة تستمد أهميتها وعلو شأنها لأنها البيتة الاجتماعية الأولى والوحيدة التي تستقبل الإنسان منذ ولادته ، وتستمر معه مدى حياته، تعاصر انتقاله من مرحلة إلى مرحلة مما يستدعي القول بعدم وجود نظام اجتماعي آخر يحدد مصير النوع الإنساني كله كما تحدده الأسرة .
بناء الأسرة وتكوينها
ورد في كتاب الله ذكر الأهل والعشيرة والعيلة، ولم يرد فيه الأسرة بلفظها وقد استنبط العلماء من مدلولات تلك الآيات الكريمة ثلاث تقسيمات للأسرة هي كالآتي :
١- الأسرة تتكون من الزوج والزوجة قال تعالى: [أنت وزوجك ويا آدم أسكن الجنة].
٢- الأسرة تتكون من الزوج والزوجة والذرية قال تعالى [أرسلنا رسلاً من قبلك وجعلنا لهم أزواجاً وذرية ولقد].
٣- الأسرة تتكون من الزوج [والأولاد والأقارب قال تعالى: يا أيها الذين آمنوا قوا أنفسكم وأهليكم ناراً].
وإن كان المفهوم الأخير أوسع من سابقيه إلا أن المفهوم الأول هو الأصل في تكوين الأسرة ، وما جاء بعده فهو من ثماره وآثاره ولذلك يجدر القول بأن الأسرة في نشأتها تكونت من زوجين فهما بمثابة الأصول الثابتة لها ٠
لكن السؤال المطروح من هما الزوجان ؟ وما هي صفات وخصائص كل ومن آياته[منهما ؟ يقول تعالى في كتابه: أن خلق لكم من أنفسكم أزواجاً لتسكنوا إليها وجعل بينكم مودة ورحمة إن في ذلك لآياتٍ لقوم يتفكرون]
بيّنت الآية إن الزوجة نعمة ورحمة لأنها من جنس الزوج فهي قطعة منه يسكن

إليها وتسكن إليه ،يكمل كل منها نقص الآخر بما يحقق فطرته ، إذ فطرت المرأة على رقة في الشعور،ولين الجانب ،وجمال التقويم، مما يشبع شوق الرجل، ويرضي ذوقه، ويكفي حاجته، ويهيئ له أسباب الراحة (أن المرأة سكن الرجل وراحته والظل الهادئ الجميل الذي يميل ويلجأ إليه بعد يوم مرهق من الجد والكدح، وهذا السكن لا يتحقق لو أن المرأة تركت مهمتها كزوج وأم لتشارك في العمل إلى جوار الرجل) .

إن ميدان المرأة الحقيقي هو التربية وغرس القيم في نفوس الصغار، فالأمومة شرف قصره الله على المرأة، وتتحقق عظمتها الحقيقية في إتقانها هذا الدور، أما تخليها عن هذا الدور، وتسابقها في ميدان لا يناسب طبيعتها بحجة إثبات الذات وتحدي الرجال، سبب لها متاعب جمّة ،وترتب عليه ما نراه من تفكك أسري ، ودمار أخلاقي ، وضياع الذرية، بحدوث تلكم الانحرافات السلوكية الكثيرة ، وعدم تحقق الأمن المنشود لها وللأسرة والزوج والأبناء ، مما انعكس سلبا على المجتمع، بانفتاح ثغرة كبيرة عليه، لا يتم التخلص منها إلا بالعودة الحميدة للمرأة في ميدانها الطبيعي .

إن المرأة التي حققت بعض النجاحات في مجالات العمل وأهملت دورها الأساسي كأم وزوجة لهي امرأة فاشلة لأنها ضيعت أولادها وبيتها ، وتخلت عن رسالتها الحقيقية ٠

ما الدور الذي ننشده للأسرة لتحقيق الأمن

إن الأسرة التي نريدها هي الأسرة المتمسكة بعقيدتها الإسلامية السمحة قولاً وسلوكا ، المعتزة بانتمائها لأمتها الإسلامية، المستوعبة لأصول دينها والمحافظة على الإلتزام به ، المبتعدة عن ضعيفه ،المنفتحة على العالم المعاصر بصدر رحب ، وعقل ناضج ، تفيد من تقدمه بما لا يتعارض مع عقيدتها وما تحمله من قيم نبيلة .

إنها الأسرة المتخلصة من عقدة التخلف بمختلف أشكاله ، الآخذة على نفسها بتدريب أفرادها بالتعبير عن الرأي في حدود احترام الآخرين .

إنها الأسرة التي تشيع في البيت الاستقرار والود والطمأنينة ، والتي تقوم بإبعاد ذويها عن كل ألوان العنف والكراهية والبغض ، ذلك أن معظم مشاكل المنحرفين الذين اعتادوا على الإجرام في الكبر، تعود إلى حرمانهم من الاستقرار العائلي ، إذ لم يجدوا بيتاً هادئاً فيه أب يحدب عليهم ، وأم تدرك معنى الشفقة فلا تفرط في الدلال ولا في القسوة . لأن إشاعة الود والعطف بين الأبناء، له الأثر البالغ في تكوينهم تكوينا سليما.

الناشئة التي نتطلع إليها

هم رجال القرن الحادي والعشرين الذين سيكونون في سباق مع الزمن ، وسيواجهون تحديات جسام بطغيان القيم المادية على القيم المعنوية وبالتقدم التقني الذي بات يقفز قفزات خيالية ٠

بحيث يخرج مؤهلا مشاركا مع الآخرين، لا مستهلكاً فحسب ويكون له دور في صنع القرار المصيري على الأقل قي نطاق أسرته ثم مجتمعه ،بعيدا ممن يسيطر على تفكيره ضيق الأفق ٠

إننا نتطلع إلى ناشئة هم على وعي بواقعهم المتخلف، وقادرين على تجاوزه ، ساعين للمعرفة بأدق ما وصل إليه عصرهم من علوم وآداب ، ومتسلحين بالقيم الروحية والمعنوية التي تحدد معالم شخصياتهم الإسلامية
(وعلينا أن لا نجبرهم على بعض عاداتنا الاجتماعية التي لا علاقة لها بالدين أوبالاخلاق والتي ألفناها بحسب زماننا ، وإنما علينا أن نغرس فيهم حسن التلاؤم مع مجتمعهم المستقبلي، وذلك لأنهم قد خلقوا لزمان غير زماننا) .
أهداف تكوين الأسرة
يهدف الإسلام من تكوين الأسرة إلى تحقيق أهداف كبرى تشمل كل مناحي المجتمع الإسلامي، ولها الأثر العميق في حياة المسلمين وكيان الأمة المسلمة .
ويمكن إجمال هذه الأهداف في ثلاث نقاط رئيسية:
١- الهدف الاجتماعي الذي يتحقق به تماسك المجتمع وترابطه وتوثيق عرى الأخوة بين أفراده وجماعاته وشعوبه وهو الذي خلق من الماء بشراً فجعله نسباً وصهراً وكا[بالمصاهرة والنسب قال تعالى: ن .]ربك قديرا
٢- الهدف الخلقي اعتبر الإسلام بناء الأسرة وسيلة فعّالة لحماية أفرادها شيبا وشباباً ، ذكوراً وإناثا من الفساد، ووقاية المجتمع من الفوضى،إن تحقيق هذا الهدف يكون بالإقبال على بناء الأسرة ، لأن عدم ذلك يحصل به ضرر على النفس باحتمال الانحراف عن طريق الفضيلة والطهر ، كما يؤدي إلى ضرر المجتمع بانتشار الفاحشة وذيوع المنكرات وتفشي الأمراض الخبيثة .
٣- الهدف الروحي، إن بناء الأسرة خير وسيلة لتهذيب النفوس وتنمية الفضائل التي تؤدي إلى قيام الحياة على التعاطف والتراحم والإيثار،حيث يتعود أفرادها على تحمل المسئوليات، والتعاون في أداء الواجبات .
ومن خلال تحقيق هذه الأهداف الكبرى، يمكن أن تحقق هناك أهداف أخرى في ظلال الأسرة، مثل إقامة شرع الله، وتحقيق مرضاته، لأنّ البيت المسلم ينبني على تحقيق العبودية لله تعالى، ولذلك ورد تعليل إباحة الطلاق حين تطلبه المرآة فإن خفتم أن لا يقيما حدود الله فلا[بالخوف من عدم إقامة حدود الله قال تعالى: .]جناح عليهما فيما افتدت به
كما أنّ الأسرة تحقق حفظ النوع الإنساني بإنجاب النسل ، ثم تتحمل المسئولية بتربيتهم وتوجيههم بما يسهم في بناء شخصيتهم السوية، لأن الإسلام جعل الأسرة هي المحضن الطبيعي الذي يقوم على رعاية الطفل ، واعتبر كل انحراف يصيب الناشئة مصدره الأول الأبوان ، لأنه يولد صافي السريرة ، سليم الفطرة ، قال عليه الصلاة والسلام: (ما من مولود إلا يولد على الفطرة ، فأبواه يهودانه أو ينصرانه أو يمجسانه ، كما تنتج البهيمة بهيمة جمعاء هل تحسون فيها من جدعاء) .
ولهذا أثبتت الإحصاءات العلمية أن تربية الملاجئ تؤثر على نمو الطفل واتزانه العاطفي ، كما أثبتت أن فترات الطفل هي سنواته الست الأولى ، وأن طفل الأسرة المستقرة المتوافقة ،غير طفل الأم العاملة المرهقة والمشتتة فكريا في أداء وظيفتها، كما أن نتائج التفكك الأسري في الغرب، سبب الجنوح والتشرد والجريمة والانحراف لمعظم الناشئة .

فالأسرة هي البيئة الأولى التي ينشأ فيها الأطفال صالحين كما أنها المجال الفريد لغرس عواطف حب الله ورسوله وحب المسلمين ، الذي تزول
معه كل عوامل الشحناء والصراعات المختلفة ، فيخرجوا إلى الحياة رجالاً عاملين نافعين يكونون لبناة صالحة للمجتمع .

أهمية الأمن

إن كلمة الأمن خفيفة على اللسان ، عميقة في الوجدان ، مطمئنة للجنان ، أنها نعمة عظمى، وغاية أسمى، يسعى إليها كل إنسان، بل هو مطلب أساسي لا تستقيم الحياة بدونه، وضعه الله جنباً لجنب مع مطلب وضرب الله مثلاً قرية كانت[الغذاء ، بل قدّمه عليه تارات لأهميته . قال تعالى : أولم[وقال تعالى :]آمنة مطمئنة يأتيها رزقها رغداً من كل مكان فكفرت بأنعم الله]نمكّن لهم حرما آمنا يجبى إليه ثمرات كل شيء رزقا من لدنا ٠٠٠

إن الأمن هو غاية المنى التي يسعى كل أحد للاستظلال بظلاله ولا حياة مع الخوف الذي تتحول الدنيا فيه إلى أرض مسبعة يفترس القوي فيها الضعيف ، وتصبح الحياة ظلمات بعضها فوق بعض .

إن الحياة مع الأمن تصير جنات، ظلالها وارفة ، يتبوأ الإنسان فيها حياة طيبة مباركة ، ويعيش عيشة راضية ، يثمر وينتج ، يصان عرضه وأرضه ، ودينه وماله ، ودمه،وأهله ونفسه وجميع من حوله ، يحمى ولا يهدد، يتفيأ ظلال الحرية، آمنا في جميع أحواله كل ذلك في ظل الإسلام بالعمل بكل ما يرضي الله، حتى يتم لهم الأمن في الآخرة بنيل رضا الله وثوابه . إن الأمن المطلوب هو الأمن على الحياة الطيبة في الدنيا، والأمن بحصول النجاة من غضب الله في الآخرة .

الذين آمنوا ولم[قال تعالى: يلبسوا إيمانهم بظلم أولئك لهم الأمن وهم لماذا كان لهم ذلك ؟ لأنهم]مهتدون خافوا مقام ربهم فجعل الأمن عاقبة أمرهم لأنه جاء في الحديث القدسي:(لا أجمع لعبدي أمنين ولا خوفين أبدا إن هو أمنني في الدنيا، أخفته يوم القيامة، وإن هو خافني في الدنيا أمنته يوم القيامة)

إن الأمن يلزم لكل نبضة حياة ، وحركة بناء ، ولكل كيان اجتماعي كبر أم صغر ، يحتاج إليه الأفراد كما تحتاجه الجماعات .

إذا حصل اختلال في مجال من مجالات الحياة كالقحط والكساد أو النقص في الأطباء أو المعلمين ، فإن الضرر الذي ينتج عن ذلك يكون محدودا على المجال الذي وقع عليه، وبالتالي يسهل احتواؤه والتغلب عليه لكن لو اضطرب ميزان الأمن واختل النظام العام فإن جميع نواحي الحياة تتأثر،فتسود الفوضى، ويحل الخوف والاضطراب، وينتشر الإجرام فتصبح مقدرات المجتمع بأيدي المجرمين مما يجعل تتوقف حركة البناء،وعجلة الإنتاج فيضطر الناس للهجرة إلى مجتمعات أكثر أمنا، هم ورؤوس أموالهم .

الحاجة إلى الأمن

إن الأمن حاجة إنسانية، وضرورة بشرية، وغريزة فطرية، لا تتحقق السعادة بدونه، ولا يدوم الاستقرار مع فقده، لأن مصالح الفرد والمجتمع مرهونة بتوفيره، ذلك لأن (الأمن للفرد والمجتمع والدولة من أهم ما تقوم عليه الحياة ، إذ به يطمئن

الناس على دينهم وأنفسهم وأموالهم وأعراضهم ويتجه تفكيرهم إلى ما يرفع شأن مجتمعهم وينهض بأمتهم) .
إن الأمن يحقق راحة في البال، وانشراحا في الصدر، وشعورا بالسعادة واستظلالا بالطمأنينة والسكينة ، يشعر في ظلة المرء بأنه محمي مصان بفضل الله تعالى ثم بفضل من تسبب في استتبابه فينطلق في هذا الجو الآمن إلى عبادة ربه على الوجه الصحيح ، وإلى عمارة الكون بتحقيق مصالحه، أما إذا خيم الخوف وزال الأمن فإن المصالح تتعطل والقدرة على حسن العبادة تتزعزع لأنّ (ثبات الأمن وتأكيده ، وتوفير الأمان وتعميمه هو المرتكز والأساس لكل عوامل البناء والتنمية، وتحقيق النهضة الشاملة وبدون ذلك يستوطن الخوف وتعم الفوضى ويشع الضياع فتفقد الأمة أساس البناء وأسباب البقاء) .
إن حاجة الأمن تظهر في الأمور الآتية :
١- تكمن أهميته والحاجة إليه في أن قلنا[الله تعالى لما أنزل آدم من الجنة بين له ما يتحقق به أسباب الأمن قال تعالى]اهبطوا منها جميعا فإما يأتينكم مني هدى فمن تبع هداي فلا خوف عليهم ولاهم يحزنون .
٢- إن أمن الإنسان على نفسه وماله وعرضه شرط في التكليف بالعبادات .
٣- إن من لم يأمن على نفسه باستعمال الماء أو خاف لحوق الضرر به من الوصول إليه تنقل إلى التيمم .
٤- يسقط عن المكلف استقبال القبلة عند عدم الأمن .
٥- يشترط لوجوب الحج أمن الطريق .
٦- كما أجاز الشرع التلفظ بكلمة الكفر عند عدم الأمن مادام القلب مطمئنا .
٧- عد النبي عليه الصلاة والسلام الأمن من أعظم النعم وأحد حاجات الإنسان الأساسية إذ جاء عنه قوله (من أصبح منكم آمنا في سرية معافى في جسده عنده قوت يومه فكأنما حيزت له الدنيا) .
أقسام الأمن
يتفرع الأمن بالنسبة للإنسان إلى نوعين داخلي وخارجي، ذلك لأنه إحساس داخلي في النفس البشرية يدعمه الواقع العملي، ولهذا حذر الإسلام أتباعه من إطلاق الإشاعات، ومن إذاعة أنباء الأمن أو أنباء الخوف ، ونشرها بين الناس دون الرجوع إلى ولي الأمر، لأنّ الأولى تدعو إلى التراخي عن الاستعداد، وعدم أخذ الأسباب، والثانية تفت من عضض بعض الناس، ويأتي هنا دور الأسرة في توجيه أبنائها على عدم ترويج الإشاعات، حفظا للأمن الداخلي ، وصيانة للمجتمع من الداخل حتى لا يتسرب إليه الضعف أو الخوف والرعب ، فيحقق الأمنان ، طمأنينة النفس واستقرارها من كل أنواع الشرور والأذى التي يمكن أن تتعرض له.فيأمن الإنسان في دينيه وعرضه وماله وأهله وبيته وبيئته، وفي ظل ذلك يؤدي كل أحد واجبه على أحسن ما يكون الأداء .
أما باعتبار ما يؤول إليه فينقسم الأمن إلى قسمين هما :
١- الأمن في الدنيا، وهو الأمن المقيد .
٢- الأمن في الآخرة ، وهو الأمن المطلق .

فالأول هو الاطمئنان الذي يحصل للإنسان على ضرورات الحياة وما يكملها ، بحيث لا يعتدي أحد على تلك الضرورات والمكملات، فإذا هم أحد بالاعتداء على شئ منها وجد ما يزجره من الزواجر التي وضعها الخالق عقابا شرعيا عاجلا أو عقابا أخرويا آجلا، وهذا القسم من الأمن حرص عليه جميع الأحياء لأنه محسوس ، عاجل ، والنفس مولعة بحب العاجل .

إن الأمن الدنيوي الذي يمنّ الله به على الأمم لا يدوم مع الكفران وضرب الله[، بل يبدلها الله به الخوف والجوع ، وسوء الحياة ، كما قال تعالى : مثلا قرية كانت أمنت مطمئنة يأتيها رزقها رغدا من كل مكان فكفرت بأنعم الله فأذاقها]الله لباس الجوع والخوف بما كانوا يصنعون

ومن الأمم التي أمتن الله عليها بالأمن في الدنيا ثم بدّلها به خوفا لكفرانها مشركوا قريش حيث قال الله مبيّنا حال . فلما أصروا] فليعبدوا رب هذا البيت الذي أطعمهم من جوع وآمنهم من خوف[أمنهم : على الكفر ومحاربة الله ورسوله ، أبدل أمنهم خوفا ، وغناهم فقرا ، وشبعهم جوعا ، وهو ما حكاه عنهم في آية سورة النحل السابقة .

إن الحديث عن الآمن الدنيوي وحده مفصولا عن الأمن الأخروي إنما هو حديث عن حلم بالسعادة في ساعة من الزمن ، من عمرنا القصير .

إن الإنسان مهما أوتي من نعمة ، ومن سلامة نفس وبدن ووفرة رزق ، لا يحس بالأمن الكامل ، أو الأمن بمعناه المطلق الذي ينافي كل خوف مهما كانت أسبابه .

لأن أمن الدنيا أمن مقيد، ولا يتحقق الأمن المطلق إلا بالاتصال بالمنهج الرباني .

القسم الثاني : الأمن الأخروي ، وهذا هو الأمن الحق إذا وفق الله له أمة من الأمم فهيأ لها أسبابه ، وحجب عنها موانعه ، يتحقق لها بتحققه أمن الدنيا وأمن الآخرة ، وأهم أسبابه الالتزام بمنهج الله وعبادته وحده لا شريك له ، فالأمة التي تؤمن بالله ، وتعمل صالحا ،هي الأمة الجديرة بالإستخلاف والتمكين ، والأمن في الأرض، فهي موعودة بالأمن التام يوم يخاف الناس ، وبهذا نعلم أن الأمن المطلق ، لا يوجد إلا في دار النعيم التي وعد الله بها عباده ادخلوها[الصالحين قال تعالى: ففي الجنة لا يكون خوف ولا فزع ، ولا انقطاع ولا فناء .]بسلام آمنين

مكانة الأمن في الكتاب والسنة

أثار القرآن الكريم انتباه الإنسان بشدة إلى حاجته الملحة للشعور بالأمن ، ليس فقط من مختلف الأخطار المحدقة بحياته ، بل أولا من عذاب الله ومكره ، ومن خسف الأرض، ومن الأعاصير والفيضانات ، ومن الرياح المحملة بالحصباء ومن الجوع والخوف والنقص في الأنفس والثمرات ، وأكد كتاب الله أن الأمن الحقيقي الكامل هو أمن الإنسان في الدار الآخرة ، والذي يتقرر بدءً ونهاية في هذه الدنيا فلا ينال أحد من الخلق الأمن إلا بسببين هما :

١- الإيمان بالله

٢- العمل الصالح ، فلا سعادة للإنسان بدونهما في الدارين كما قال تعالى :

الذين[.]آمنوا وتطمئن قلوبهم بذكر الله ألا بذكر الله تطمئن القلوب

إن الأمن النفسي الذي يتحقق بالدين الحق، يغلق منافذ الخوف كلها في نفس الإنسان

المؤمن فلا يخاف إلا الله: لا يخاف من البشر ، ولا من المخلوقات الظاهر منها والخفي ، كما لا يخاف من المجهول أو الموت ولا ما بعده لأنه عرّف الحقيقة ، وانكشفت له الغاية من خلقه، وهذا الذين آمنوا ولم يلبسوا إيمانهم بظلم أولئك[ما أكده كتاب الله في قوله تعالى : . بل قد قرن كتاب الله نعمة الأمن بنعمة الطعام في قوله]لهم الأمن وهم مهتدون . وجاء أيضا] فليعبدوا رب هذا البيت الذي أطعمهم من جوع وآمنهم من خوف [تعالى : تقديم نعمة الأمن على نعمة الرزق في قول الله على لسان نبيه إبراهيم عليه الصلاة . إن الفرد] رب اجعل هذا البلد آمنا وارزق أهله من الثمرات ... [والسلام : والأسرة والمجتمع يحتاجون إلى أمرين ضروريين هما الكفاية والأمن ، وقد أعطى كتاب الله الأمن درجة من الأهمية تناسب درجة الحاجة إليه والشواهد على ذلك كثيرة تتضح مع من عمل صالحا من ذكر أو أنثى[ما سبق من الآيات في الآيات الآتية : قال تعالى : وقال تعالى :]وهو مؤمن فلنحيينه حياة طيبة ولنجزينهم أجرهم بأحسن ما كانوا يعملون

وعد الله الذين آمنوا منكم وعملوا الصالحات ليستخلفنهم في الأرض كما استخلف[الذين من قبلهم وليمكننّ لهم دينهم الذي ارتضى لهم وليبدلنهم من بعد خوفهم أمناً ولو أن أهل القرى أمنوا واتقوا لفتحنا[وقال تعالى :]يعبدونني لا يشركون بي شيئا ، وقال تعالى]عليهم بركات من السماء والأرض ولكن كذبوا فأخذناهم بما كانوا يكسبون إن الذين يلحدون في آياتنا لا يخفون علينا أفمن يلقى في النار خير أم من يأتي[: .]آمنا يوم القيامة أعملوا ما شئتم إنه بما تعملون بصير

إن هذه الآيات كلها تبين الشروط التي يمكن يحصل من خلالها الإنسان على الأمن الإلهي في الدنيا والآخرة .

ولا شك أن رب الأسرة يستعرض لأبنائه هذه الآيات ثم يترك لهم جو الحوار والنقاش حولها ، ويطلب منهم أن يضربوا القصص والأمثال من الواقع المشاهد لديهم . ثم يعقب على ذلك فيقول لهم يا أبنائي (إن الله جعل الإيمان سببا للأمن وطيب الحياة والتمكين والاستخلاف في الأرض ونزول البركات من السماء، والثبات في الدنيا والآخرة وحصول الأجر الوفير في الآخرة ، وحسن العافية وتكفير السيئات ، وعدم الخزي والخذلان يوم القيامة) .

أما النصوص التي تدّل على الأمن في السنة النبوية فكثيرة منها على سبيل المثال لا الحصر .

قوله × : (لا يحل لمسلم أن يروع مسلما) .

وقوله : (من نظر إلى أخيه نظرةً يخيفه بها أخافه الله يوم القيامة) وقوله : (من حمل علينا السلاح فليس منا) وقوله × : (المسلم أخو المسلم لا يظلمه ولا يخذله ولا يكذبه ، ولا يحقره ، التقوى هاهنا ، ويشير إلى صدره ثلاث مرات، بحسب امرئ من الشر أن يحقر أخاه المسلم، كل المسلم على المسلم حرام : دمه وماله وعرضه) .

ومن دعائه عليه الصلاة والسلام قوله : (اللهم إني أسألك الأمن يوم الخوف) .

ففي هذه الأحاديث دعوة من النبي عليه الصلاة والسلام وحث منه على كل عمل

يبعث الأمن والاطمئنان في نفوس المسلمين ، كما فيها نهي عن كل فعل يبعث الخوف والرعب بين المسلمين قليلا كان ذلك أو كثيرا ، باعتبار أن الأمن من أجلّ النعم التي تفضل الله بها على عباده ، ولذلك نهى عليه والصلاة والسلام أن يروع المسلم أخاه المسلم .

بل جعل عليه الصلاة والسلام أن تحقق الأمن للإنسان بمثابة ملك الدنيا بأسرها ، فكل ما يملكه الإنسان في دنياه لا يستطيع الانتفاع به إلا إذا كان آمنا على نفسه ورزقه . قال عليه الصلاة والسلام: (من أصبح منكم آمنا في سربه معافى في جسده ، عنده قوت يومه ، فكأنما حيزت له الدنيا) .

دور الأسرة في تحقيق الأمن لأفرادها

الأمن التربوي

يأتي الطفل إلى هذه الدنيا كالصحيفة البيضاء النقية في عقله وفكره ومشاعره , وعنده الاستعداد الفطري لأي شيء يقدم إليه، ولذلك على الأبوين أن يتنبها لهذه النقطة ، ويدركا مدى خطورتها و أهميتها على نشأة الطفل ونموه ومستقبل حياته كلها . فبيدهما أن يأخذا به إلى مسار النجاة ويكون قرة عين لهما،وبيدهما أن يهملاه أوينحرفا به إلى دروب المهالك

ذلك أن الأسرة هي المؤسسة الأولى المسئولة عن التنشئة الاجتماعية للأطفال , ويرجع ذلك إلى أن الأسرة هي الجماعة الوحيدة التي تتفاعل مع الطفل لفترة طويلة من الزمن , في المرحلة الأساسية من حياة نموه ، ولذلك فهي تشكل عاداته ومواقفه , وتسهم في تكوين معتقداته عن طريق غرس القيم التي تؤمن بها .

إن قيام الأسرة بالوظيفة العضوية أو الاجتماعية أو الاقتصادية أمر طبيعي لأن الطفل عند ولادته غير قادر على القيام بهذه الوظائف ، بل عاجز عن القيام بأي وظيفة تضمن له استمرارية الحياة ، لذا كان لزاما على الأسرة أن تقوم بهذه الوظائف .

وسائل الأسرة في تحقيق الأمن

يتوقع الناشئة ذكورا وإناثا أن تقوم الأسرة بإشباع حاجاتهم الجسمية و النفسية ، والاجتماعية ، والدينية والعقلية ، فهم في حاجة إلى الرعاية الأبوية التي توفر لهم الحماية والأمن وتجنبهم الأضرار الجسمية ، كما يحتاجون إلى التأييد والتشجيع الذي يحقق نموهم الذاتي والاجتماعي ، فهم يمرون في الأسرة بالخبرات الخاصة بأسلوب الحياة الذي يهيئهم للقيام بدورهم الإيجابي في شئونهم ، والإشباع لحاجاتهم، وحاجات الآخرين ، فيكتسبون المعلومات والمعارف الأولية عن العالم، وعن الناس الذين يعيشون من حوله ، وبالتالي يشاركون في حياة الأسرة. بممارسة اتخاذ القرارات، وتنمية المهارات، والاستفادة من أساليب التصرف، والسلوك في المواقف المختلفة .

الأسرة وتحقيق الأمن النفسي والجسدي للناشئة

تعد الأسرة هي المحضن الطبيعي الذي يتولى حماية الطفولة الناشئة ورعايتها وتنمية أجسادها وعقولها وأرواحها، وفي ظلها تتلقى مشاعر الحب والرحمة والتكافل، وتنطبع بالطابع الذي يلازمها مدى الحياة، وعلى هدي الأسرة وتوجيهها

تتفتح ، وتفسر معنى الحياة الإنسانية وأهدافها، وتعرف كيف تتعامل مع الأحياء.
إن مرحلة الطفولة هي فترة إعداد وتدريب للدور المطلوب من كل حي في مستقبل حياته، لأن وظيفة الإنسان هي أكبر وظيفة، ودوره الذي ينتظره أعظم الأدوار، لأنه سيحمل أمانة الاستخلاف ودور المبتلى الممتحن بأمانة الله الملقاة على عاتقه لذا كان إعداده وتدريبه للمستقبل أدق وأطول و أشق، ومن هذا المنطلق كانت حاجته لملازمة والديه أشد من حاجة أي طفل لنوع من الأحياء الأخرى.
وقد أثبتت التجارب العملية أن أي مؤسسة أخرى غير مؤسسة الأسرة لا تعوض عنها ، ولا تقوم مقامها، وإن جادل الماديون في هذه الحقيقة وزعموا أن لا ضرورة للأسرة، وأن نشأة الطفل في محضن صناعي تساوي نشأته بين أبويه، بل يزيدون فيتحدثون عن إمكان صنع الأطفال بعيدا عن الأسرة وأعبائها الثقال، وكل ذلك مصادم للحقيقة والواقع، فالفطرة الإنسانية لا تقبل الزور، بل سرعان ما تنفضح الأنظمة المخادعة التي تشقي البشرية من حيث توهم إسعادها، فدور المحاضن والمدارس الداخلية لا توفر لكل طفل من العناية والرعاية ما توفره الأسرة لأفرادها تحت إشراف الأم ورعايتها، حنانا وحفاظا على جسده أولا ورفعا لمعنوياته ونفسياته ثانيا .
فالأسرة تعنى بولاية الطفل ورعايته، وتتعهده بما يغذيه وينميه ويؤدبه، ويحافظ على سلامته وأمنه من جميع الأخطار التي يمكن أن تحدق به ،
إن الحفاظ على الطفل في صغره من كل أنواع المخاوف التي تسبب له الأذى كالهوام، والسقوط، والأدوات الحادة والجارحة، والنار وغيرها، من وظائف الأسرة نحوه، فالأبوان مسئولان عن حفظه والمحافظة عليه ماديا ومعنويا ، ومن ذلك الاهتمام بالعقبات التي تعترض سبيله، ومن أهمها الخوف الذي هو غريزة فطرية في الإنسان فلا بد من وجود الخوف باعتدال فيه، حتى تكون حياته آمنة ، لأن الطفل الذي لا يخاف أبدا لا بد أنه مصاب بانحراف في نفسه، فالخوف ضروري لبناء شخصية الطفل ووقايته من الحوادث ، والتعرض للمخاطر، كالابتعاد عن النار والآلات الجارحة ، والأدوات الكهربائية وغيرها .
ومن مهام الأسرة تدريب الطفل على الخوف من الله تعالى،وتعليمه أن الضر والنفع لا يأتي إلا من الله ، وإن أتى من غيره فيكون بتقدير من الله تعالى وبإذن منه .
فتدربه الأسرة على العلاقة بينه وبين ربه ، وتخبره أن الله معه إن أحسن في عمله وحسّن خلقه مع الآخرين ، فالله يكافئه بالحسنات ويرفعه الدرجات العليا، وتغرس فيه المعية الإلهية، والحفظ الرباني له ، وإن أحس بخوف علّمه والداه الأدعية والأذكار التي تزيل عنه ذلك الخوف، وبذلك يرتبط بالإسلام منذ نعومة أظفاره ،
ومن واجبات الأبوين نحو أطفالهما رعايتهم باستمرار، والاهتمام بطعامهم وشرابهم وألعابهم، وتوجيههم إلى ما يفيدهم من الألعاب دون إكراههم على شيء معين منها، لأنه بقليل من التوجيه يمكن أن يكون اللعب وسيلة ناجحة لغرس بعض الصفات الخلقية والسلوكية الهامة في الأطفال ذكورا كانوا أو إناثا .
الأسرة وتحقيق الأمن الغذائي
تتوقف حياة الإنسان منذ أن يولد إلى أن يموت على ضروريات لا بد لـه منها،وهي

التي تتمثل في الغذاء والكساء والمقر، بالإضافة إلى ما يتبع ذلك من الحاجيات التي تحقق له نوعا من الراحة وتلبي له متطلبات غريزته مثل التداوي والتعليم .
إن مطالب الحياة تنقسم إلى الضرورية والحاجية والتحسينية، يهمنا هنا الأول منها ومنه نتناول دور الأسرة في تأمين الأمن الغذائي لأفرادها.
أن المولود أول أمر يحتاج إليه منذ ولادته هو التغذية، وأفضل غذاء له في الفترة الأولى من حياته هو لبن أمه الذي أودع الله فيه عناصر التغذية، والمواد النافعة للرضيع، فقد أمر الله الأم بإرضاع ولدها من لبنها لينتفع به ويستفيد منه] والوالدات يرضعن أولادهن حولين كاملين لمن أراد أن يتم الرضاعة..[قال تعالى: .
إن الطفل بأمس الحاجة في العامين الأولين من حياته إلى الغذاء عن طريق الرضاع الذي ينمي لحمه وينشذ عظمه، والأب هو المسئول الأول عن الطفل ومرضعته سواء كانت أمه أو غيرها ، لأنها تغذي الصغير بلبنها، فوجب الإنفاق عليها لتتغذى وتغذي الصغير بدورها . فالله تعالى أوصاها في الآية السابقة برعاية جانب الطفل وتأمين الغذاء له ، ذلك أن حضانة الطفل والسهر على مصلحته، والقيام بشئونه واجب على الأم ، لأنها ذات قلب رقيق ، وهي وحدها التي تطيق ذلك وتصبر عليه ، ولهذا فالأم أحق بحضانة الطفل في حال انفصالها عن الأب لحنانها وعطفها وشفقتها على ولدها أكثر من غيرها حتى من الأب .]..لا تضار والدة بولدها..
[نفسه قال تعالى:
ولا شك أن لتأمين الرضاع للطفل أهمية بالغة في حياته النفسية والجسدية والأمنية والاجتماعية، حيث (أثبتت الأبحاث العلمية أن الطفل الذي يرضع من ثدي أمه، لا يرضع الحليب فقط ، وإنما يرضع معه الحب والحنان، فيحس بدفء الأمومة وحنانها، وهذا يساعد الطفل على أن ينمو في صحة نفسية جيدة، ويكون بعيدا عن الإصابة بالأمراض النفسية في مراحل عمره اللاحقة) .
كما أن للغذاء الذي يحصل عليه المولود عن طريق الرضاعة الطبيعية دور في سلوكياته في مستقبل حياته فقد بينت الدراسات التي أجريت على بعض محترفي الإجرام في العالم أن كثيرا منهم قد حرموا من الرضاعة الطبيعية في طفولتهم وهكذا نجد أن تأمين الغذاء والرضاعة والحضانة من الأسرة لأفرادها له دور بارز في التنشئة السليمة البعيدة عن الانحراف والعنف والجريمة مما يترتب عليه إيجاد أفراد صالحين مستقيمين يكوّنون لبنات أساسية لمجتمع متماسك تقوم علاقاته على التآلف والمحبة.
الأسرة وتحقيق الأمن العقدي
إن تحقيق الأمن من أولى القضايا في حياة الناس , لذلك بذلت فيه الطاقات وصرفت في تحقيقه الجهود .
ولا يمكن أن يتحقق الأمن الافي ظل عقيدة صحيحة تتفق مع فطرة الإنسان التي فطر عليها ، ولا تتمثل تلك العقيدة إلا في التي أنزلها الخالق إلى الخلق .
ويأتي أهمية دور الأسرة في غرس العقيدة الإسلامية في نفوس أفرادها ، بل ينبغي أن تعنى بتقديم التربية الإيمانية على غيرها لأن الدين : (له أثره الواضح على النمو النفسي والصحة النفسية ، والعقيدة حين تتغلغل في النفس تدفعها إلى سلوك

إيجابي ، والدين يساعد الفرد على الاستقرار ، والإيمان يؤدي إلى الأمان ، وينير الطريق أمام الفرد في طفولته ، عبر مراهقته إلى رشده ، ثم شيخوخته) .
إن الأسرة المسلمة التي تولي الجانب الإيماني جل اهتمامها إنما تتبع طريق النبي × في تربية أصحابه رضوان الله عليهم ، فقد بدأ تربيتهم قبل كل شيء بالجانب الإيماني، فبدأ أولا بغرس العقيدة الصحيحة الصالحة في نفوسهم، ذلك أنه لا يمكن أن يتحقق للإنسان سعادة بلا سكينة لأنه لا توجد في الحياة نعمة أغلى ولا أفضل ولا أيمن هو الذي أنزل السكينة في قلوب[من سكينة النفس، وطمأنينة القلب، قال تعالى: .]المؤمنين ليزدادوا إيمانا مع إيمانهم...
فلا تتحقق السكينة إلا بالإيمان بالله تعالى، الإيمان الصادق العميق في القلوب . لأن النفوس مجبولة عليه، ومع ذلك تحتاج أن تتعلم أصوله وجزئياته، وأصلح أوقات غرسه السنوات الأولى من حياة الطفل ، لأنه يصغي إلى المربي بكل جوارحه ويقبلها دون نقاش كما أن خياله الواسع يساعده على تخيل الجنة والنار ، وأهوال القيامة ، والملائكة ،وعالم الجن وغيرها
إن غرس العقيدة في نفوس الناشئة يكون بوسائل عدة منها : تلقينه كلمة التوحيد ، كما كان السلف يعلمون أولادهم في أول حياتهم كلمة التوحيد ومنها تعليمه القرآن الكريم . لأنه أصل الدين وأساسه وفي حفظه أو حفظ جزء منه حفظ له ، فينشأون على الفطرة ، ويسبق إلى قلوبهم أنوار الحكمة كما يعلمهم السيرة النبوية ، والمغازي ، وسير الصحابة والتابعين ، وحكايات الأبرار وقصص الصالحين .
كما على المربي أن يعلم ناشئته أصول الإيمان وحقائقه فيلقنه الإيمان بالله ، وملائكته وكتبه ورسله واليوم الآخر والإيمان بالقدر خيره وشره .
كما يعلمهم أركان الإسلام الخمس ، ومستلزماتها فيحفظهم الشهادتين ، وإقام الصلاة ببيان ما تشتمل عليه من أعمال العبادة من ذكر واستغفار ودعاء وتلاوة القرآن ، وإيتاء الزكاة ومحاسنها ببيان وجوب مساعدة المسلمين بعضهم لبعض .
وصوم رمضان وما فيه من تدريب عملي على كف الشهوات، وتربية الإرادة على الصبر ، وحج بيت الله الحرام وما فيه من تجرد وانخلاع عن الدنيا.
إن الأسرة التي تقوم بغرس العقيدة في نفوس أفراد ناشئتها لا شك أنها تملأ أوقات الفراغ لديهم بكل نافع ومفيد ، وبالتالي تجنبهم الوقوع في الانحراف ، وتبعدهم عن كل مظاهر العنف ، وتبني شخصياتهم على الخير والعمل الداؤب ، وبالتالي تحقق لهم الأمن في أنفسهم بتحقيق حاجاتهم الدينية والنفسية ، وهذا يدفعهم للشعور بحاجات المجتمع وقيمه بما يحقق له الأمن والاستقرار .
الأسرة وتحقيق الأمن الاقتصادي
تعتمد الأسرة في حياتها على عدد من المقومات الأساسية بما يمكنها من القيام بدورها كمؤسسة اجتماعية في تحقيق الأمن، لأن نجاحها يتوقف على تكامل هذه المقومات، ومنها تحقيق الأمن الاقتصادي .
إن الأسرة تحتاج إلى دخل اقتصادي ملائم يسمح لها بإشباع حاجاتها الأساسية من مسكن ومأكل وملبس، كما تحتاج إلى سلامة أعضائها من الأمراض الجسدية ، وتدبير ما يلزمهم من خدمات صحية .

ولذلك اهتم الإسلام بوضع القاعدة التي لها الأثر الأكبر في الارتفاع بالمستوى المعيشي للفرد لينفق ذوا سعة من[والأسرة بدعوته إلى الإنفاق حسب الوسع والطاقة . قال تعالى : . ففي الآية بيان (الموازنة]سعته ومن قدر عليه رزقه فلينفق مما آتاه الله ... بين الدخل والاستهلاك ، فالنفقة على قدر حاجة البيت ، وعلى قدر حالة الزوج إعسارا أو إيسارا ، فهو لا يكلف الزوج أن ينفق فوق طاقته ، ولا يقبل منه أقل من متطلبات حياة أسرته ، واجتناب التبذير والإسراف وتضييع الأموال ، وصرفها في أمور لا تستحق الصرف) .

ولا شك أن كثيرا من الدراسات الاقتصادية أكدت أن الأسباب الرئيسية للانحرافات الاجتماعية تنبع جميعها من العوامل الاقتصادية . وأن كثيرا من الشرور تصاحب الفقر عادة، ولذلك كان للفقر أثرا واضحا في انحراف أو استقامة أفراد الأسرة .

والفقر يوصف بأنه الحالة التي لا يكفي فيها دخل الأسرة عن إشباع حاجاتها الأساسية المتغيرة للمحافظة على بنائها المادي والنفسي والاجتماعي والتعليمي ، فالفقر هو الذي يحرم الأسرة من المشاركة الاجتماعية .

إن كثيرا من الدراسات أكدت عن طريق البحث أن الحالة العقلية للمجرمين ترجع إلى الانحطاط الاقتصادي من ناحية ، وإلى التفكك الأسري من ناحية أخرى . وقد يحقق الدخل مطالب الأسرة المادية ، لكنه لا يحقق لها الشعور بالأمن , أو الإشباع النفسي والاجتماعي .

كما أن السكن السيئ يعتبر سببا في الانحراف فقد أكدت الحقائق العلمية أن المسكن غير الملائم يلعب دورا أساسيا في السلوك المنحرف فقد أثبتت الدراسات التي اهتمت بهذا الجانب أن نسبة الانحراف تزداد في المناطق المتخلفة التي تنقصها المرافق المادية ، ويكثر فيها التجمع ، كما ترتفع فيها درجة التزاحم، ونتيجة للازدحام الشديد في الأسرة يشتركون صغار الأولاد والبنات في نفس المكان مع الكبار وأحيانا مع غير أعضاء الأسرة ، كما يشترك المراهقون من الجنسين في الحجرة الواحدة .

إن السكن المشترك أو الضيق يدفع الطفل إلى الهروب من المنزل والتجمع في الشارع، نتيجة ما يشعر به من توترات وضغوط، وهذا ما يدفعه إلى الالتقاء مع غيره من الأحداث وتكوين العصابات التي تشجع على الانحراف .

إن كل أسرة في أي مجتمع هي ذات دخل وإنفاق، لكن الأسر تختلف فيما بينها من ناحية طريقة حصولها على الدخل : ثابتا أو متغيرا، أسبوعيا أو شهريا أو سنويا، كما تختلف فيما بينها من ناحية التصرف فيه ، فالأسرة المتأثرة بالتقاليد والعادات السائدة في مجتمع معين قد تندفع وراء مظاهر الإسراف ، أو اقتناء بعض الكماليات وبالتالي تستنفد كل دخلها ولا يبقى منه شيء للظروف الطارئة أو الأزمات ، أو قد يكون الإسراف على حساب بعض الضروريات ، وهكذا عندما تفشل الأسرة في تحقيق الاستقرار الاقتصادي يؤدي بها الموقف إلى أنواع من الصراع يقوم بين أعضائها من جانب وبينها وبين البيئة الخارجية من جانب آخر وهذا الصراع يولد أربعة أنواع من التصرفات هي على التوالي: العدوان ، النكوص ، الجمود ، الاستسلام .

وكلها لا شك ضد تحقيق الأمن داخل الأسرة ويكون لهذه السلوكيات أثارها الضارة على الأعضاء ومن ثم تظهر في نشاطهم وعلاقتهم بالمجتمع ، لأنهم يفقدون الثقة بأنفسهم وبالتالي لا يأمنهم المجتمع ولا هم يأمنونه، ويأتي دور الأسرة في توجيه أفرادها إلى أهمية المحافظة على المال لأنه عصب الحياة وقوامه التي تقضي به مصالح الناس ، والمحافظة عليه تكون بالنهي عن إهداره ، وتضييعه بالإسراف في استعماله أو صرفه لمن لا يحسن استعماله أو بالتبذير فيه .

الأسرة وتحقيق الأمن الصحي

يهدف الإسلام من تكوين الأسرة المسلمة إلى صيانة الأفراد والمجتمع من الأمراض الخبيثة والأوبئة المختلفة جنسية كانت أو غير جنسية .

ذلك أن الاهتمام بصحة الأفراد يعدّ هدفا أساسيا يجب أن تضعه الأسرة نصب عينيها إذا أرادت أن توفر لأولادها نموا طبيعيا متكاملا ، لأن الصحة هي الدعامة الأولى في الشعور بالرضا والسعادة في حياة الناشئ، ولأنها هي التي تعده بالقدرة والطاقة للقيام بأعماله ومناشطه في الحياة، وهي من العوامل الرئيسية في تنمية القدرات العقلية عند الفرد ، وذلك باعتبار أن العقل السليم في الجسم السليم ، كما أنها من العوامل الهامة في زيادة كفاءة الفرد الخلقية والاجتماعية والتعبدية ، وفي عمارة الأرض وترقية الحياة وتنميتها ، فالصحة تكاد تكون أهم شئ في حياة الإنسان .

ولا شك أن المرض يؤثر في حياة الأسرة تأثيرا بالغاً سواء من الناحية الاقتصادية أو الاجتماعية أو الجو النفسي المحيط بها

فبالصحة يحقق الإنسان آماله ورغباته، وينجز أعماله، ويؤدي واجباته ولأهمية الصحة عدّ الإسلام حفظ الذات وحفظ الجسد أمراً واجبا على الفرد ويأتي دور الأسرة في تحقيق الأمن الصحي لدى أفرادها عن طريق وقايتهم من كل أسباب الأمراض النفسية ، وتربيتهم على اكتساب القواعد التي تعلمهم النظافة والطهارة بما يحفظ سلامة أجسادهم .

الأسرة وأمن المجتمع

يتحقق الأمن في الأسرة أولا، وذلك بأن يقوم كل واحد من أركان الأسرة بدوره المنوط به، الدور الذي من أجل تحقيقه تكونت الأسرة، فالذكر والأنثى أوجد الله في كل منهما خصائص قبل الوظائف، فيحقق كل منهما وظيفته من خلال خصائصه، ويتحمل مسئولياته مع تعاون الجميع في أداء الواجبات ، قال ×: (كلكم راع وكلكم مسئول عن رعيته، فالإمام راع ومسئول عن رعيته، والرجل راع في أهله ومسئول عن رعيته والمرأة راعية في بيت زوجها ومسئولة عن رعيتها ..) .

فقد اعتبر الإسلام أن بناء الأسرة وسيلة فعّالة لتحقيق الأمن، ولحماية الأفراد من الفساد، ووقاية المجتمع من الفوضى، إن التربية الأمنية تبدأ في نطاق الأسرة أولا، ثم المدرسة، ثم المجتمع، فالأسرة هي المدرسة الأولى التي يتعلم فيها الطفل الحق والباطل، والخير والشر، ويكتسب تحمل المسئولية، وحرية الرأي، واتخاذ القرار، كل هذه القيم وغيرها يتلقاها الطفل في سنيه الأولى، دون مناقشة، حيث تتحدد عناصر شخصيته، وتتميز ملامح هويته،وإذا لم تتهيأ الفرصة بشكل كاف داخل

الأسرة لتعلم هذه القيم، فإنه يتعذر عليه بعد ذلك اكتسابها لكي تكون جزءا من سلوكه .
إنّ الأمن لا يفرض بسلطة، وإنما ينبع من أفراد المجتمع، من دخائلهم، من ضمائرهم، من أسلوب معاملاتهم، وللأسرة دور أساسي في غرسه في ناشئتها، وتعميقه في قلوبهم من البداية.
ولا شك أن أفراد الأسرة يمرون بمراحل مختلفة منذ ميلادهم إلى أن يشبوا ويكبروا،ويتحملوا المسئوليات الضخام،وفي كل مرحلة من مراحل نموهم يحتاجون أن تحقق لهم أسرهم الاستقرار النفسي والطمأنينة في مختلف أحوالهم كما تحقق لهم الإشباع في جميع حاجاتهم المتنوعة.
وعليها أن تبتعد عن الوسائل الخاطئة في تربية أولادها مثل استخدام القسوة و الشدة , والصرامة في معاملة الأولاد، وإثارة الرعب والخوف في نفوسهم، أو المبالغة في تدليلهم، والإفراط في التسامح والصفح عنهم .
وكذلك البعد عن الاستهزاء بهم والسخرية منهم أو إذلالهم ، أو التدخل المبالغ في شؤونهم بالرقابة الصارمة ٠
لأن استخدام القسوة التي يتبعها الآباء لضبط سلوك الطفل غير المرغوب فيه ، والتي يتضمن العقاب الجسدي كالضرب أو الصفع، أو كل ما يؤدي إلى الألم الجسمي، والمصحوب بالتهديد أوالحرمان٠
إن هذا العقاب يتضمن نتائج سلبية كثيرة حسب ما أثبتته الدراسات التجريبية، كأن ينشأ الطفل على تعلم السلوك العدواني ٠
لأن الآباء يمثلون نموذجا عدوانيا يقلده الطفل، فيلجأ لاستخدام أساليب القسوة، لحل الصراع في تعامله مع الأصدقاء والآخرين، إضافة إلى أن الطفل قد يتجنب التعامل مع الآباء الذين يعاقبونهم، مما يقلل التطبيع لدى الآباء إلى أبنائهم . لأنّ الشخصية الانفعالية والتوتر المصاحب للعقاب البدني قد يعطل قدرة الآباء على الحكم الموضوعي لحل المواقف , ويؤدي المزيد من النتائج السلبية سواء على مستوى نمو الطفل الاجتماعي .
أو على مستوى طبيعة العلاقة بين الآباء والأبناء .
يقول أحد الآباء إن الضرب والعنف يؤدي تنشئة جيل معقد منحرف .
ويقول آخر إن الضرب يجب أن يكون في فترات متباعدة لأن من الضروري أن نربيهم على نوع من الخشونة .
فالقسوة وإن أدت إلى الإساءة إلى معاملة الأطفال لكن لابد منها .
ويقابل القسوة , التساهل الذي يشجع الطفل على تحقيق رغباته بالشكل الذي يحلو له , والاستجابة المستمرة لمطالبه , وعدم الحزم في تطبيق منظومة الثواب والعقاب .
إن ضبط سلوك الطفل يعد شرطا أساسيا للنمو في اتجاه إيجابي ,فالآباء المتساهلون يعرقلون إحساس الطفل بالأمان , حيث لا يبعث الإفراط في التساهل على الثقة , لأن الرضوخ المستمر لمطالب الطفل قد يعكس ضعف الآباء . وهذا ينافي حاجته للشعور بقوتهما اللازمة لحمايته , لأن وجود درجة معينة من حزم الوالدين ضرورية للتنشئة السوية , وأن عدمها يؤدي إلى نمو الناشئة في الاتجاه السلبي

وبين القسوة والتساهل يظهر هناك اتجاه الإهمال لدى الوالدين,إذ يتجنبان فيه التفاعل مع الطفل ، فيترك دونما تشجيع على السلوك المرغوب عنه , ودونما توجيه إلى ما يجب أن يقوم به , أو إلى ما ينبغي عليه أن يتجنبه .
وهذا الإهمال لا يساعد الناشئة على غرس العادات الحسنة في نفوسهم في مرحلة مبكرة من حياتهم , لأنهم ينشأون على ما عودهم عليه المربون .
ويظهر هناك اتجاه آخر من الوالدين تجاه ناشئتهم وهو التذبذب : أي عدم التوازن في السلطة بين الأبوين , فالسلوك الذي يثاب من أحدهما قد يرفض من الآخر , ويعتبر هذا من أكثر الاتجاهات السلبية , لأن الأطفال قد يتكيفون مع آبائهم متساهلين أو متسلطين لكنهم يجدون صعوبة مطالب متغيرة وغير متوقعة , بل يؤدي بهم ذلك إلى الانحراف وعدم التوافق , فيصبحون أكثر عدوانية وتمردا , لأنه يسمح لهم بالسلوك مرة ويرفض مرة أخرى .
ومن الوسائل الخاطئة المبالغة في تدليلهم بالحماية المفرطة , وهذا لاشك خطر على صحة الطفل النفسية , يؤدي به في النهاية إلى نوع من الانحراف .
لأنه إذا قام أحد الوالدين أو كليهما نيابة عن الطفل بالواجبات أو المسئوليات التي يمكن القيام بها , والتي يجب تدريبه عليها إذا أردنا له أن يكون شخصية مستقلة .
لأن الحماية الشديدة تؤدي إلى قلة المواقف المناسبة لتنمية ثقل الطفل بقدراته .
ولذلك كان من الأهمية زرع الثقة في نفس الناشئة , وتركه لاكتساب خبرات جديدة مع مساعدته بالتقويم والتعديل والتوجيه المسحوب بالاحترام النابع من القلب ، بهذا العمل يعد الوالدان أولادهما لممارسة حياتهم المستقبلية , لأنه يتعود الاعتماد على النفس , وتقوى إرادته وعزيمته , وتنمّى مواهبه .
كما أن من الوسائل الخاطئة الاستهزاء بالأطفال والسخرية منهم أو إذلالهم. ويجب استبدالها بالاحترام الذي يحمل على إكرامهم وتقديرهم ولو أخفقوا في العمل، بل إن احترامهم يقتضي الثناء عليهم عند النجاح واستشارتهم في بعض الأمور ، واستحسان رأيهم الصائب، وإرشادهم برفق إلى خط رأيهم.
وإذا كان أحد الوالدين أو بعض الأقارب يستهزئ بالطفل أو يواجهه بالنقد الجارح كانتقاد الشكل أو العقل ، فعلى الأطراف الأخرى أن تدعم الطفل وتنمي ثقته بنفسه وتمدحه، وتمنع الأطراف الأخرى من الانتقاص من الطفل لأن ذلك يضعف ثقته بنفسه في المستقبل ويهز شخصيته ويجعله مستعدا للتخلي عن أفكاره بسرعة إذا انتقده الآخرون، ولو كانت تلك الأفكار صائبة، لأنه لم يتعود على الثقة بالنفس واحترامها،منذ الطفولة .
بل يجب أن يتحول هذا الاحترام إلى الحب والحنان لأنه من أهم الحاجات التي يتطلبها الناشئة .
إن وسائل إشباع حاجة الحب لديهم تختلف من مرحلة إلى مرحلة ففي مرحلة الطفولة المبكرة يلدُ المربي بملاعبة الطفل وترقيصه ومداعبته بأرق العبارات وتقبيله وضمه ، وبعد أن يبلغ خمس سنوات يحب الطفل أن يجلس قريبا من الوالدين أو يضع رأسه على فخذ أحدهما أو يقبلهم أو غير ذلك ، بل عن تشتد حاجته عند رجوعه من المدرسة أو من مكان لم يصحب فيه والديه أو عند وجود

مشكلة خارج البيت أو داخله ، وفي مرحلة المراهقة يظل محتاجا إلى الحنان والحب من والديه ، وذلك أنه قد يخجل من إظهار هذه العاطفة وبخاصة إذا كان والداه ينتقدان حاجته إلى الحب أو ينكران أن يقبلهما أو يسند رأسه إليهما أو يحسان بالإزعاج والتضايق عندما يعبر عن حبه لهم .
إن عدم إشباع هذه الحاجة يؤدي إلى انعدام الأمن وعدم الثقة بالنفس ، فيصعب على الطفل التكيف مع الآخرين، ويصاب بالقلق والانطواء والتوتر، بل يعد الحرمان من الحب أهم أسباب الإصابة بمرض الاكتئاب في المستقبل .
ومن الناحية الاجتماعية تحدث فجوة بين المربي والطفل عندما لاتشبع حاجته إلى الحنان فيحس الطفل بالانقباض تجاه والديه ويستقل بمشكلاته ، أو يفضي بها للآخرين دون والديه ،ويصبح عنده جوعة عاطفية ، تجعله مستعداً للتعلق بالآخرين
إنّ العوامل التي يمر بها أفراد الأسرة تحت مظلة الأسرة المستقرة الهادئة له الأثر الفعّال في حياتهم المستقبلية عندما يكونون أعضاء لمجتمع أو يكونون أزواجا في أسر. إنّ الشخص الذي يمر في طفولته بخبرات سارة توفر له الأمن والحب يمكنه النجاح في إقامة علاقات اجتماعية سارة، وإقامة علاقات أسرية سعيدة آمنة، كما أن الطفل المحروم من الحب أو المهمل أو التعس لا بد من أن يصبح أبا قاسيا، أو زوجا سيئا، أو شريكا غير موفق ، أرأيتم إذا دور الأسرة في تحقيق أمن المجتمع، حيث أن أفراد الأسرة هم الذين سيصبحون لبنات المجتمع، ورجال الغد، متمثلين في تحمل المسئوليات، أزواجا كانوا أو زوجات، أو مسئولين في مختلف قطاعات المجتمع، فإن ربوا على الخير والفضيلة والأمن واسعاد الآخرين فسيصبحون كذلك، وستصبح أسرهم الامتداد الأقوى في إمداد المجتمع بأفراد صالحين مصلحين.
أما إذا لم تؤد الأسرة دورها بأن تقاعست عن واجباتها تجاه البيت والناشئة، فعند ذلك لا تسأل عما يحدث للأفراد من المشاكل التي لا تحمد عقباها تجاه أنفسهم وتجاه والديهم وتجاه المجتمع ، وأن هذه الثلمة الكبيرة التي تحدث الآن لمجتمعنا من وجود إرهاب الأفراد والأسر والمجتمع والدولة لمن هذا القبيل . حيث حصل نوع من التقصير تجاه الناشئة من أطراف متعددة ومنها: تقصير الأسرة عن دورها المنوط تجاه أبنائها حيث انشغل الأب بتجاراته وأعماله تاركاً مسئوليته لغيره ، وانشغلت ربة البيت عن بيتها وزوجها وأبنائها بوظيفتها وأسواقها وزيارات صديقاتها، مسندة وظيفتها الحقيقة للخادمة التي أصبحت الأم الجديدة التي تعلق بها الأبناء أكثر من الأم لعنايتها بهم في الظاهر، أما الحقيقة تقول إن كثير من الأبناء يتعرضون للقسوة والإهمال من الخادمة خاصة في حال غياب الأم . وبالتالي ينشأون على الحقد وعقوق الوالدين وبغض المجتمع . ويتعودون على والاتكالية ، وتنعدم عندهم روح المبادرة ويتسع داء الفراغ ، الذي يتولد عنه تفريغ طاقاتهم في كل ما يضرهم ويضر أسرهم ومجتمعهم .
فمتى عادت الأسرة في أداء واجباتها ودورها الحقيقي رجع للمجتمع أمنه وسلامته كما كان يتمتع به من قبل .
نسأل الله تعالى أن يديم علينا نعمة الأمن والإيمان إنه ولي ذلك والقادر عليه وصلى الله وسلم على نبينا محمد وعلى آله وصحبه وسلم ...

الخاتمة
الحمد لله وحده والصلاة والسلام على من لا نبي بعده ..... وبعد
قد أصبح واضحا من خلال العرض السابق، إن الحياة لا تهنأ بدون أمن، وأنّ المجتمع لا يستقر بدون أمن، وأنّ الحضارة لا تزدهر بغير أمن، فإذا ساد الأمن في المجتمع اطمأنت النفوس، وانصرفت إلى العمل المثمر، فيعم الخير والرخاء عموم العباد والبلاد،وتقل الأزمات والمخاوف والقلاقل،
وبالتالي يكون الأمن ضروريا للفرد والأسرة والمجتمع، على حد سواء، وبشكل لا يمكن الفصل بينهم، كما لا يمكن أن يشعر الإنسان بالأمن والطمأنينة في مجتمع تسوده الفوضى، وتنتشر فيه المخاوف، وترتكب فيه الجرائم، ذلك أنّ أمن المجتمع مرتبط بأمن الفرد الذي يعيش فيه، وهذا يفرض على الأسرة أن تتحمل جلّ المسئولية تجاه أمن المجتمع، بغرسه وتنميته في نفوس أفرادها وسيكون مردود ذلك وثمرته عليها وعلى المجتمع.
النتائج
١- إنّ تحقق الحاجات النفسية الاجتماعية والأمنية الثقافية والاقتصادية والصحية للناشئة يسهم ببث الطمأنينة والاستقرار في نفوسهم .
٢- إن إشباع الأسرة لكل حاجات أبنائها باعتدال وانتظام يترك في نفوسهم عدم التعدي على حاجات الآخرين من أفراد المجتمع مما يسهم في أمنه
٣- إن أمن المجتمع لا يتحقق إلا بأمن الأفراد ، وأن أمن الأفراد لا يتم إلا في محضن الأسرة ، عبر دورها في عملية التطبيع الاجتماعي بنقل القيم التي تتفق مع الواقع الديني والثقافي للمجتمع .
٤- إن أفضل وسيلة لنشر الأمن هي تربية الأفراد على العقيدة الصحيحة ، وعلى المحبة والتسامح وكظم الغيظ والتواضع للمؤمنين .
٥- إنّ الأسرة إذا حققت الأمن الذاتي في أفراد أبنائها فقد حققت الأمن في المجتمع ، لأنه عبارة عن أسر متعددة، ينطبع بما تنطبع به أسره.
التوصيات
١- ينبغي أن تجعل الأسرة المسلمة تربية أولادها وتنشئتهم التنشئة الصالحة من أولى مهامها ، مطبقة تعاليم الإسلام وشرعه في شتى مجالات حياتها ، مدركة أن نجاحها يكمن في إخراج أبناء صالحين تنتفع بهم ويمتد نفعهم إلى الأقارب والمجتمع والإنسانية عامة .
٢- أن تبتعد الأسرة عن إرهاب ناشئتها وتخويفهم منذ الصغر ومنعهم من تحقيق مطالبهم عن طريق إشباع رغباتهم لأن توفير الأمن والشعور به منذ الصغر يحدد شخصية الطفل .
٣- أن تسعى الأسرة في إيجاد جو يسوده الوئام والتعاطف والتراحم داخل الأسرة لأن الناشئة إذا نشئوا في جو يسوده ذلك تحقق فيهم الأمن والاستقرار وبالتالي حققه في مجتمعهم .
٤- إعداد الآباء والأمهات لتحقيق وظائفهم من الوجهة السليمة لأن التربية الأسرية في الوقت الحاضر لم تعد تربية عادية لأن متطلبات الحياة فرضت عليها التطور

مما يستدعي حاجة الأسرة إلى فهم التربية الصحيحة بمراحلها المختلفة وفق منهج الإسلام عن طريق دورات منظمة للآباء والأمهات تقوم بها مؤسسات خدمة المجتمع .

٥- أن يكون هناك اهتمام أكبر بالأسرة يتعلق بتوجيهها لأنها أصبحت تواجه مشاكل كبيرة في التربية لتعقد الحياة وتبرز مظاهر الاهتمام هذه في إيجاد أسابيع ثقافية تحت عناوين مختلفة مثل الأسرة أولا ، الإسرة والوطن ، من أجل الأسرة ، والأسرة والقراءة ، الأسرة والتراث وغيرها حتى يكون لها الأثر في تركيز الانتباه نحو ثقافة الأسرة .

مراجع البحث

١. إبراهيم الصرايرة، أمن المجتمع مسئولية مشتركة بين المواطن والأجهزة الأمنية، ضمن محاضرات الموسم الثقافي الثاني , الأردن , جامعة مؤتة سنة ١٩٨٣ م.

٢. إبراهيم مصطفى وآخرون , المعجم الوسيط، القاهرة، مجمع اللغة العربية سنة ١٩٦٠ م.

٣. ابن ماجة، سنن ابن ماجة، تحقيق محمد فؤاد عبد الباقي،دار إحياء الكتب العربية، سنة ١٩٥٢م.

٤. ابن منظور , لسان العرب , طبعة دار المعارف.

٥. أبو حاتم البستي، صحيح ابن حبان، تحقيق محمد عثمان، المدينة المنورة ١٩٧٠م.

٦. أبو داود السجستاني سنن أبي داود،، مكتبة ومطبعة مصطفى محمد، د.ت.

٧. أبو عيسى محمد بن عيسى، سنن الترمذي، تحقيق إبراهيم عطوة، مطبعة مصطفى البابي الحلي،طبعة ١٣٨٥هـ..

٨. أحمد بن حنبل، المسند، طبعة القاهرة، سنة ١٣١٣هـ.

٩. أحمد بن شعيب النسائي، سنن النسائي، دار الفكر، بيروت سنة ١٩٨٧هـ.

١٠. أحمد بن فارس بن زكريا، معجم مقاييس اللغة، القاهرة، مصطفى البابي الحلبي وأولاده سنة ١٣٨٩ هـ.

١١. أحمد بن محمد، المصباح المنير في غريب الشرح الكبير، بيروت، المكتبة العلمية د. ت.

١٢. أحمد عمر هاشم , الأمن في الإسلام , مصر , دار المنار للطباعة والنشر , سنة ١٤٠٦ هـ.

١٣. أحمد يوسف، أثر العقيدة في تحقيق الأمن النفسي ص١٧، الفجالة، دار الثقافة للنشر والتوزيع، د.ت.

١٤. إسماعيل ابن كثير الدمشقي، المصباح المنير في تهذيب تفسير ابن كثير، للإمام، هذبه جماعة من العلماء بإشراف صفي الرحمن المباركفوري، الرياض، دار السلام للنشر، ط١، ١٤٢٠هـ.

١٥. أكرم ضياء العمري، التربية الروحية والاجتماعية في الإسلام، الرياض، دار اشبيليا، سنة، ١٤١٧هـ..

١٦. ب وولمان، مخاوف الأطفال ترجمة محمد الطيب،القاهرة،مكتبة الأنجلوا، ط٢ سنة ١٩٩١م.
١٧. باقر شرف القرشي، النظام التربوي في الإسلام، بيروت، دار المعارف للمطبوعات سنة ١٩٨٣ م.
١٨. حامد عبد السلام زهران، علم نفس النمو، القاهرة، عالم الكتب، ط٤، سنة ١٩٧٧م.
١٩. حسين محمد يوسف , أهداف الأسرة في الإسلام والتيارات المضادة، القاهرة، دار الاعتصام , ط٢ سنة ١٣٩٨ هـ.
٢٠. خليل الجر المعجم العربي الحديث،لاروسي،مكتبة باريس سنة ١٩٧٣هـ.
٢١. الراغب الأصفهاني، مفردات ألفاظ القرآن، تحقيق صفوان عدنان داوودي، دمشق، دار القلم، وبيروت، دار الشامية، ط١ سنة ١٤١٢هـ.
٢٢. الزبيدي، تاج العروس، بنغازي، دار ليبيا للنشر والتوزيع ١٩٦٦ م.
٢٣. عبد الحميد كشك، الأمن في ظل الإسلام، الإسكندرية، المكتب المصري الحديث , ١٩٨٧ م.
٢٤. عبد الرحمن بن عبد الخالق الغامدي دور الأسرة المسلمة في تربية أولادها في مرحلة البلوغ، الرياض، دار الخريجي، ط١ ١٤١٨ هـ٠
٢٥. عبد العزيز الفوزان، وتحقيق الأمن في الفقه الإسلامي، رسالة علمية مخطوطة لم تنشر نوقشت عـام ١٤١٧ هـ.
٢٦. عبد العزيز سليمان الحازمي، أثر الترابط الأسري في تكوين شخصية الشباب، الرياض , الرئاسة العامة لرعاية الشباب , ١٤١٥ هـ.
٢٧. عبد العزيز محمد النغيمشي، المراهقون دراسة نفسية إسلامية للآباء والمعلمين والدعاة، الرياض، دار المسلم للنشر والتوزيع،ط٢، ١٤٢٢هـ.
٢٨. عبد الله أحمد قادري , أثر التربية الإسلامية في أمن المجتمع الإسلامي، جدة، دار المجتمع للنشر، ط١ سنة ١٤٠٩ هـ.
٢٩. عبد الله بن أحمد النسفي، تفسير النسفي، بيروت، دار الكتاب العربي، د.ت.
٣٠. عبد الله خوج وفاروق عبد السلام , الأسرة العربية ودورها في الوقاية من الجريمة والانحراف , الرياض، المركز العربي للدراسات الأمنية والتدريب سنة ١٤٠٩ هـ.
٣١. عبد الله عبد المحسن التركي , الأمن في الإسلام وتطبيق المملكة السياسة الجنائية / الرياض , طبع وزارة الشئون الإسلامية والأوقاف د.ت.
٣٢. عطية صقر، الأسرة تحت رعاية الإسلام، الكويت، مؤسسة الصباح ط ١ ١٤٠٠ هـ.
٣٣. علي بن محمد الجرجاني، التعريفات، تحقيق إبراهيم الأنباري، لبنان دار الكتب العلمية، ط٢ سنة ١٤١٢ هـ٠
٣٤. عواطف علي سليمان , الأسرة والطفولة في الإسلام , دار التراث العربي , ط١ سنة ١٤٢١هـ.
٣٥. فاطمة المنتصر الكتاني , الاتجاهات الوالدية، في التنشئة الاجتماعية وعلاقاتها

بمخاوف الذات لدى الأطفال، رام الله، دار الشروق للنشر، د.ت.
٣٦. الفيروز آبادي، القاموس المحيط، بيروت، دار الجيل، د.ت.
٣٧. كافية رمضان , الأسرة وسيط تربوي , ضمن مجموعة أبحاث بعنوان: الأسرة والطفل , الشارقة , دائرة الثقافة والإعلام، ط١ ١٩٩٤م.
٣٨. كوثر محمد المناوي , حقوق الطفل في الإسلام، الرياض ,دار الأمل, ط٣، سنة ١٤١٤ هـ
٣٩. ليلى عبد الرحمن الجريبة، كيف تربي ولدك، الرياض، وزارة الشئون الإسلامية والأوقاف والدعوة والإرشاد، ط٢، ١٤٢٣هـ.
٤٠. محمد إبراهيم حور، مجموعة أبحاث، الشارقة دائرة الثقافة والأعلام،ط١، سنة ١٩٩٤م.
٤١. محمد بن إسماعيل البخاري صحيح البخاري، مصورة دارالشعب،بيروت١٣٩٠هـ
٤٢. محمد بن معجوز , أحكام الأسرة في الشريعة الإسلامية ح٢ ط سنة ١٤١٤هـ د.ت.
٤٣. محمد داوود، الإسلام والزمن المقبل، القاهرة، دار المنار، سنة ١٤١٢هـ
٤٤. محمد رشاد خليل، علم النفس الإسلامي العام والتربوي دراسات مقارنة، الكويت، دار القلم، ط١، ١٤٠٧هـ.
٤٥. محمد عقله , نظام الأسرة في الإسلام، عمان، مكتبة الرسالة الحديثة ط ١ ١٩٣٨ م.
٤٦. محمد فؤاد عبد الباقي، المعجم المفهرس لألفاظ القرآن الكريم، استنبول، المكتبة الإسلامية، د.ت.
٤٧. محمود حسن , رعاية الأسرة، الإسكندرية , دار الكتب الجامعية ,سنة ١٩٧٧م.
٤٨. محمود محمد الجوهري، ومحمد خيال، الأخوات المسلمات وبناء الأسرة القرآنية، الإسكندرية، دار الدعوة للطباعة، د.ت٠
٤٩. مسلم بن الحجاج القشيري، صحيح مسلم، تحقيق محمد فؤاد عبد الباقي،نشر رئاسة البحوث العلمية بالمملكة العربية السعودية، سنة ١٤٠٠هـ .
٥٠. الموسعة الفقهية ,الكويت إصدار وزارة الأوقاف والشئون الإسلامية، طباعة ذات السلاسل ط١ سنة ١٤٠٦ هـ .
٥١. نادية عبد العزيز الهلالي، أثر الإيمان في تحقيق الأمن وثماره في الدولة السعودية، رسالة علمية للماجستير قدمت إلى جامعة الإمام محمد بن سعود الإسلامية كلية أصول الدين قسم العقيدة ونوقشت عام١٤٢٠ هـ.
٥٢. يوسف البزة أهمية التشريع الإسلامي في حماية الأسرة ورعاية حقوق أفرادها،جامعة الدول العربية،الأمانة العامة،١٤٠٦ هـ
٥٣. يوسف القرضاوي، الإيمان والحياة، بيروت، مؤسسة الرسالة، ط٧، سنة ١٤٠١هـ

وسائـل التحـقيق في جـرائم نظـم المعلومات
سليمان مهجع العنزي، ماجستير
أكاديمية نايف العربية للعلوم الأمنية، ١٤٢٤هـ2003 / م
تهدف هذه الدراسة إلى تحديد وسائل التحقيق في مجال جرائم نظم المعلومات وذلك بالكشف عن الجوانب المختلفة المحيطة بجريمة نظم المعلومات بتحديدها، ومعرفة دوافعها وإبراز أضرارها، وحصر الأساليب والأدوات المستخدمة من قبل مجرمي نظم المعلومات، وعن كيفية الحصول على تلك الأدوات المستخدمة في ارتكاب جرائم نظم من قبل مجرمي نظم المعلومات بالمملكة، والمنافذ المستخدمة من داخل المؤسسة أو من خارجها لارتكابها، وأدوات ضبط الجريمة والتحقيق فيها، وبيان العوائق التي تحول دون استخدام تلك الوسائل، وتحديد أنواع الأدلة المثبتة لارتكاب تلك الجرائم، وتحديد الإجراءات الأمنية سواء كانت فنية أو إدارية لتحقيق أمن نظم المعلومات، ومعرفة أسس صياغة إطار عام للسياسة الأمنية الشاملة لحماية نظم المعلومات .
يبلغ مجموع عينة الدراسة بشكلها النهائي (١٤١) فرداً، وتتكون من (٣٦) محققاً، ومن (٦٨) عاملاً بمجال نظم المعلومات، ومن (٣٧) متخصصاً في المؤسسات الموفرة لتقنيات أمن نظم المعلومات .وتتكون مؤسسات عينة العاملين بالنظم من الشركات المتخصصة في مجال تقنية المعلومات تمثل (٥٠,٠ (;1642#&من مجموع مؤسسات العاملين، والقطاع الحكومي ويمثل(١٦,٢(;1642#&، والقطاع المصرفي ويمثل (١٦,٢(;1642#&، والشركات غير المتخصصة في مجال تقنية المعلومات وتمثل (١٧,٦(;1642#&، وتوفر ما نسبته (98.5;1642#&) من تلك المؤسسات الإنترنت لموظفيها، كما يرتبط (٨٦,٨ (;1642#&منها بالإنترنت عن طريق الشبكة المحلية المربوطة بمزود الخدمة، وما نسبته (79.4;1642#&) منها يوجد بها سياسات أمنية، وما نسبته (٥١,٥ (;1642#&منها تصرف أكثر من (٣٠ (;1642#&على تقنية المعلومات من أجمالي ميزانيتها، وما نسبته (45.6;1642#&)منها تمتلك أكثر من (١٠٠٠) جهاز حاسب الآلي، وما نسبته (73.5;1642#&) منها يتوفر بها قسم متخصص في أمن المعلومات.
تم استخدام أداة الدراسة (الإستبانة) لجمع البيانات اللازمة للدراسة وتكونت من البيانات العامة التي تناولت خصائص عينة الدراسة وتكونت من (٩) فقرات، أما البيانات التفصيلية فشملت مكونات السياسة الأمنية الشاملة لحماية نظم المعلومات وتكونت من (١٢) فقرة الإجراءات الفنية ولإدارية لأمن نظم المعلومات وتكونت من (٣٢) فقرة، وجرائم نظم المعلومات وتكونت من (٨١) فقرة، ووسائل التحقيق في جرائم نظم المعلومات وتكونت من (34) فقرة، والعوائق التي تحول دون استخدام تلك الوسائل وتكونت من (٢٢) فقرة، وأنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات وتكونت من (٤) فقرة. وقد تبين أن الأداة ذات ثبات Reliability عالي بلغ (٠,٧٨٠٣ .(
أظهرت نتائج الدراسة في مجال السياسة الأمنية إن أقل العناصر وضوحاً في مكوناتها بالمؤسسات على الترتيب الاحترازات الشخصية (٢٢,٧(;1642#&،

والتشارك في الخدمات (٢٢,٧(;&#1642، والعلاقة بالمنافسين والشركاء (٢٤,١(;&#1642، والوثائق ووسائط الحفظ(;1642#&27.0) ، والبرامج المطورة داخلياً (٢٩,١(;&#1642، والجانب البشري(;1642#&43.3) ، وفي مجال الاجراءات الأمنية لحماية نظم المعلومات أظهرت نتائج الدراسة إن أقل الإجراءات أتباعاً (على الترتيب) توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها (٢,٢٠)، ومنح الحوافز للالتزام بالإجراءات الأمنية(2.25) ، والتأكد من مزامنة ساعات الأجهزة باستمرار (٢,٤٤)، وربط الترقية والدورات)والحوافز الأخرى) بمدى التقيد بأمن المعلومات (٢,٦٦)، وتحديد مدة صلاحية كلمات المرور وتغييرها (٢,٧٥)، والتقدم بشكوى حول جرائم نظم المعلومات (٢,٩٥)، وتحديث النسخ الاحتياطي المركزي (٣,٠٧). وهذا يدل على أن هناك قصور أمني بأتباع تلك الإجراءات.

وفي مجال جرائم نظم المعلومات أظهرت نتائج الدراسة أن أفراد عينة الدراسة (المحققين، والعاملين بمجال نظم المعلومات) يوعون ويدركون بدرجة قوية خطورة جرائم نظم المعلومات (٤,٥٨)، كما أظهرت ارتفاع معدل جرائم نظم المعلومات بعد ظهور الإنترنت (٤,٤٨). كما أظهر نتائجها أن هناك جرائم نظم معلومات حجم حدوثها عالي وهي على الترتيب؛ إرسال وزراعة الفيروسات (٤,٠٦)، ونسخ البرامج والاستخدام غير المصرح به (٣,٨٩)، والتلاعب بإدخال البيانات (٣,٨٨)، وتغيير البرامج والإعدادات(3.86) ، وإرسال أحصنة طروادة (٣,٨٣)، والاستيلاء على ما سوى المعلومات (٣,٤٠(، وتغيير البيانات بعد إدخالها (٣,٣٢)، وتدمير الملفات وقواعد البيانات (٣,٢٦)، كما هناك أساليب حجم استخدامها عالي نحو المؤسسات (سواء من الداخل المؤسسة أو خارجها (وهي على الترتيب؛ إرسال الفيروسات بالبريد الإلكتروني أو برامج المحادثة وما شابهها (4.52)، إرفاق أحصنة طروادة بالبرامج (٤,٢١)، والنفاذ عبر الشبكة إلى الأجهزة المربوطة بها ومحاولة العثور على ملفات مشاركة غير محمية (٣,٨٧)، واستغلال الثغرات التي تكتشف في نظم التشغيل والتطبيقات العاملة معه (٣,٧٤)، ومحاولة اكتشاف المنافذ المفتوحة والدخول منها (٣,٧٤(، Spoofing IP (3.65)، واستغلال الثغرات الأمنية في مزودات web مثل مزود(3.59) IIS ، واستخدام برامج حديثة تقوم باستغلال نقاط الضعف في برامج الحماية واستغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة .(3.50) واستغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة (٣,٤٧)، كما أظهرت أن حجم استخدام منفذ شبكة الإنترنت وبرامج الاختراق الموجودة بها (٤,٢٥ (كمنفذ خارجي أعلى من المنافذ الداخلية والخارجية الأخرى كإفشاء الرقم السري من قبل الموظفين (٤,١٦)، أو المحاولة المتكررة (٣,٩٥)، أو عن طريق الأجهزة ومحركات الأقراص المرنة والليزر (٣,٩٥)، أو عن طريق الشبكة المحلية LAN وبرامج التشارك في الموارد(3.91) ، أو الشبكة الواسعة WAN والبرامج المرتبطة (٣,٨٨)، كما أظهرت هناك أدوات حجم استخدامها عالي نحو المؤسسات (سواء من الداخل المؤسسة أو خارجها)، وهي على الترتيب؛ الفيروسات وديدان

الإنترنت (٤,٥٣)، و(4.51) Cookies، والبريد الإلكتروني (٤,١٨)، والمشاركة في الملفات على الشبكة (٤,٠٨)، برامج التنصت على الشبكات (٣,٨٩)، برنامج(3.80) Net Bus، وبرنامج(3.75) Sub Seven ، وبرنامج(3.51) ICQ ، وبرنامج Password Recovery Toolkit (3.46)، وبرنامج .(3.29) Tribe Flood Network وأن هناك طرق حجم سلوكها للحصول على أدوات ارتكاب الجرائم عالي، وهي؛ الحصول عليها كبرامج مجانية من مواقع على شبكة الإنترنت (٤,٩٦)، الحصول عليها من أماكن البيع غير قانونية للبرامج (٤,٧١)، الحصول عليها كبرامج غير مجانية تشترى من مواقع على شبكة الإنترنت (٣,٦٦)، وأما من ناحية عدد تحدث جرائم نظم المعلومات بمؤسسات عيينة الدراسة بشكل يومي على الأقل بما نسبته (٢٣,٥ (;1642#&منها، كما تحدث جرائم نظم المعلومات بشكل غير منتظم على الأقل بما نسبته (٤٧,١ (;1642#&من مؤسسات عيينة الدراسة، وتتعرض ما نسبته (١٢,٨ (;1642#&من مؤسسات عيينة الدراسة إلى إنذارات بوجود جريمة عن طريق الإنترنت تصل إلى أكثر من (١٠٠٠) إنذار في الأسبوع.، وأظهرت النتائج أن هناك اعتماداً كبيراً على ضمانات موردي الأجهزة والبرامج بدلاً من تتبع الجرائم (٣,٣٨)، وأن جرائم نظم المعلومات تسببت لما نسبته (٢٠,٦ (;1642#& من مؤسسات عينة الدراسة بخسائر مادية تبلغ أكثر من (١٠ (;1642#&من نسبة أجمالي مصروفات المؤسسة في عام ٢٠٠١م. كما ارتفاع حجم بعض دوافع جرائم نظم المعلومات، وهي على الترتيب دافع التسلية وحب الاستطلاع (٤,١٩)، ودافع الوصول إلى معلومات شخصية(4.06) ، ودافع إبراز قدرات (٤,٠٢)، ودافع الانتقام (٣,٩٨)، ودافع الاقتصادي والتجاري (٣,٢٥). كما أظهرت أن هناك فروق جوهر بين حجم بين بعض الجرائم في المؤسسات وأعداد الحاسبات الآلية التي تمتلكها، وتوفر الإنترنت، وأسلوب الدخول لها، كما يوجد فرق جوهري ذي دلالة إحصائية بين نوع المؤسسة في عدد مرات حدوث جرائم نظم المعلومات بالمؤسسات، ويوجد فرق جوهري ذي دلالة إحصائية بين متوسط حجم استخدام أدوات ارتكاب الجرائم من قبل مجرمي نظم المعلومات نحو المؤسسات.

وفي مجال وسائل التحقيق في جرائم نظم المعلومات أظهرت النتائج أن برامج الحماية تساعد بما نسبته (94.2٪) في تحديد نوع الجريمة، وما نسبته (٩٥,١ (;1642#&في تحديد توقيت ارتكاب الجريمة وما نسبته (٧٥ (;1642#& في تحديد مصدر الجريمة، وما نسبته (94.2٪) في الإعلام بوجود جريمة مرتكبة، كما أنه بالإمكان الاعتماد على عنوان(94.2٪) (IP ، وبرامج الحماية (٩١,٤(;1642#&، وبرامج تتبع المخترقين (٧٤,٩(;1642#&، وبرامج تتبع مصدر الرسائل الإلكترونية(59.6٪) ، ووسائل أمن البيانات (٨٨,٥(;1642#&، وتعقب إجراءات أمن العاملين (٧٩,٨ (;1642#&بتحديد شخصية مرتكب جريمة نظم المعلومات في المؤسسات، وأظهرت نتائج الدراسة أهمية الأدوات التالية التي يمكن تساعد بضبط الجريمة (مرتبة حسب أهميتها) سجل الصلاحيات للمستخدمين (٤,٩٤)، والتقارير

التي تنتجها نظم أمن البيانات (٤,٨٦)، وبرامج النسخ الاحتياطي والتسجيل Logging (4.76)، وبرامج كشف الفيروسات (٤,٧٤)، وأدوات المراجعة Auditing (4.69) ، وتقارير الجدران النارية (٤,٥٣)، وأدوات مراقبة المستخدمين للشبكة (٤,٥٢)، وبرامج تتبع المخترقين(4.11) ، ومراجعة قاعدة البيانات (٤,٠٧)، برامج تتبع مصدر الرسائل (٤,٠٦). كما أظهرت نتائج الدراسة أهمية الأدوات التالية والمساعدة بالتحقيق (مرتبة حسب أهميتها (أداة فك التشفير (٣,٩٥)، وبرامج كسر كلمة المرور (٣,٩٣)، وأدوات استرجاع المعلومات من الأقراص التالفة مثل(3.92) View disk ، وبرامج مقارنة النسخ (٣,٧٨)، وبرامج تشغيل الحاسب مثل .(3.29) Bootable diskette كما أظهرت نتائج الدراسة أهمية أنواع الأدلة المادية المثبتة لارتكاب جرائم نظم المعلومات التالية، (مرتبة حسب أهميتها (دليل تسجيل الوقائع (٤,٥٠)، ودليل التغير الظاهر على البرامج (٣,٨٦)، ودليل وجود أحصنة طروادة (٣,٥٦)، ودليل وجود فيروسات (٣,٥٣).

أما في مجال معوقات استخدام وسائل التحقيق في جرائم نظم المعلومات، تعتبر عينة الدراسة أن هناك معوقات عدم وجود تشريعات واضحة خاصة بجرائم نظم المعلومات في البلد (٤,٦٣)، ومعوقات متعلقة بالجريمة هو عدم المعرفة بمكونات عناصر جريمة نظم المعلومات من قبل الأطراف المعنية بالجريمة(3.56) ، ومعوقا ت تتعلق بالجهات المتضررة من جرائم نظم المعلومات، وتشمل؛ عدم تقدم معظم المؤسسات المتضررة من جرائم نظم المعلومات بشكوى للجهات الرسمية (٤,٠٩)، وعدم التدريب على استخدام التقنية المساعدة في كشف المجرمين (٣,٨٥)، ومقاومة الموظفين للوسائل الأمنية للإبقاء على قدر من الحرية (٣,٨٣)، وعدم قناعة العاملين بمجال نظم المعلومات في تدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية(3.83) ، وعدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق (٣,٤٨)، وعدم التنسيق بين الأجهزة الأمنية والمؤسسات المستخدمة لنظم المعلومات .(;1642&#93.3) أما معوق الأحجام عن الإبلاغ عن جرائم نظم المعلومات فهي بسبب الحفاظ على السمعة (٤,٧٥)، وبسبب عدم الرغبة في الظهور بمظهر الضحية (٤,٣٨)، وبسبب الخوف من المسؤولية (٤,٢٧)، وبسبب محدودية الآثار المترتبة على الجريمة (٤,٠٩(، بسبب عدم اكتشاف الجريمة رغم القناعة بإمكانية وجودها في الواقع (٣,٦١)، أما المعوقات المتعلقة بجهات التحقيق فهي؛ عدم توفير الأجهزة والبرامج المناسبة للتحقيق (٨٦,١(;1642&#&، وعدم توفير المتخصصين والخبراء في الحاسب الآلي (;1642&#69.4) وعدم التدريب في معاهد متخصصة بالتحقيق في جرائم نظم المعلومات(;1642&#86.1) ، أما معوق عدم توفر الكفاءة البشرية القادرة على التحقيق في جرائم نظم المعلومات فيشمل عدم توفر المهارة العالية لاستخدام الحاسب الآلي والإنترنت لدى حوالي نصف العينة (٤٧,٩(;1642&#&، ومعوق عدم المعرفة بمتطلبات أمن المعلومات لدى أكثر من ثلثي العينة (٦٦,٧(;1642&#&، ومعوق عدم المقدرة على إتباع السياسة الأمنية للتعامل مع

الجرائم لدى أكثر من ربع العينة(19.5٪) ، ومعوق عدم المعرفة بأساليب ارتكاب جرائم نظم المعلومات لدى أكثر من ثلثي العينة (٧٢,٢٪)، ومعوق عدم المقدرة على الإثبات الجنائي لجرائم نظم المعلومات لدى أكثر من نصف العينة (٥٢,٢ .٪)كما أظهرت الدراسة وجود فرق جوهري ذات دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية وسائل التحقيق والمعوقات التي تحول دون استخدامها