خاص لموقع المنشاوي للدراسات والبحوث www.minshawi.com

بحث بعنوان
الاستخدامات الغير مشروعة لتقنية المعلومات عبر شبكة الإنترنت

إعداد الباحث
دشن بن محمد القحطاني
dashen_k@hotmail.com

١٤٢٨-١٤٢٩هـ

المحتـــــويـــات

المبحث الأول : تعريف عام بتقنية المعلومات المتمثلة في الإنترنت.وتشمل :

- تعريف الإنترنت وبداياته .
- من يملك الإنترنت ؟.
- توسع شبكة الإنترنت.
- شبكة الإنترنت في المملكة العربية السعودية .

المبحث الثاني :بعض الاستخدامات الغير مشروعة لتقنية المعلومات متمثلة في الإنترنت ومنها :

- الإرهاب .
- التجسس الإلكتروني .
- الجرائم المنظمة والمافيا .
- القرصنة على الإنترنت .
- غسيل الأموال .

المبحث الثالث : الاستراتيجيات والإجراءات الأمنية المقترح اتخاذها للوقاية من الاستخدامات الغير مشروعة للتقنيـــة ومنها :

الأمن الإداري والمؤسسي .

أمن الأفراد .

أمن المنشآت .

أمن الاتصال الإلكتروني .

أمن الأجهزة والبرامج .

أمن التشغيل .

التوصيات والخاتمة

المقدمة :

منذ أن خلق الله الإنسان ، وهو في صراع مع الحياة ، من أجل البقاء ، ومن أجل تسهيل عيشته على هذه البسيطة ، فبدأ بإيجاد الطرق و الوسائل التي سخرها لخدمته ، ومن بين هذه الوسائل وسائل المواصلات ، وذلك لتناقل الأخبار والمعرفة، ولتسهيل التعامل بين الناس ، ومن أجل التبادل التجاري والثقافي بين الشعوب والأفراد ، بالإضافة إلى الجانب العسكري وتبادل الاتفاقيات والمفاوضات .

ولقد بدأ الإنسان في هذا العصر يتعرض 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 ازداد الاعتماد على نظم المعلومات والاتصالات في آخر عقدين من القرن الماضي ازديادا مضطردا حتى أصبحت تلك النظم عاملاً رئيساً في إدارة جميع القطاعات المختلفة كالقطاع المصرفي والتجاري والأمني فضلاً عن المشاريع الحيوية والحساسة كتوليد ونقل الطاقة . 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 أوجدت وسائل التقنية الحديثة صعوبات التحول المعلوماتي لدى مجتمعات الدول المتقدم ،و نجدها تخطط و تفكر في المؤسسات المطلوب إيجادها لاحتضان ذلك التحول والسير به في الطريق المستقيم ، إلا إننا نفتقد ،كما تفتقد معظم دول العالم الثالث ، مناهج التفكير المستقبلي المنظم ، لذا لا نجد أي أثر للدراسات و البحوث العربية المستقبلية التي تهتم بهذا المجال ، لغياب المنطلقات الأساسية التي تدعم زخم هذا الاتجاه وترعى حضانته ورعايته بجانب الاهتمام العلمي و التخطيط السليم ، سوء بعض الدراسات التي تهتم بجرائم الإنترنت ، ومنها دراسة أجرتها منظمة

(Busieness Software Alliance) في الشرق الأوسط حيث أظهرت أن هناك تباين بين دول منطقة الشرق الأوسط في حجم خسائر جرائم الحاسب الآلي حيث تراوحت ما بين (٣٠) مليون دولار أمريكي في المملكة العربية السعودية والإمارات العربية المتحدة و (١,٤) مليون دولار أمريكي في لبنان(موثق في البداينة،١٤٢٠هـ: ٩٨)

كما أظهرت دراسة قامت بها الأمم المتحدة حول جرائم الحاسب الآلي والإنترنت بأن (٢٤ – ٤٢ ٪) من منظمات القطاع الخاص والعام على حد سواء كانت ضحية لجرائم متعلقة بالحاسب الآلي والإنترنت (البداينة، ١٩٩٩م: ٥).

وقدرت الولايات المتحدة الأمريكية خسائرها من جرائم الحاسب الآلي مابين ثلاثة وخمسة بلايين دولار سنويا، كما قدرت المباحث الفيدرالية (FBI) في نهاية الثمانينات الميلادية أن متوسط تكلفة جريمة الحاسب الآلي الواحد حوالي ستمائة ألف دولار سنويا مقارنة بمبلغ ثلاثة ألاف دولار سنويا متوسط الجريمة الواحدة من جرائم السرقة بالإكراه.

وبينت دراسة أجراها أحد مكاتب المحاسبة الأمريكية أن مائتين وأربعين (٢٤٠) شركة أمريكية تضررت من جرائم الغش باستخدام الكمبيوتر(Computer Fraud).

كما بينت دراسة أخرى أجريت في بريطانيا أنه وحتى أواخر الثمانينات ارتكب ما يقرب من (٢٦٢) مائتين واثنين وستين جريمة حاسوبية وقد كلفت هذه الجرائم حوالي (٩٢) اثنان وتسعون مليون جنيه استرليني سنويا (محمد ، ١٩٩٥م : ٢١).

وأظهر مسح أجرى من قبل (the computer security institute) في عام (١٩٩٩م) إن خسائر (١٦٣) شركة من الجرائم المتعلقة بالحاسب الآلي بلغت أكثر من مائة وثلاثة وعشرين مليون دولار، في حين أظهر المسح الذي أجري في عام (٢٠٠٠م) ارتفاع عدد الشركات المتضررة حيث وصلت إلى (٢٧٣) شركة بلغ مجموع خسائرها أكثر من مائتين وستة وخمسين مليون دولار (Rapalus,2000)، كما بينت إحصائيات الجمعية الأمريكية للأمن الصناعي إن الخسائر التي قد تسببها جرائم الحاسب الآلي للصناعات الأمريكية قد تصل إلى (٦٣) بليون دولار أمريكي وان (٢٥٪) من الشركات الأمريكية تتضرر من جرائم الحاسب الآلي في حين أصيب (٦٣٪) من الشركات الأمريكية والكندية بفيروسات حاسوبية، وأن الفقد السنوي بسبب سوء استخدام الحاسب الآلي وصل (٥٥٥) مليون دولار (Reuvid,1998, p. 14)

ومن الصعوبة بمكان تحديد أي 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 التامين على الاستثمارات المالية (EFI) للإفلاس وبلغت خسائرها مليارين دولار أمريكي. وهناك أيضاً حادثة انهيار بنك بارينجر البريطاني في لندن اثر مضاربات فاشلة في بورصة الأوراق المالية في طوكيو حيث حاول البنك إخفاء الخسائر الضخمة باستخدام حسابات وهمية ادخلها 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 بالإفراد والشركات وخاصة الشركات الكبيرة حيث ينتج عنها توقف إعمال بعض تلك الشركات نتيجة إتلاف قواعد بياناتها، وتتراوح أضرار الفيروسات ما بين عديمة الضرر إلى البسيط الهين وقد تصل إلى تدمير محتويات كامل الجهاز، وإن كان الأكثر شيوعا من هذه الفيروسات هو ما يسبب ضررا محصورا في إتلاف 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 أمريكي، في حين وصلت الأضرار المادية لفيروس الحب الشهير (٨,٧) مليون دولار واستمر انتشار الفيروس لخمسة أشهر وظهر منه (٥٥) نوعا. (Ajeebb.com,8/8/2001)

وانطلاقاً من هذا الأساس ، يتحتم على الدول أن تعي مستقبل تقنية المعلومات وتأثيرها على المجتمع والبناء الجديد الذي تهدف له ، وذلك نظراً لأهمية تقنية المعلومات واستخدام الكمبيوتر في مختلف القطاعات وعلى كافة الأصعدة وفي هذا الإطار جاءت أهمية الدراسة لتلقي الضوء على الأساليب الغير مشروعة التي تستخدم تقنية المعلومات الاستخدام الخاطئ والغير واعي و الذي لا يتوافق مع القيم الشرعية و الدولية متمثلتاً في الإنترنت الذي يقدم جملة متنوعة من الاستخدامات التي تضعها تحت تصرف الأمور التعليمية والسياحة والإعلامية والثقافية والعلمية والعسكرية والاقتصادية والأمنية ، ومع استخدام الشبكات الدولية ترتفع يومياً درجة الاعتداء على خصوصية وسرية المعلومات بقصد التجسس أو التخريب أو السرقة أو ربما الابتزاز .وأمام هذا الخطر تبرز مخاوف السلطات الرسمية في معظم بلدان العالم من تبادل المعلومات ، ويستبد بها القلق من أن تكون هذه المعلومات ذات صلة بالتجسس السياسي أو العسكري أو تكون لها صلة بأنشطة إجرامية.

ونحن في هذا البحث سنحاول أن نلقي الضوء على الإنترنت عموماً وعن أهميته والدور الذي تقدمه تلك الوسيلة وتقديم رؤية أمنية حول الاستخدامات غير المشروعة عبر شبكة الإنترنت من خلال عرض لأهم الأساليب

المستخدمة وتقديم إستراتيجية وحلول ومقترحات قد تساعد في التقليل من خطر هذه الاستخدامات والعمل على مواجهة هذا التهديد والوقاية منه .

حيث سيتطرق الباحث في هذه الورقة إلى مباحث تنطلق منها الدراسة، وهذه المباحث هي:-

المبحث الأول: تعريف عام بتقنية المعلومات المتمثلة في الإنترنت.

البحث الثاني: الاستخدامات الغير مشروعة لتقنية المعلومات في الإنترنت .

المبحث الثالث : الإستراتيجيات والإجراءات الأمنية المقترح اتخاذها للوقاية من الاستخدامات الغير مشروعة للإنترنت

المبحث الأول : تعريف عام بتقنية المعلومات المتمثلة في الإنترنت وتشمل :

- تعريف الإنترنت : بداياتها ونشأتها .
- توسع شبكة الإنترنت.
- بعض خدمات الإنترنت .
- مستلزمات الاتصال بالشبكة .
- من يملك الإنترنت ؟.

تعريف الإنترنت:

يعيش العالم الآن ثورة معلومات هائلة بفضل الله أولا ثم بفضل وجود شبكة المعلومات العالمية (الإنترنت) التي تربط معظم أجزاء العالم، مكونة قرية إلكترونية صغيرة. وتعد شبكة الإنترنت مظهرا من مظاهر هذا العصر ولها تأثير كبير على حياة الشعوب في الجوانب العلمية والعملية، كما تعد الإنترنت من أهم مصادر المعلومات.

وقبل الحديث عن نشأة وتطور شبكة المعلومات العالمية (الإنترنت) يحسن أن يقدّم الباحث تعريفاً علمياً بهذه الشبكة، فشبكة الإنترنت أو الشبكة العالمية للمعلومات أو شبكة المعلومات العالمية كلها أسماء لمسمّى واحد، وهي شبكة مرتبط بعضها ببعض بوساطة حاسبات مختلفة الأنواع. ويرجع اختلاف الباحثين في إيجاد تعريف موحد لها لاختلاف زوايا النظر إليها. فالباحث ينظر إليها على أنها مرجع علمي ضخم ومكتبة عامرة بالكتب والمراجع والدوريات، وينظر إليها رجل الأعمال على أنها مجال تسويقي لكثير من منتجاته، ويراها الإعلامي وسيلة سهلة وسريعة لنقل الأخبار والتواصل مع المؤسسات الإعلامية.

وفي مجال التعريفات العلمية، فإن الإنترنت تعني في اللغة الإنجليزية ترابط الشبكات أو شبكة الشبكات (الفنتوخ ، ١٤٢١هـ : ١١) . وفي الاصطلاح يعرِّفها سيمبسون على أنها "خطوط اتصال تلف الكرة الأرضية

من جميع الجهات وتقوم بتحقيق الاتصال بين ملايين الحاسبات (سيمبسون ،١٩٩٩م:١٣). ويعرفها مصطفى السيد على أنها طريق المعلومات السريع ، ويذكر كنت أنها شبكة الشبكات أو مجموعة الشبكات العالمية (فدوي ، ١٤٢٤هـ :١٨). ويقدم عبد القادر الفنتوخ تعريفاً لشبكة الإنترنت وهو "ترابط بين الشبكات أو شبكة الشبكات حيث تتكون الإنترنت من عدد كبير من شبكات الحاسب المترابطة والمتناثرة في أنحاء كثيرة من العالم، ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول واحد هو برتوكول الإنترنت(TCP/IP) (الفنتوخ ، ١٤٢١هـ : ١١). ويذكر عبد العزيز الزومان تعريفا أوسع من غيره بأن الإنترنت "شبكة تربط مجموعة كبيرة من شبكات الحاسب الآلي المنتشرة في شتى أنحاء العالم حيث تتبع كل شبكة جهة مستقلة مثل الجامعات ومراكز البحوث والشركات وشركات تقديم خدمات الإنترنت" (الزومان ، ١٤٢٣هـ :٥).

من الملحوظ على التعريفات السابقة عدم الاختلاف الكبير بين الباحثين الغربيين والشرقيين فيها، أما ما يظهر من اختلاف فهو اختلاف تنوع لا تضاد، إذ هناك عناصر تجمع معظم تعاريف الإنترنت وذلك لعدم تباين عمل الإنترنت وخدماتها.

بداية الإنترنت:

لم تكن شبكة الإنترنت وليدة لحظتها بل سبقها كثير من المخترعات في مجال الحاسبات والشبكات، ولكن البدايات الأولية للشبكة العالمية تعود إلى عام ١٩٥٧م عندما أمر الرئيس الأمريكي (إيزنهاور) بإيجاد قاعدة بيانات للمعلومات العسكرية وتأمين عدم إتلافها تحسبا لقيام حرب نووية، وذلك في ظل الاحتياطات الاستراتيجية التي اتخذتها وزارة الدفاع الأمريكية وقت الحرب الباردة بين المعسكرين الشرقي بقيادة الاتحاد السوفيتي والغربي بقيادة الولايات المتحدة الأمريكية، وذلك بعد قيام الاتحاد السوفيتي بغزو الفضاء وازدياد النشاط بين المعسكرين في سباق التسلح النووي.

وكلفت الإدارة الأمريكية مؤسسة (راند) للأبحاث بدراسة وإيجاد وسائل لضمان استمرار الاتصال بين السلطات الأمريكية في حال نشوب حرب نووية ، وانتهت الدراسات إلى ضرورة وجود شبكة غير مركزية للقوات الأمريكية. وفعلاً قامت الإدارة الأمريكية ممثلة في وزارة الدفاع بتنفيذ هذا المشروع تحت مسمى "أربانت (ARPANET*)" في ١٩٦٩/١/٢م(فدوي ، ١٤٢٤هـ :١٨).

---

* أربانت (ARPANET)هي اختصار لـ (Advanced Research Project Agency Net). انظر: وجدي عبد الفتاح سواحل، انتفاضة الإنترنت: من الجهاد المسلح إلى الجهاد الإلكتروني، ط١، الجيزة، مركز الإعلام العربي، ١٤٢٢هـ، ص ٦.

وتقوم هذه الاستراتيجية على مفهوم أنه في حال تدمير مركز ما من مراكز الاتصال، فسيؤدي ذلك إلى شلل الحاسبات في ذلك المركز مما يؤدي إلى اضطراب في الإسناد الخاص بالمعلومات (الدناني ، ١٤٢٠ : ٤٣) مما يعني إعادة التوجيه الديناميكي للمعلومات من رابط إلى رابط آخر، حتى إذا قطع أحد هذه الروابط أو تعطل قامت الشبكة تلقائيا بتحويل حركة المعلومات إلى روابط أخرى لتصل إلى هدفها.

ويعتمد مشروع أربانت (ARPANET) على الربط بين جهات بحثية تابعة لوزارة الدفاع الأمريكية، بما فيها الجامعات وبين وزارة الدفاع لتبادل المعلومات (شاهين ، ١٩٩٦ :١٢) وقد بدت الشبكة في أوائل نشأتها صغيرة تربط بعض الأجهزة في أماكن متفرقة.

بعد ذلك تطورت (ARPANET) لتغطي كامل الولايات المتحدة الأمريكية(الدناني ، ١٤٢٠ : ٤٤). واستمر الأمر منذ نشأة المشروع عام ١٩٦٩م حتى عام ١٩٧٢م حيث تم توصيل ٧٢ مركز أبحاث بالشبكة، وكانت كلها تعمل لصالح وزارة الدفاع الأمريكية. وفي نهاية السبعينيات الميلادية انقسمت إلى قسمين رئيسين هما: ميلنت MILNET وهو اختصار لكلمتي (MilitaryNet) ويختص بالمجالات العسكرية، والثاني أربانت (ARPANET) ويختص بالمجالات والاتصالات غير العسكرية(شاهين ، ١٩٩٦ :١٣).

وشهد منتصف السبعينيات وأوائل الثمانينيات الميلادية مرحلة الازدهار لشبكة الإنترنت، وذلك بعد عقد المؤتمر الدولي لاتصالات الحاسب عام ١٩٧٢م بواشنطون، الذي حضره ممثلون من دول مختلفة، وناقش اتفاقية برتوكول الاتصال بين شبكات الحاسب، وفيه اختير رئيس للمجموعة التنفيذية للشبكة العالمية وكلف هذا الرئيس بوضع برتوكول يمكن أن تستخدمه أية شبكة للاتصال بشبكة أخرى في العالم. ثم طورت هذه البرتوكولات ليصبح هذا العمل تحت مسمى ربط الشبكات، ليصبح بالإمكان دخول أول مؤسستين من خارج الولايات المتحدة الأمريكية تقدمتا بطلب الدخول في هذا المشروع، وهما جامعة لندن، والمؤسسة الملكية للرادار بالنرويج في السبعينيات الميلادية(الدناني ، ١٤٢٠ : ٤٥) ، إلى أن أصبحت العديد من الشبكات المختلفة في بلدان متعددة يتصل بعضها ببعض، وإن لم تكن الإنترنت بالحجم والضخامة التي هي عليها الآن، إذ إن هذا النمو جاء بعد سنوات من ارتباط الشبكات ودخول العديد من المؤسسات والشركات والمنظمات المختلفة إلى الشبكة من خلال الحاسب الآلي. ومع حلول عام ١٩٨٣ م استُخدمت "أربانت (ARPANET)" بكثافة كبيرة، خصوصاً من قبل الجامعات، إلى حد أنَّها بدأت تعاني من ازدحام يفوق طاقتها، وصار من الضروري إنشاء شبكة جديدة(الزومان ، ١٤٢٣هـ :٦). وفي عام ١٩٨٦م أنشأت هيئة العلوم الوطنية الأمريكية شبكة تحت مسمى "نسفنت" (*NSFNET) ليستفيد

---

* "نسفنت" (NSFNET) هي اختصار لـ (National Science Foundation Net). انظر وجدي عبد الفتاح سواحل، مرجع سابق، ص ٧.

منها الباحثون في شتى المجالات العلمية لمصلحة المؤسسات الأكاديمية الرئيسة في الولايات المتحدة الأمريكية، وقد ربطت الشبكة بوساطة خمسة أجهزة حاسب فائقة السرعة، وأصبحت بعد ذلك بمثابة العصب لشبكة الإنترنت(فدوي ، ١٤٢٤هـ :٢٢) ، وأدى تزايد أحمال الشبكة إلى توسيع سعة شبكة هيئة العلوم الوطنية عام ١٩٨٨م ليربط ثلاث عشرة شبكة إقليمية بالإضافة إلى مراكز الحاسب الآلي العملاقة. وتتابع تزايد الأحمال لتزيد سعة الشبكة مرة أخرى عام ١٩٩١م(الزومان ، ١٤٢٣هـ :٦).

وفي فترة الثمانينيات الميلادية قل الاهتمام بالشبكة من قبل المؤسسة العسكرية الأمريكية وتركت أمر إدارتها للجامعات الأمريكية المشتركة فيها، لتنتشر سريعاً في الجامعات الأوروبية ثم في الجامعات الآسيوية، وأصبحت وسيلة مهمة في ذلك الوقت لنقل المعلومات وتبادل البريد الإلكتروني بين الجامعات المتصلة بالشبكة (الدناني ، ١٤٢٠ : ٦).

ومع هذا الازدياد السريع المتلاحق ظهرت عام ١٩٩١م خدمة البحث بوساطة الشبكة العالمية للمعلومات والتي يرمز لها بـ "WWW. WORLD WIDE WEB" وتسمى شبكة النسيج العالمية. والتي اكتشفها بفضل الله الباحث البريطاني تيم بيرنرز، الذي كان يعمل في مختبر الفيزياء بجنيف، حيث قام بمحاولة تصميم البرنامج عام ١٩٩٠م وانتهى منه في العام نفسه ليصبح النسيج على الإنترنت في صيف عام ١٩٩١م(الزومان ، ١٤٢٣هـ :٦) ، وأتاح هذا النسيج العنكبوتي (WEB) إمكان تجهيز المعلومات بطريقة ربط النصوص وإمكان انتقالها من وثيقة لأخرى، ومن موقع لآخر عن طريق تأسيس روابط ذات صلة بالموضوع المتوافر على الشبكة، كما تسمح الشبكة بالدخول والاستفادة من خدمات الإنترنت المتعددة واستعراض الملفات المخزنة والصور والفيديو، والبحث في قواعد البيانات، وعرض الوسائط المتعددة، لذا يمكن القول إن النسيج العنكبوتي هو اللب الفاعل للإنترنت (الزومان ، ١٤٢٣هـ :٧).

وفي عام ١٩٩٢م ارتبطت معظم الجامعات الأمريكية بهيئة العلوم وارتبطت معها وكالة أبحاث الفضاء "ناسا"(NASA)، وأمكن استخدام الصوت والفيديو في الإنترنت، وفي عام ١٩٩٣م توافر إمكان نقل الصور عالية الجودة والصوت عبر مسارات اتصال عالية السرعة عقب اكتشاف النسيج، وبعد اكتشاف النسيج ألعنكبوتي وزيادة الاشتراك في الإنترنت من قبل الجهات والأفراد، أغلقت شبكة هيئة العلوم الوطنية واستبدلت بها الجهات التجارية، لتدخل شركات تقديم خدمات الإنترنت للأفراد بصورة تجارية عام ١٩٩٤م.

وبعد ذلك دخلت الجهات الإعلامية والتجارية إلى الشبكة لتقديم الخدمات تجاريا، والاستفادة من الإعلان الإلكتروني على الشبكة، فقد بدأت الجهات الإعلامية تقديم الأخبار عبر اشتراكات ربحية إلى أن ظهر عقم هذه الطريقة فاتجهت إلى تقديم ذلك مجانا والاستفادة من الإعلان الإلكتروني. كما استفادت هذه الجهات من القوائم البريدية تجاريا، فمن خلال نوع الأخبار التي يطلبها المشترك تقوم بتزويدها لأصحاب السلع فيكون الإعلان حسب

نوع الخدمة الإخبارية*. إضافة إلى ذلك فقد تطورت الإنترنت كماً وكيفاً من خلال تعدد المواقع وتنوعها، ومن خلال الأساليب الإخراجية للمواقع.

لقد وجدت شركات متخصصة تقدم الإنترنت للدول وليس على مستوى الأفراد، وذلك عبر (كيابل) بحرية بأسعار منافسة وبسرعات أفضل من الأقمار الصناعية. وهذا بدوره أثر في حياة الشعوب المستخدمة للإنترنت من خلال الانفتاح الإعلامي الكبير الذي قدمته الإنترنت فأصبح بإمكان الشاب الإبحار في عالم واسع جدا من المعلومات.

لقد زادت مساحة الحرية والتعبير عن الرأي وأصبحت واقعاً مشاهداً، وربما لا تكون هناك جدوى كبيرة من منع كتب أو أشرطة مسموعة أو مرئية. إذ من خلال الإنترنت يمكن نشر أي مادة إعلامية دون الحاجة إلى الفسح الإعلامي.

ولم يتوقف تطور الإنترنت وأثرها عند هذا الحد، فلقد بدأت بعض شركات الإنترنت تقدم خدمة الإنترنت لاسلكياً في عدد من الدول ومنها المملكة العربية السعودية بوساطة شركات منها شركة أروبت وشركة أول نت في مناطق محددة من بعض المدن(مجلة مفتاح الإنترنت ، العدد٤٠ : ٧)

وأحدثت الإنترنت تغييراً في حياة الشعوب المستخدمة لها، وذلك من خلال العولمة الإعلامية التي تمثل انتشار فكر واحد وثقافة واحدة بين شعوب العالم.

وهناك سؤال يتردد كثيراً وهو من يملك ويدير الإنترنت ؟ وجوابه أن لا أحد في الوقت الراهن يملك الإنترنت ، وإن كان يمكن القول في البداية بأن الحكومة الأمريكية ، ممثلة في وزارة الدفاع ، ثم المؤسسة القومية للعلوم ، هي المالك الوحيد للشبكة ، ولكن بعد تطور الشبكة ، ونموها ، لم يعد يملكها أحد ، واختفى مفهوم التملك ، ليحل محله ما أصبح يسمى بمجتمع الإنترنت ، كما أن تمويل الشبكة تحول من القطاع الحكومي ، إلى القطاع الخاص .

ومن هنا ولدت العديد من الشبكات الإقليمية ، ذات الصبغة التجارية ، والتي يمكن الاستفادة من خدماتها مقابل اشتراك (أبو الحجاج ، ١٩٩٨م : ١٨) .

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

---

* مثال المشترك الذي يطلب أخبار السيارات ويتابعها، تقوم الجهة الإعلامية بتزويد ذلك لشركات السيارات مقابل مبالغ مادية تدفعها شركات السيارات، فتقوم هذه الشركات بإرسال رسائل إلكترونية إلى المشترك من بريد الشركة فيكون الإعلان حسب اهتمامات المشترك دون أن يعلم كيف حصل هذا.

وظهر حديثا ما يشير في هذه الأيام إلى وجود سباق فضاء من نوع آخر ، حيث استطاعت شركة ستارباند (star band) في تجربة أجرتها في شمال أمريكا ، من إكمال مشروع إنترنت بواسطة أقمار اصطناعية ذي اتجاهين ، وسرعته تبلغ (٥٠٠) خمسمائة ك . ب في الثانية ، من الإنترنت إلى الحاسب الآلي ، وسيبدأ تسويقه إلى المستهلك قريبا (الجزيرة ، ٢٠٠٠) .

شبكة الإنترنت في المملكة العربية السعودية:

تعد المملكة العربية السعودية من المجتمعات العالمية المحافظة على تقاليدها، وتتحفظ على إدخال المستحدثات، وغالباً ما تكون المجتمعات المحافظة أبطأ في تبني المستحدثات (إفريت روجرز : ص٨٤) ، وهذا ملحوظ عند دخول الإذاعة والتلفاز والقنوات الفضائية وأخيراً الإنترنت.

وتعد خدمة الإنترنت من الخدمات الحديثة التي انتشر استخدامها في المجتمع السعودي انتشاراً سريعاً وقت دخولها، مقارنة بالإذاعة أو التلفاز أو القنوات الفضائية أو حتى الحاسب الآلي. ويمثل دخول الإنترنت إلى المملكة نقلة نوعية وحضارية لا تقل عن دخول خدمة الكهرباء والهاتف إلى المجتمع، حيث أحدث دخولها تغييراً في مفاهيم مستخدميها وأساليب حياتهم (الفنتوخ ، ١٤٢١هـ : ص ٢٣٣) . وقد ارتفع معدل استخدام الإنترنت في المملكة العربية السعودية إلى ١٤٠% عام١٩٩٩م عما كان عليه في عام ١٩٩٨م حيث وصل عدد المشتركين إلى ١١٢٥٠٠مشترك (مجلة الرسالة الثقافية، ١٤٢٤ :ص٤٤) ، هذا عدا من يستخدمون البطاقات وخدمات الإنترنت المتاحة في المقاهي والشركات وبعض الإدارات الحكومية، وكانت شركة الاتصالات السعودية تتوقع أن يصل عدد مستخدمي الإنترنت عام ١٤٢٥هـ إلى ثلاثة ملايين مستخدم(مرآة الجامعة ، ١٤٢٥ :ص ١٣).

دخلت خدمة الإنترنت رسمياً إلى المملكة العربية السعودية على إثر قرار مجلس الوزراء رقم (٧/ب ١٠٩٩١) وتاريخ ١٤١٦/٧/٢٠هـ بتكوين لجنة مشتركة من الجهات المعنية للقيام بعمل الترتيبات والإعداد اللازم لإدخال خدمة الإنترنت إلى المملكة، وبناء على توصيات اللجنة صدر القرار رقم ١٦٣ وتاريخ ١٤١٧/١٠/٢٤هـ، حيث تضمن الموافقة على إدخال خدمة الإنترنت إلى المملكة العربية السعودية، وتضمن ذلك القرار ترتيبات البنى الخاصة بخدمة الإنترنت، وتم تكليف مدينة الملك عبد العزيز للعلوم والتقنية بإدارة خدمات الإنترنت المقدمة إلى الأفراد والجهات الحكومية.

وأنشأت مدينة الملك عبد العزيز للعلوم والتقنية وحدة خاصة لهذا الغرض تحت مسمى وحدة خدمات الإنترنت(محمد بن سعود ، ١٤٢٤:ص٧) ، وقامت بوضع اللوائح والضوابط المنظمة لعمل الإنترنت في المملكة، وإعداد الطاقات البشرية اللازمة لذلك، كما قامت المدينة بتقويم القطاع الخاص الراغب في تقديم خدمة الإنترنت

للمستخدمين، وكان ذلك على مسارين، المسار التقني والمسار المالي، ومن ثم تتأكد المدينة من مدى نظامية الجهة المتقدمة بالطلب (الزومان ، ١٤٢٣هـ :ص٢٠). وبالإضافة إلى ما سبق فإن بعض المراكز الطبية والبحثية مثل مستشفى الملك فيصل التخصصي بالرياض بدأ يستخدم الإنترنت للأغراض الطبية والبحثية منذ عام ١٩٩٤م. وقد كان هناك ما يفوق ٨٠٠٠ مستخدم سعودي يستخدم الإنترنت قبل دخولها رسميا إلى المملكة عن طريق دول أخرى.

ومع أن الخدمة كانت متاحة للشركات والمؤسسات منذ صدور توصيات اللجنة الخاصة بالترخيص للإنترنت إلا أن تقديم الخدمة للأفراد رسمياً لم يحصل إلا في٢٦/٨/ ١٤١٩هـ(الزومان ، ١٤٢٣هـ :ص٢٠) ، وهو وقت متأخر بعض الشيء مقارنة بدول أخرى كتونس والكويت ومصر ولبنان والمغرب وغيرها من الدول العربية، وتعد تونس أول دولة عربية تدخل خدمة الإنترنت، وذلك في عام ١٩٩١م، ثم الكويت عام ١٩٩٢م، ثم مصر عام ١٩٩٣م، ثم لبنان الذي أدخل الخدمة عام ١٩٩٣م إلى الجامعة الأمريكية وقدّم الإنترنت إلى الجمهور عام ١٩٩٦م ،ثم المغرب عام ١٩٩٤م، ثم قطر وسوريا عام ١٩٩٦م(مي السنو: ص١٤٦).

توفير خدمة الإنترنت في المملكة العربية السعودية:

وضح قرار مجلس الوزراء رقم ١٦٣ الصادر بتاريخ ١٤١٧/١٠/٢٤هـ، المتضمن الموافقة على إدخال خدمة الإنترنت إلى المملكة العربية السعودية، وضح كيفية تنظيم الإنترنت ومن المعني بها، لذا فلا يوجد جهة رسمية غير مدينة الملك عبد العزيز للعلوم والتقنية تقدم خدمات الإنترنت في المملكة سواء للأفراد أو الجامعات أو مزودي الخدمة أو الجهات الرسمية. بمعنى أنه لا يوجد إلا منفذ رسمي معتمد واحد فقط هو منفذ مدينة الملك عبد العزيز للعلوم والتقنية*.

والإجراء النظامي لطلب الخدمة هو تقديم طلب بذلك إلى مدينة الملك عبد العزيز للعلوم والتقنية بشكل رسمي، وعلى طالب الخدمة تعبئة النموذج المعد لذلك، و من ثم ترسل المدينة خطاباً إلى الجهات الرسمية المعنية للسؤال عن وضع المتقدم بالطلب من الناحية المالية والسلوكية وعدد المخالفات...إلخ، للنظر في إمكان تنفيذ طلبه أو رده. ولا تقدم المدينة الخدمة للأفراد أو الجهات الحكومية أو التجارية مباشرة بل يحصل الأفراد على الخدمة من خلال مزودي الخدمة الذين يحصلون بدورهم على الخدمة من المدينة ويتم تقديمها من قبلهم بشكل تجاري أو بشكل غير تجاري. وتعد جامعة الملك سعود أول جهة ترتبط بمركز تشغيل شبكة الإنترنت (الهاجري ، ١٤٢٥:ص٥٣). وتقدم مدينة الملك عبد العزيز خدمة الإنترنت للشركات المزودة للخدمة وللجامعات السعودية فقط مقابل مبالغ مالية ورسوم غير تجارية تصل في حدها الأدنى إلى ١٥٠ريالا وفي حدها الأعلى إلى ٤٥٠ريالا، باختلاف عدد الخطوط المطلوبة،

* مجلس الوزراء السعودي، قرار الموافقة على إدخال خدمة الإنترنت، رقم ١٦٣، تاريخ ١٤٢٥/١٠/٢٤هـ، ص ٣.

وتجري المدينة تخفيضا مع مرور الأيام على أسعار الخدمة(محمد بن سعود ، ١٤٢٤:ص٥٣) ، بالإضافة إلى ما تتقاضاه شركة الاتصالات من رسوم على المشتركين جراء الاتصال بالإنترنت من الهاتف الثابت،

المبحث الثاني : الاستخدامات الغير مشروعة لتقنية المعلومات متمثلة في الإنترنت ومنها :

- استخدام الإنترنت لتنفيذ العمليات الإرهابية
- التجسس الإلكتروني .
- الجرائم المنظمة .
- القرصنة على الإنترنت .
- غسيل الأموال .
- تهديدات التجارة الإلكترونية وبطاقات الائتمان .

الاستخدامات الغير مشروعة للإنترنت :-

ونقصد بالاستخدامات الغير مشروعة للإنترنت بأنها أي عمل غير قانوني تستخدم فيه شبكة الإنترنت كأداة أو موضوع للجريمة . ويمكن أن نعبر عنها بمصطلح جرائم الإنترنت .ومن هذه الاستخدامات الغير مشروعة ما يلي :

أولاً : الإرهاب

ظهر مفهوم الإرهاب في بلدان عديدة وتعني بها الاستخدام الغير قانوني للقوة أو العنف ضد الأفراد أو الممتلكات الخاصة أو العامة بهدف إرغام الحكومة أو المدنيين أو أي فئة أخرى على قبول هدف سياسي أو اجتماعي يخدم الإرهابيين . ومع ظهور الإنترنت أصبحت وسيلة للاتصال ممتازة لما يسمى بالجماعات الإرهابية وكذلك ظهور مصطلحات ومفردات ومفاهيم جديدة مثل الإرهاب الالكتروني .

ويحظى هذا النوع من الإرهاب بميزة خاصة عند الجماعات الإرهابية ، وذلك لان شبكة الإنترنت مجالها مفتوح وواسع ، ليس له حدود ، يتوسع في كل يوم ، ويمكنهم من موقعهم في أي بلد الوصول لأي مكان يريدونه دون أوراق أو تفتيش أو قيود . فكل ما يحتاجونه بعض المعلومات لاقتحام الحوائط الإلكترونية . كما أن تكاليف القيام بمثل هذه الهجمات الإلكترونية لا يتجاوز أكثر من حاسب آلي واتصال بالشبكة العنكبوتية .ومن الأمثلة على الإرهاب الالكتروني :

أحداث ١١سبتمبر في الولايات المتحدة الأمريكية . فلقد كشفت التحقيقات التي أجرتها السلطات الأمنية الأمريكية حول أحداث ١١سبتمبر ٢٠٠١م أن الإرهابيين الذين نفذوا تلك الهجمات استعانوا بالإنترنت لتمرير

رسائل ضمن صور رقمية أو ملفات موسيقية معدلة يصعب الكشف عن التعديلات التي أدخلت عليها وتعرف هـــذه التقنية باسم " ستيجانو جرافي " .

ونقلت " نيويورك تايمز " عن موظف سابق في وزارة الدفاع الفرنسية قوله حول التخطيط لتفجير الـــسفارة الأمريكية في باريس " كانت لدى هذه الجماعة الإرهابية تعليمات تقضي بتنفيذ كل اتصالاتها وتمرير رسائلها كافـــة من خلال نشر صور معدلة بشكل بسيط على الإنترنت " . وقامت فكرة " ستيجانو جرافي " على أحداث تعديلات طفيفة في صور أو ملفات موسيقية يصعب للعين أو الأذن أن تتعرف عليها (عبدالحميد ،٢٠٠٢:ص٨٦) .

ولا يمكن كشف هذه التغيرات إلا باستعمال برامج كمبيوتر خاصة والتي تحلل الاختلافات في الرسوم البيانية للمعلومات الرقمية التي تؤلف الرسم أو النغمة الموسيقية . وأشار المهتمون بهذه القضية إلى أن البرامج الخاصة بكشف هذه التقنية ليست كاملة بعد .

وعلى الرغم من ذلك فهي تكشف الكثير من تلك العمليات على الإنترنت ، وقال تنيت هوسميـــد المـــدير التنفيذي في شركة " ويب ستون تكنولوجيز " في نيويورك : يبدو أن الكثير من الصور التي نشرت في الآونة الأخيرة في عدد من المواقع على شبكة الإنترنت قد تضمنت تعديلات من هذا القبيل " . وقال " هوسميد " إنه وجد بعضا من هذه المواد المعدلة على موقع " أي باي " للمزادات الذي يتيح لأي شخص نشر صور من دون أية ضوابط . يذكر أن هوسميد يعمل مع القوات الجوية الأمريكية .

وفي الإطار ذاته قال الدكتور نيل " جونسون" خبير تقنية " ستيجانو جرافي " من جامعة جورج ماسون إنـــه صادف مؤخرا العديد من المادة الرقمية المعدلة خلال تحضيره لدراسة يعدها حول هذا الموضوع . وأوضح أنـــه لـــن يكشف عن هذه المواقع كي لا ينتبه الإرهابيون للموضوع ويقومون بنشر هذه المواد على مواقع أخرى . وقال " إميل للظن إن منفذي الهجمات الإرهابية في ١١ سبتمبر استعانوا بهذه التقنية لتمرير رسائلهم وربما تشير الرسائل المضبوطة حديثا إلى احتمال تحضيرهم لعمليات جديدة " . وتعود كلمة " ستيجانو جرافي " إلى أصول يونانية وهـــي تعـــني " الكتابة المخبأة " .

واعتبرت من أقدم الطرق لإخفاء الرسائل ، ولكن علماء الكمبيوتر لم ينتبهوا لأمرهم إلا مـــؤخرا . وقـــال جونسون إن الحلفاء أصيبوا بالريبة خلال الحرب العالمية الثانية من استعمال الألمان لهذه الأساليب إلى درجة منعـــت معها الولايات المتحدة من استلام الرسائل التي تحتوي على مرفقات . وفي السنوات الأخيرة وصلت هذه الأســـاليب إلى الإنترنت بدرجة كبيرة ، وذلك بواسطة برامج مجانية سهلة الاستعمال تسمح باختيار وســـائل تـــشفير لإخفـــاء الرسالة بشكل كبير وبهذه الطريقة فإن كشف وجود الرسالة ليس كافيا لأن محتواها لن يكون في متناول من كشفها

وقال جونسون : " في السنتين الماضيتين تضاعف عدد الأدوات التي تسمح بتطبيق تقنية " ستيجانو جرافي " إلى ١٤٠أداة والرقم قابل للارتفاع " .

وشبه بروس شناير مؤسس إحدى شركات أمن المعلومات والإنترنت تقنية ستيجانو جرافي " بإلقاء رسالة من شخص ما في مكان معين بانتظار أن يأتي إنسان آخر ويأخذها علما بأنه لا أحد يعرف معنى الرسالة إلا هذان الشخصان " . وأضاف " العنصر الأهم في هذا الإطار أن المرسل يستطيع إلغاء الرسالة من دون حاجة للإيصال بالمتلقي لا من خلال البريد الإلكتروني ولا رسائل قصيرة عبر الموبايل كل ما هنالك صورة منشورة على الشبكة أمام سائر الناس لا يعرف معناها ،لا شخص واحد يقوم بتنزيلها إلى جهازه ساعة ما يشاء " .

وأوضح هوسميد أن استخدام هذه الرسائل جزء من جرائم الإنترنت وإرهاب الفضاء الافتراضي وقال " طلبت من قيادة القوات الجوية إجراء دراسة حول هذه الأساليب لمعرفة أنواع الوسائل والأسلحة التي يستخدمها الإرهابيون والخطط التي يرسمونها ويريدون تنفيذها " . ووجه هوسميد " ما يزيد على مائة برنامج خاص بتقنية " ستيجانو جرافي " على الإنترنت وقال : " كانت المفاجأة كبيرة عندما أخبرتنا الشركات المصنعة لهذه البرامج أنه تم تنزيلها ما يزيد على مليون مرة " . ربما يكون هناك بعض مخترقي الشبكات المتهمين بالمسألة كما يمكن أن بعض مستخدمي الإنترنت العاديين استغلوا هذه البرامج لمجرد الاطلاع عليها ولكن في المقابل ليس هناك شك في أن هنالك إرهابيين استعانوا بهذه البرامج .

وأضافت : " من المثير أن يكون هناك ملايين الأشخاص يتواصلون مع بعضهم بعضا من دون علم الآخرين في حين أن الرسائل موجودة أمام الجميع " . وشرح هوسميد أن ما يقارب النصف في المائة من ملايين الصور التي فحصت من مواقع المزادات المختلفة احتوت على رسائل مخبأة . ولدهشته فإن تلك التي عثر عليها على مواقع " أي باي " كانت مشفرة وغير قابلة للقراءة وقال : " استعمل عدد من الصور مرات متكررة ، وهذا يشير إلى أن الذين قاموا بإخفاء الرسائل لم يكونوا من المحترفين لا يستعمل الصورة إلا مرة أو اثنتين على الأغلب " .

أما الدكتورة " جيسيكا فريدريك " من جامعة نيويورك فرأت أن ما يزيد من صعوبة هذه التقنية يكمن في اعتمادها على نوعيات الصور الأكثر استخداما عبر الإنترنت . وقالت " يصعب كشف عمليات التمويه في هذه النوعيات من الصور لأن الرسائل تبحث عن الأدلة الإحصائية التي تتغير في الصورة ولكن ملفات jpeg تحتوي على إحصائيات متغيرة أصلا " . وقامت فريدريك مؤخرا بتصميم برنامج لكشف هذه التقنية بناء على طلب من قيادة القوة الجوية التي تستعمله للبحث عن خطط هجومية مقبلة .

غير أن " نيلز بروفوس " من جامعة ميشيجن والذي طور بدوره برنامجا خاصا يكشف هذه التقنية وأوضح أنه لم يجد شيئا في مليوني صورة فحصها على موقع " أي باي " وفي تجربة متقدمة لتطوير برنامجه قال بروفوس "

استطعنا كشف رسائل صغيرة موجودة في بعض الصور " . ونفى " بروفوس " نية للكشف عن مصادر الصور قائلا : " أن الجهات أخذت على عاتقها تعقب الهجمات وإحباط الحيوية منها "(عبدالحميد ،٢٠٠٢:ص٩٥) .

في هذا الإطار فإن الدكتور " روبرت موريس " المستشار في منظمة الأمن القومي رفض الكلام عن هذا الموضوع قائلا : إن استعمال التقنيات الحديثة في العمليات الإرهابية شيء غريب مستغرب ، فالتطورات العصرية حتمت على الجماعة الإرهابية مجاراة العصر ولكن في الوقت الحالي لا يمكننا الكشف عما توصلنا إليه في هذا السياق.

ثانياً : التجسس الإلكتروني

" في عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي " (البداينه ، ١٩٨٨م) .

لقد تحولت وسائل التجسس من الطرق التقليدية إلى طرق حديثة استخدمت فيها التقنية الحديثة خاصة مع وجود الإنترنت ، وذلك بسبب ضعف الوسائل الأمنية المستخدمة في حماية الشبكات سواء كانت هيئات حكومية أو مؤسسات خاصة ، وذلك من خلال اختراق هذه الشبكات والمواقع من قبل الهكرز (hackers) ، فيقوم هؤلاء في العبث أو إتلاف محتويات تلك الشبكة ، هذا من جانب .

ومن جانب آخر وهو الأهم ، والذي يشكل الخطر الحقيقي على تلك المواقع ، فيكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخباراتية للحصول على أسرار ومعلومات الدولة ومن ثم إفشائها إلى دول أخرى معادية أو استغلالها لما يضر المصلحة الوطنية لتلك الدولة .

فلقد كشف النقاب عن شبكة دولية ضخمة للتجسس الإلكتروني تعمل تحت إشراف وكالة الأمن القومية الأمريكية ، بالتعاون مع أجهزة الاستخبارات والتجسس في كندا وبريطانيا واستراليا ونيوزيلاندا ، وقد أطلق عليها اسم (echelon) ، حيث عملت على رصد المكالمات الهاتفية والرسائل بكافة أنواعها ، وخصص هذا النظام للتعامل مع الأهداف غير العسكرية ، وبطريقة تجعله يعرض كميات هائلة جدا من الاتصالات والرسائل الإلكترونية عشوائيا باستخدام خاصية الكلمة المفتاح بواسطة الحاسبات المتعددة ، وحيث تم إنشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية ، ومنها :

- محطة رصد الأقمار الصناعية الواقعة في منطقة واي هو باي بجنوب نيوزيلاندا .
- محطة جيرالديتون الموجودة بأستراليا .
- المحطة الموجودة في منطقة موروينستو في مقاطعة كورنوول في بريطانيا المحطة الواقعة في الولايات المتحدة الأمريكية في منطقة شوجرجروف وتبعد ٢٥٠كيلو متر جنوب واشنطن .ولا يقتصر الرصد على

المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية الخاصة بالاتصالات الدولية بل يشمل الاتصالات التي تجري عبر أنظمة الاتصالات الأرضية أو الشبكات الإلكترونية ، أي أنه يرصد جميع الاتصالات التي تتم بأي وسيلة .ويعتبر الأفراد والمنظمات والحكومات الذين لا يستخدمون أنظمة الشفرة التأمينية أو أنظمة كودية لحماية شبكاتهم وأجهزتهم أهداف سهلة لشبكة التجسس هذه ، وإن كان هذا لا يعني بالضرورة أن الأهداف الأخرى التي تستخدم أنظمة الشفرة في مأمن تام من الغزوات الاستخباراتية لهذه الشبكة . ولا يقتصر التجسس على المعلومات العسكرية أو السياسية بل تعداه إلى المعلومات التجارية والاقتصادية بل وحتى الثقافية(عبد المطلب ، ٢٠٠١م : ٣٠- ٤٥) .

ففي تقرير نشرته وزارة التجارة والصناعة البريطانية أشارت إلى زيادة نسبة التجسس على الشركات من ٣٦% عام ١٩٩٤م إلى ٤٥% عام ١٩٩٩م . كما أظهر استفتاء أجري عام ١٩٩٦م لمسؤولي الأمن الصناعي في الشركات الأمريكية حصول الكثير من الدول وبشكل غير مشروع على معلومات سرية لأنشطة تجارية وصناعية في الولايات المتحدة الأمريكية (داود ، ١٤٢٠هـ : ٦٢) هذا وإن بعض الشركات العاملة في تقنية المعلومات تتجسس بعضها على بعض كما فعلت شركة real net works ، وانتل ومايكروسوفت وغيرها ، بالإضافة إلى شبكات ومواقع انترنت عديدة ، وذلك للحصول على معلومات تعطيها الأفضلية على منافستها في الأسواق(فادي ،٢٠٠٠: ص٢٨).

ومن الأساليب الحديثة للتجسس الإلكتروني أسلوب إخفاء المعلومات داخل المعلومات وهو أسلوب شائع وأن كان ليس بالأمر السهل ، ويتلخص هذا الأسلوب في لجوء المجرم إلى أخفاء المعلومة الحساسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهر ها وبذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبساً ، كما قد يلجأ إلى وسائل غير تقليدية للحصول على المعلومات السرية (داود ، ١٤٢٠هـ : ص ٦٧) .

وبعد الاعتداءات الأخيرة 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 خصيصاً 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 عمليات 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) .

التبعية العربية :

إذا نظرنا إلى حلول أمن المعلومات المطبقة في الأنظمة المعلوماتية والشبكات ، التي تعتمدها كثير من الحكومات العربية ، مثل جدران النار ، ستجدها جميعاً مصنعة خارجياً وستجد كذلك أن العشرات منها تعتمد على حلول أمنية مصنعة في إسرائيل ! وما يزيد الطين بلة .

فالاعتماد الكلي على تقنيات أجنبية للحفاظ على أمن معلوماتنا ، وتطبيقها على الشبكات الرسمية التابعة للدول العربية ، هو تعريض للأمن الوطني والقومي لهذه الدول للخطر ، ووضعه تحت سيطرة دول غربية ، بغض النظر عما إذا كانت هذه الدول عدوة أو صديقة ! الدول تتجسس على بعضها بغض النظر عن نوع العلاقة بينها ، وهذه حقيقة قائمة لا يمكن نفيها . وقد تطورت أساليب التجسس كما ذكرنا ، في هذا العصر ، وأصبحت الأسلحة المعتمدة هي الوسائل إلكترونية ، وخاصة عبر الإنترنت(عبد المطلب ، ٢٠٠٦م : ص٣١٠) .

ثالثاً : الجرائم المنظمة والمافيا عبر الإنترنت : .

ينبغي في البداية أن نفرق بين انواع المافيا ، المافيا الأساسية الأم التي تضرب بأصولها إلى المافيا الايطالية ، والتي تتواجد في الكثير من البلدان ، وبشكل أساسي في إيطاليا وأمريكا . والعصابات الإجرامية ، التي تشبه من الناحية التنظيمية ومن ناحيتي الوسائل والأهداف النوع الأول . والعصابات الصغيرة ، التي تضم الشباب والناشئين الذين قد يطلقون على أنفسهم أسم مافيا على اعتبار أنها قد تبث الرعب في صدور الآخرين . علماً بأن المافيا تمارس نشاطاتها على شبكة الإنترنت بأسلوبين هما :

١. استخدام الشبكة كأداة تعين في المراسلات ، وإدارة العمليات ، واصطياد الضحايا وتوسيع الأعمال وغسل الأموال .
٢. استحداث منظمات افتراضية تمارس أعمالا تخالف القوانين في بلدان متعددة ، وكذلك تجارة المخدرات حيث تدار في الخفاء .

فلقد ظهر ٢١٠ موقع يحتوي اسم نطاقها على كلمة مافيا ، وكذلك ٢٤ موقع يحتوي على كلمة مافيا ، هذا عدا المواقع الأخرى التي تحتوي على أسماء مثل كابوني وغيره من مشاهير المافيا ، في حين يوجد أربع مواقع للمافيا اليهودية (الجنيدي ، ١٩٩٩م : ٣٦) .

وتحاول المافيا عموما أن تقوم بنشاطاتها مستفيدة من وسائل الاتصال الفوري عبر الشبكة فقد تناقلت الأنباء على سبيل المثال قصة إحدى المنظمات الإجرامية التي تستخدم ICQ كشبكة اتصال بين عناصرها .

والجدير بالذكر أن المواقع المخصصة باستخدام الأعضاء فقط كثيرة ، وتطالعك فور دخولك صفحة تطالب بتسجيل اسم العضو وكلمة المرور الخاصة به ، وتسجل هذه المعلومات على مزودات خاصة بعد تشفيرها .

فلقد أصبحت الجريمة المنظمة ، وبسبب تقدم وسائل الاتصال والتكنولوجيا والعولمة ، غير محدودة لا بقيود الزمان ولا بقيود المكان ، وإنما أصبح انتشارها على نطاق واسع وكبير ، وأصبحت لا تحدها الحدود الجغرافية . (اليوسف ، ١٤٢٠هـ ، ص ٢٠١)

ولقد استغلت عصابات الجريمة المنظمة " الإمكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة " . (حبوش ، ١٤٢٠هـ : ٢٥٣)

رابعاً : القرصنة عبر الإنترنت

" ستطغى القرصنة عبر الإنترنت، على أنواع القرصنة التقليدية الأخرى " ، هذا ما أعلنته أحداث دراسات اتحاد برمجيات الأعمال (BSA (Business Software Alliance ، وهي منظمة تمولها كبرى شركات البرمجيات في العالم ، مثل مايكروسوفت ولوتس ، لمراقبة وتحليل سوق البرمجيات .

ولقد دقت النتيجة التي توصلت إليها المنظمة ، ناقوس الخطر ، في محيط الشركات التي تقوم دعائمها على إنتاج البرمجيات . فقد أشارت إلى أن قراصنة البرمجيات ، طوروا أساليب جديدة من القرصنة ، ليتجاوزوا العوائق التي تضعها شركات البرمجيات أمامهم ، الأمر الذي سيؤدي حتما ، إلى ازدياد معدلات القرصنة من جديد ، بعد أن عانت هذه الشركات من تقليص هذه المعدلات من خلال السنوات القليلة الماضية ، حيث هبطت نسبة قرصنة برمجيات الأعمال في العالم إلى ما دون خط الأربعين في المائة ، وهو أدنى مستوى له حتى الآن (فادي ،١٩٩٩م : ص٢٨)

تنظر الشركات الكبرى بحذر إلى نمو معدلات القرصنة عبر ويب . فقد أدى ارتفاع أعداد مستخدمي الإنترنت بمعدلات وصلت إلى ٧٠٠ في المائة سنويا وازدياد المعدل القياسي لنقل البيانات ، ليصل إلى ٥٦ كيلوبت في الثانية وانخفاض تكلفة الاتصال بإنترنت في معظم مناطق العالم ، بل ومجانيته في بعض المناطق إلى تسهيل وتوسع عمليات تبادل البرامج المقرصنة عبر الشبكة .وتنتشر الآن في الإنترنت عشرات المواقع التي تتضمن مختلف الأنواع من

البرامج ، كالألعاب ونظم التشغيل والبرامج الخدمية ، ويصطلح على تسمية هذه المواقع في مجتمع إنترنت السفلي بمواقع (Warez) ، وقد تجد في واحد منها برامج يقدر ثمنها في السوق بعشرات الآلاف من الدولارات . ويمكنك جلب أي من تلك البرامج مجانا ، أو قابل حفنة دولارات . بالنقر فقط على زر الماوس (فادي ،١٩٩٩م : ص٢٨) .

وقد بلغ مقدار الخسائر التي تسببت بها القرصنة العالمية في العام ١٩٩٨م ، حوالي ١١ مليار دولار أمريكي في مجال البرمجيات وحدها ، بدون النظر إلى قرصنة الموسيقى ، وذلك حسب الإحصائيات التي أجرتها منظمة اتحاد صناعة البرمجيات والمعلومات SIIA .

وتتسبب القرصنة في الدول المنتجة للمعلوماتية ، في خسارة أعداد كبيرة من العمال وظائفهم ، وخسارة الحكومات مليارات الدولارات ، من أموال الضرائب . وتقدر الإحصاءات في الولايات المتحدة الأمريكية ، مثلا أن ١٣٠٠٠٠شخص يفقدون وظائفهم سنويا ، كنتيجة مباشرة لعمليات القرصنة ، كما تحرم الخزينة الأمريكية من تحصيل ضرائب تصل إلى مليار دولار سنويا ، للسبب ذاته . وتتسبب القرصنة عبر الإنترنت بجزء كبير من هذه الخسائر ، وينمو هذا الجزء باستمرار مع نمو الإنترنت . ولا يبالي العاملون في مجال القرصنة عبر الإنترنت كثيرا بهذه الخسائر الكثيرة التي يتسببون بها ، بل يجد الكثير منهم التبريرات والحجج التي تضفي الشرعية على عملهم ، ويتبعون منطلقا يجعلهم يظهرون بمظهر أصحاب الحق.

ولم يتوقف الأمر عند هذا الحد ، ولم يكتف القراصنة بالسطو على عالم البرمجيات والفن ، بل بدؤوا أخيرا بطرق باب نوع جديد من التقنيات ، فقد ظهرت أخيرا مواقع عديدة تختص بترويج محاكيات (emulators) للأنظمة الحاسوبية المختلفة وقرصنة برامج هذه الأنظمة مثل محاكيات أنظمة Sega, Neogeo ,Play Station, Nintendo للألعاب وتحويل ألعابها التي يباع معظمها على شكل " كارتريدج " ، إلى صيغة رقمية وترويجها في الإنترنت . واستطاع كثير من المبرمجين قرصنة الدارات الإلكترونية التي تنتجها شركات ألعاب الفيديو التي لا تتوفر بصورة تجارية مثل Capcom وتحويلها إلى هيئة رقمية .

وعلى الرغم من أن معظم هذه الألعاب تعود إلى عدة سنوات مضت ، إلا أن الكثير منها ما زال يتمتع بشعبية واسعة ، ويعود على الشركات المنتجة بعوائد مادية جيدة ، الأمر الذي دفع هذه الشركات إلى رفع القضايا ضد المواقع التي تروج لمثل هذه المحاكيات والألعاب .

القرصنة عربيا :

قد يعود سبب أعراض معظم العالم وبشكل خاص في عالمنا العربي عن سن القوانين المضادة لقرصنة البرمجيات إلى أنها من الدول المستهلكة للبرمجيات ولا يحدث فيها سوى القليل من عمليات الإنتاج. ويسود الاعتقاد بأن سن مثل هذه القوانين يصب في مصلحة الدول المنتجة للبرمجيات، حيث إن التقليل من القرصنة يزيد فرص العمل

والضرائب التي تجنيها هذه الدول من الشركات المنتجة للبرمجيات. والأمثلة على ذلك عديدة .. فالصين ، مثلا تعرض عن سن قوانين صارمة لحظر القرصنة البرمجية ، لأن مثل هذه القوانين تصب بشكل مباشر في مصلحة الولايات المتحدة . وذهبت الأرجنتين إلى ما هو أبعد من ذلك حيث أصدرت إحدى المحاكم العليا الأرجنتينية ، قانونا يبيح قرصنة البرمجيات ويعلن شرعيتها(فادي ،١٩٩٩م : ص٣٢).

يمكن لذلك أن نتفهم وجهة نظر الدول النامية في هذا المجال ومن بينها بعض الدول العربية ، إذ إن سن هذه القوانين يعني في ظل ارتفاع أسعار البرمجيات ، مقارنة بدخل الفرد المتدني في معظم هذه الدول ، أن يبقى الفرد بعيدا عن التقنيات الحديثة التي لن يتمكن من الحصول عليها لارتفاع ثمنها . ويحول ذلك دون رفع مستوى الثقافة المعلوماتية بين الناس !لكن لعمليات القرصنة وجها آخر ، هو أنها تحول دون ترويج المبرمجين العرب منتجاتهم محليا ، لعلمهم أنها ستدخل في سوق القرصنة مباشرة ، بدون أن تعود عليهم ولو بجزء يسير من الجهود والأموال التي بذلوها خلال عمليات الإنتاج .

ولقد ظهر في السنوات الأخيرة شكل جديد من أشكال القرصنة العربية . فقد انتقلت حمى القرصنة العربية إلى شبكة الإنترنت ، وبدأنا نشهد أنماطا مختلفة منها في أرجاء ويب . حيث كانت بدايات القرصنة العربية في إنترنت عبر المواقع التي قدمت الموسيقى والأغاني المقرصنة ، على هيئة ملفات ، MP3 VAW وامتدادات شركة REALNETWORKS ، منتهكة الحقوق الفنية لأصحابها . وانتشر بعد ذلك عدد من المواقع العربية التي تقدم برامج مقرصنة كاملة عربية وعالمية . وظهرت أخيرا مواقع عربية تعرض نصوصا منسوخة من كتب ومجلات، أو من مواقع عربية أخرى (عبدالمطلب ، ٢٠٠٦: ص٣٨٠).

وتكمن المشكلة في أن الكثير من مستخدمي الإنترنت العربي ، لا يعلمون أن عمليات نسخ البرامج أو الموسيقى أو النصوص ونشرها في الإنترنت هي عملية غير قانونية ، بل إن معظم أصحاب المواقع الشخصية العربية ، يتسابقون في تقديم الأغاني والبرامج والنصوص المقرصنة لجذب الزوار إلى مواقعهم ولا توجد للأسف في معظم البلدان العربية قوانين حماية فكرية عامة ، ناهيك عن الحماية الفكرية في الإنترنت ، فلا يتمكن أصحاب الإبداعات الفكرية والفنية والبرمجية ، من الحفاظ على حقوقهم من عمليات القرصنة عبر الإنترنت . ويؤدي انتشار القرصنة عموما إلى تراجع الإنتاج الفكري والفني والبرمجي القليل أصلا في العالم العربي .

لكن يمكن على الرغم من ذلك أن يتخذ المتضررون من أصحاب الإبداعات الفكرية والفنية والبرمجية إجراءات ضد عمليات سرقة حقوقهم عبر الإنترنت ، حيث تقدم الكثير من المواقع والمنظمات عددا من الأساليب الكفيلة بمنع هذه السرقات ويمكن أن يلجأ المتضررون إلى هذه الأساليب مؤقتا إلى أن تسن البلدان العربية القوانين الكفيلة بحفظ حقوق المبدعين .

وجدير بالذكر أن وضع ارتباطات أو وصلات تشعبيه في الموقع ، إلى برامج أو ملفات مقرصنة في مواقع أخرى ، لا يعتبر ممنوعا قانونيا في الولايات المتحدة الأمريكية ، التي يوجد فيها معظم مواقع إنترنت في العالم . وأدى هذا التناقض في القوانين ، إلى حدوث شبه اتفاق بين القراصنة في العالم بحيث يبني الموقع الرئيس في الولايات المتحدة الأمريكية ، التي تحتوي على أكبر عدد من مستخدمي إنترنت في العالم ، وتوضع البرامج والملفات المقرصنة على مزودات في مناطق أخرى من العالم ، كالصين مثلا ، ثم توضع وصلات مباشرة إلى تلك البرامج في الموقع الأمريكي .

ويتقاسم القراصنة في طرفي العالم الفوائد حسب اتفاق بينهم . ويتطلب لذلك متابعة دائمة لمثل هذه المواقع وربما احتاج الأمر إلى إجراء حملات مضادة كالتي تجريها شركة مايكرو سوف حيث تقدم الجوائز لكل من يدل على جهات تقرصن منتجاتها(عبدالمطلب ، ٢٠٠٦: ص٣٨٢) .

خامساً : غسيل الأموال عبر الإنترنت

رغم أن مشكلة غسيل الأموال أصبحت من المشاكل الرئيسة التي تعاني منها الحكومات إلا أن هذا النوع من الجرائم يبدو وكأنه جريمة بدون ضحايا، ويأتي لدى الكثيرين في منزلة متأخرة بعد عمليات السطو السرقة وغيرها من الجرائم أو الجنح.

ولقد نشأ مصطلح " غسيل الأموال " العام ١٩٣١ لدى محاكمة ألفونس كابوني، الشهير باسم كابوني . يصف هذا المصطلح واحدا من أهم الأطوار ، التي تمر بها الأموال التي تحصلها عصابات المافيا ، والتي تتأتى أساسا من أعمال الابتزاز والسرقة ، والدعارة ، والقمار ، علاوة على تهريب المخدرات . وتحتاج هذه العصابات لذلك ، إلى إبراز مصدر قانوني لهذه الأموال الطائلة .

ويعتبر القيام بأعمال مشروعة ثم خلط الأموال القذرة مع تلك التي تجنيها الأعمال بشكل قانوني ، واحدا من الطرق التي كانت المافيا قادرة على اتباعها لفترة طويلة . ويوضح موقع http://www.laundryman.u--net.com/page6mleth.html عددا من الطرق المتبعة في غسيل الأموال . والطريف في الأمر أن آل كابوني حوكم حينها لتهربه من دفع الضرائب وليس للأعمال غير المشروعة التي كان يشتبه أنه يديرها (عبدالمطلب ، ١٩٩٩) .

ولقد عرف الاتحاد الأوروبي . في مارس /آذار ١٩٩٠ ، مصطلح غسل الأموال ، بأنه " تحويل أو نقل الممتلكات (The conversion or transfer of property) ، مع العلم بمصادرها الإجرامية الخطيرة لأغراض التستر وإخفاء الأصل غير القانوني لها ، أو مساعدة أي شخص يرتكب مثل هذه الأعمال " .

ويمكن ملاحظة العديد من الاتجاهات العامة المتعلقة بالخصائص الحديثة لغسل الأموال وأهمها :

- الطبيعة العالمية لظاهرة غسل الأموال ، والتي تتجاوز الحدود الجغرافية القومية ، إذ يميل غالسو الأموال إلى نقل نشاطاتهم إلى أماكن ليس فيها إجراءات مضادة لغسل الأموال ، أو الإجراءات فيها ضعيفة .
- تم رصد طرق جديدة لغسل الأموال عبر الإنترنت ، بدأت تعمل منذ أكثر من عامين . فالاستخدام المتنوع للإنترنت كالمقامرة ، والنشاطات المصرفية المقترنة بها ، علاوة على العمليات المصرفية عبر الشبكة ، يوفر آلية يمكن استخدامها في الحركة السريعة للنقود الإلكترونية ، بالمقارنة مع الاستخدام التقليدي للنقود الورقية .
- الاتجاه المتنامي لدى غاسلي الأموال ، للتحرك بعيدا عن البنوك نحو قطاع المؤسسات المالية غير المصرفية كسوق صرف العملات (Currency exchange houses) ، وسوق الحوالات المالية . ولعل اللافت للانتباه خاصة ، هو الاتجاه نحو القطاعات غير المالية ، من تجارة البضائع الثمينة ، كالمجوهرات ، والسيارات الفخمة إلى المؤسسات الخدمية (كمكاتب المحاماة والمحاسبة القانونية) ، والوكالات العقارية وغيرها .
- الازدياد المستمر في كمية الأموال القذرة . التي يجري تهريبها خارج بلدان عديدة ، ليجري توظيفها في الهيكل الاقتصادي المالي في بلدان أخرى .

وتشير أصابع الاتهام ، لدى الجهات الحكومية الأمريكية والأوروبية إلى نوادي الإنترنت للقمار ، والتي اصطلح على تسميتها الكازينوهات الافتراضية Virtual casinos ، إذ إن معظم هذه النوادي التي تعلن عبر الإنترنت تقول إنها موجودة فيزيائيا في حوض الكاريبي Caribbean Basin . وعلى الرغم من صحة هذا الادعاء في العديد من الحالات فهو كاذب في الكثير من الحالات الأخرى (جنيدي ، ١٩٩٩:ص٣٧).

ولقد تابعت شرطة FBI في نيويورك مثلا ، مواقع الإنترنت المنغمسة في الخداع وغسل الأموال ، وركزت تحقيقاتها على عمليات المقامرة ومديريها . وتبين أن مواقع الإنترنت هذه موجودة في الواقع في كاراكاو ، وجزر الانتيل وجزيرة انتيجوا ، وجمهورية الدومينيكان . وبعد خمسة أشهر من العمل المكثف والشائك ، صدرت اتهامات وجرت اعتقالات بحق العديد من مديري تلك المواقع .

وفي العلاقة بين الإنترنت وغسل الأموال تبين ، " أنها سريعة ، ومغفلة التوقيع ، ولا توقفها الحدود الجغرافية"! هكذا وصف أحد الباحثين حركة الأموال عبر الشبكة . والجودة ذاتها التي تجعل من إنترنت والبطاقات الذكية وغيرها من التقنيات الحديثة ، محل شعبية وترحيب الجمهور ، تجعلها أيضا موضوع ترحيب وجاذبية للمجرمين الذين يتوقون لغسل أموالهم بهدوء وسرعة معا ! يقدر المتخصصون أن هناك ٤٠٠ مليار دولار ، يتم تنظيفها سنويا ، في مختلف أنحاء العالم بطرق مختلفة ، وإذا كان المجرمون الكنديون مثلا يقومون بتهريب حقائب مليئة بكمبيالات بقيمة ١٠٠٠ دولار إلى بلدان ذات قوانين مصرفية متهاونة فإن ما يدعى اليوم النقود الإلكترونية Electronic-cash or E-money يمثل وسيلة سهلة النقل من مكان لآخر بمجرد استخدام الكمبيوتر .

وتشبه البطاقات الذكية (smart cards) إلى حد بعيد بطاقات البنوك بيد أنها تتميز باحتوائها على مايكرو معالج. وقد شاع استخدام هذه البطاقات في أوروبا واستراليا وكثير من البلدان الأخرى ، لكنها محدودة الاستخدام في أمريكا وكندا . ويمكن للمرء أن " يعبئ " هذه البطاقة بمكافئ إلكتروني من النقود ، عن طريق أجهزة الصرف البنكي أو عبر أجهزة الهاتف المزود بهذا النظام ، ومن ثم يستخدمها للدفع مقابل بضائع أو تحويلها إلى حساب بنكي(جنيدي ، ١٩٩٩:ص٣٨).

إحدى تقنيات البطاقة الذكية هي تقنية موندكس Mondex الشهيرة ويقول ايف دوجاي الخبير الدولي في تعقب العمليات الإجرامية الإلكترونية ، ضمن مؤتمر مخصص لغسل الأموال : " إن هذه التقنية تسمح للمستخدمين بتحويل الأموال عبر جهاز مودم ، أو عبر إنترنت ، مع ضمان تشفيره وأمن العملية ، وإذا تم هذا بالفعل ، فإنه يمكن القول أننا قد نواجه مشكلة تتعلق بغسل الأموال . وأنا لا أقول إننا في مشكلة لكننا قد نقع فيها " . وأضاف : " يجب الاعتراف بأن غاسلي الأموال أذكياء وبارعون ، وهم يتطلعون باستمرار ، إلى ابتكار طرق جديدة لخداع السلطات ونحن نحاول أن نفكر كيف سيقومون بذلك وأن نهيئ أنفسنا بناء على ذلك ، لكن من المؤكد أن الاحتمال قائم بأن تتم عمليات غسل أموال بسرعة أكبر وربما بدون أن تترك آثارا خلفها " (دوجاي ،١٩٩٥).

ولا يوجد حاليا ما يمنع أي شخص من استخدام إنترنت لإنشاء بنك افتراضي أو متجر لصرافة العملات ، أو شركات زائفة في بلدان بعيدة عن الضرائب ، تغض فيها الحكومات الطرف عن عمليات غسل الأموال . وعلى هذا ستعاني عمليات غسل الأموال عبر الإنترنت من بعض الصعوبات ، في بلدان بنوكها منضبطة ومتعاونة مع الشرطة وتقوم بإجراءات للتحقق من أن عملاءها لا يودعون أموالا قذرة لطمس نشاطاتهم غير القانونية . لكن وبما إنه ثمة مؤسسات مالية لا يمكن ضبطها بطريقة البنوك كمؤسسات الصرافة مثلا ، فإنه من الممكن في النتيجة ملاحظة كمية كبيرة من الأموال تنتقل عبر الشبكة لتصب في النهاية في بنك موجود في أحد بلدان " التهرب الضريبي " إن الأخطار المحتملة من جراء ذلك كبيرة حتما ، لأن تعاملات غاسلي الأموال مع البنوك عبر الإنترنت ، تتصف بالسرية.

المبحث الثالث : استراتيجة الإجراءات الأمنية المقترح اتخاذها للوقاية من الاستخدامات الغير مشروعة للتقنية ومنها :

- الأمن الإداري والمؤسسي .
- أمن الأفراد .
- أمن المنشآت .
- أمن الاتصال الإلكتروني .
- أمن الأجهزة والبرامج .
- أمن التشغيل .
- التخطيط المفاجئ .

إستراتيجية أمن المعلومات

هي مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشاة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها ، وتهدف إلى تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الكمبيوتر والشبكات وكذلك حماية المعلومات بكافة أشكالها ، وفي مراحل إدخالها ومعالجتها وتخزينها ونقلها وإعادة استرجاعها . كما تهدف إلى تحديد الإلكترونية التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر ،وبيان الإجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها.

إعداد استراتيجية أمن المعلومات:

عند إعداد استراتيجية أمن المعلومات لا بد أن يساهم في إعدادها وتفهمها وتقبلها وتنفيذها مختلف المستويات الوظيفية في المنشأة الواحدة إضافة إلى حاجتها إلى التعاون والدعم الكامل من الجميع ، من هنا فأن المعنيين بأعداد سياسة أمن المعلومات يتوزعون إلى مراتب وجهات عديدة داخل المنشأة ، لكن بوجه عام تشمل مسؤولية أمن المعلومات مديري الشبكات وموظفي وحدة الكمبيوتر ومديري الوحدات المختلفة في النشأة كوحدة الإعمال والتسويق والبحث وغيرها وتشمل أيضاً فريق الاستجابة للحوادث والأعطال وممثلي مجموعات المستخدمين ومستويات الإدارة العليا إلى جانب الإدارة القانونية (الجنيدي ، ١٩٩٩م : ٥٢).

فاعلية استراتيجية أمن المعلومات :

من حيث فاعلية الاستخدام : لكي توصف استراتيجية أمن المعلومات بأنها فاعلة يتعين أن تعمم بشكل شامل على كافة قطاعات الإدارة وأن تكون مقبولة واقعية من الشخص المناط به تنفيذها إلى جانب توفر الأدلة التوجيهية

والإرشادية لضمان استمرار التنفيذ وعدم التقاعس فيه والتنفيذ هنا هو الاستخدام الفعلي لأدوات الحماية التقنية من جهة والتطبيق الفعلي لقواعد العمل والتعامل مع البيانات ونظمها من جهة أخرى ، ولا تحقق الاستراتيجية نجاحاً أن كان ثمة غموض فيها لهذا لا بد أن تكون واضحة دقيقة في محتواها ومفهومة لدى كافة المعنيين .

أما من حيث المحتوى: فإن أساس أمن المعلومات تمتد إلى العديد من المناحي المتصلة بنظم المعلومات وإدارتها والتعامل معها إضافة إلى المسائل المتعلقة بالمعلومات ذاتها وتعامل الغير مع معلومات المنشأة ، من هنا تشمل الاستراتيجية سياسة واضحة بشأن اقتناء وشراء الأجهزة التقنية وأدواتها ، والبرمجيات ، والحلول المتصلة بالعمل ، والحلول المتعلقة بإدارة النظام .كما تشمل استراتيجية الخصوصية المعلوماتية ، وهي التي تحدد مراتب المعلومات وقيمتها ووصفها من حيث السرية كما تبين الاستثناءات التي تعتمدها الإستراتيجية على حق الخصوصية لموظفي المنشأة مع مبررات هذه الاستثناءات ، كرقابة البريد الإلكتروني ، أو رقابة الدخول إلى المنشأة ، أو رقابة الوصول إلى ملفات المستخدمين بالمنشأة . لذا يجب أن تنطلق أساسي أمن المعلومات من تحديد المخاطر ، أغراض الحماية ، ومواطن الحماية ، وأنماط الحماية اللازمة ، وإجراءات الوقاية من المخاطر ، وتتلخص المنطلقات والأسس التي تبنى عليها استراتيجية أمن المعلومات القائمة على الاحتياجات المتباينة لكل منشأة من الإجابة على تساؤلات ثلاثة رئيسية وهي :- ١) ماذا أريد أن أحمي ؟ ٢) من ماذا أحمي المعلومات ؟ ٣) كيف أحمي المعلومات ؟(أبو الحجاج ، ١٩٩٨م : ٢٥)

الإجراءات الأمنية التي يقترح اتخاذها :

يتكون أمن أنظمة معالجة البيانات إلكترونيا من عدة عناصر أساسية: الأمن الإداري والمؤسسي، أمن الأفراد، أمن المنشآت، أمن الاتصالات الإلكترونية، أمن البرامج والأجهزة، أمن العمليات والتخطيط للطوارئ.

الأمن الإداري والمؤسسي:

يشمل الأمن الإداري تطوير سياسة أمنية شاملة وصياغة إجراءات لتنفيذ هذه السياسة وإن كانت الخطط العملية لضمان الأمن الإداري تتفاوت وتختلف بناء على حجم وطبيعة العمل الذي تؤديه المنظمة إلا أن أدنى المستويات من المتطلبات يجب أن يشتمل على الآتي :

١. تطوير الإجراءات التي تضمن تحديد المخاطر .
٢. تحديد وتعريف واجبات الفرد الأمنية وتقسيم المسؤوليات بصورة مناسبة .
٣. تحديد أماكن يحظر دخول العامة أيضا فيها.
٤. صياغة اتباع إجراءات تفويضية .

٥. تحديد الوحدات التابعة الخارجية.

٦. إعداد خطة للطوارئ.

ويأتي في المرتبة الثانية بعد ذلك أهمية ، ضرورة إيجاد التنظيم الإداري الفاعل لتنفيذ هذه السياسة والإجراءات إذ إن وعي وإدراك كبار الإداريين بمتطلبات أمن أنظمة معالجة البيانات الالكترونية وإدراكهم لأهمية إقامة علاقة عمل وثيقة بين نظم الإدارة الآلية والمجموعة المكلفة بضمان الأمن الشامل له اعتبار خاص مؤسس للأمن الإداري المطلوب (عبدالمطلب ،٢٠٠٦: ص ٤٠٦) .

أمن الأفراد :

يشمل أمن الأفراد متطلبات أمنية محددة في مواصفات الوظيفة والتأكيد على استيفاء المتقدمين لهذه المتطلبات وضمان تنمية وتعزيز الدافع الأمني لديهم وتوفير التدريب المناسب لبلوغ ذلك . كما تشمل أيضا وسيلة الإشراف على والتحكم في مصادر النظام عبر اتباع إجراءات مناسبة للأفراد وتحديد صلاحياتهم .

كما تتطلب بالإضافة إلى ذلك الاهتمام والتركيز على إجراءات استخدام واستئجار الأفراد وفصلهم عن الخدمة . لذلك فإن موظفي الخدمة الخارجية أو موظفي المساعدة والدعم مثل عمال الصيانة أو النظافة أو المبرمجين المتعاقد معهم والذين يخضعون للإشراف فيما يتعلق بدخولهم إلى المناطق الممنوعة يجب أن يخضعوا أيضا مثل الموظفين الدائمين للإجراءات الأمنية التي تختص بالأفراد (عبدالحميد ،٢٠٠٦:ص٤٠٧).

أمن المنشآت :

يجب أن تخضع كل تجهيزات أنظمة معالجة البيانات الالكترونية إلى نظام لتوفير الحماية يتساوى ويعادل حساسية البيانات التي تتم معالجتها والخدمات التي يتم تقديمها . لذلك يجب أن تأخذ بعين الاعتبار المتطلبات التالية عندما يتعلق الأمر باختيار إجراءات أمن المنشآت :

١. تخطيط الموقع ، مثل الموقع والتصميم ، إنشاء المباني ، نظام التدفئة ، إضاءة السور الخارجي والأسوار الحاجبة.

٢. التحكم في الدخول إلى المناطق الممنوعة (مثل الحدود الأمنية ، " مراقبة والتحكم في دخول الزوار ، مراقبة المفاتيح وشارات الدخول ، أفراد الحراسة وأجهزة الإنذار) .

٣. الحماية ضد الأضرار المادية (الحريق ، الفيضانات ، الانفجارات ، الزلازل ، الهجوم على المباني) .

٤. الحماية ضد مخاطر انقطاع مصادر الطاقة والخدمات البينية الأخرى ، (مثل أنظمة تبريد الهواء ، ونظام تبريد المياه ، ومراقبة مصادر الطاقة ، وضمان إمداد متواصل بمصادر الطاقة والحماية من الغبار والأتربة) .

٥. حماية وسائط حفظ بيانات أنظمة معالجة البيانات إلكترونيا ومصادر إمدادها وتوفرها (مثل التصرف في المخلفات ، حاويات الحفظ ، النقل ، إجراءات التبريد ، والتعبئة) .

إن العلاقة الوثيقة بين الجوانب البيئية والجوانب التي تختص بالبرامج والمنشآت في أمن أنظمة معالجة البيانات الإلكترونية يجعل التنسيق بين نظام الكمبيوتر وموظفي الأمن التقليديين أمرا أساسيا خاصا في مراحل التخطيط وتصميم النظم الجديدة والمنشآت(عبدالمطلب ،٢٠٠٦: ص ٤٠٨).

أمن الاتصالات الإلكترونية:

تعتبر الاتصالات مكونا أساسيا في جميع الأنظمة الآلية بمختلف أنواعها إذ إن استخدامها يزيد من جغرافية الحدود الأمنية فيما يتعلق بتوفر مجموعة معقدة من الخدمات ، وكما هو الحال فيما يتعلق بتنوع أوجه الاتصالات ينطبق الأمر أيضا على تقاطع الاتصالات بين الخطوط أو إرسال المعلومات وتوجيهها إلى جهات غير معنية ، ورصد الإشعاع الكهرومغناطيسي من الأجهزة – فهنالك بعض الإجراءات المضادة لمواجهة التهديدات الإلكترونية والتهديدات التي تواجه الاتصالات تشمل المراقبة والفحص الإلكتروني وفحص الثغرات وتصميم محطات اتصالات بمواصفات خاصة .

إلا أن صعوبة وتعقد أنظمة الاتصال يحتم التعامل مع كل حالة بصورة فردية . ونسبة لزيادة الاعتماد على الاتصالات ازدادت أيضا احتمالية فقدان المقدرة على تقديم خدمات آلية بفعل فشل أو عجز في أنظمة الاتصالات (عبدالمطلب ،٢٠٠٦: ص ٤٠٩).

أمن الأجهزة والبرامج :

يتعلق أمن البرامج بخصائص حماية الجهاز التي تم استخدامها في مميزات معدات معالجة البيانات إضافة إلى إجراءات الدعم والتحكم اللازمة لشمولية وتكامل هذه الخصائص . ويلاحظ أنه يمكن تقسيم خصائص أنظمة أمن الكمبيوتر سواء أكانت منفذة في المكونات الصلبة أو البرامج إلى خمس فئات :

١. آليات التعريف ، لتحديد هوية المستخدمين المصرح لهم .

٢. خصائص العزل ، التي تؤكد بأن مستخدمي النظام محظورون من الوصول للبرامج والبيانات التي لا يستحقونها .

٣. إجراءات المراقبة والكشف ، التي تساعد في الكشف عن انتهاكات الأمن المطبقة عادة عن طريق البرامج .

٤. أساليب الاستجابة ، لمواجهة أذى انتهاكات الأمن مثل المكونات الزائدة والدوائر ومنطق تصحيح الخطأ .

٥. خصائص تحكم الوصول ، التي توفر الموارد لنظام المشاركة المختار ، بإزالة أو إبطال إجراءات العزل للحالات المصرح بها (عبدالمطلب ،٢٠٠٦: ص ٤١٠) .

أمن التشغيل :

يرتبط أمن التشغيل بالسياسة والمنتجات الضرورية التي تؤكد بأن القدرة التشغيلية متاحة وأن الأوضاع الأمنية من خلال البيئة الإلكترونية مقبولة بحيث لا يكون في مقدور أي فرد تخريب التحكم في النظام . والاعتبارات المتصلة بإنشاء والمحافظة على نظام أمن ملائم هي باختصار كما يلي :

١. تعريف هوية موجودات الـ (EDP البيانات ، البرامج ، المكونات الصلبة ، وسائط تخزين البيانات ، الخدمات والتجهيزات) التي تتطلب الحماية .

٢. بيان قيمة كل الموجودات .

٣. تعريف هوية الحظر الأمني المرتبط بكل الموجودات .

٤. تحديد قابلية سقوط نظام الـ EDP في هذا الأخطار .

٥. تقييم خطر التعرض المرتبط بكل الموجودات (احتمالية عدد مرات الحدوث المضاعفة بتأثير الحدوث) .

٦. اختيار وتطبيق المقاييس العلمية الأمنية .

٧. تدقيق وتحسين برنامج أمن EDP بصورة مستمرة .

ومن المتعارف عليه أن الأمن المطلق هدف غير واقعي وأن السياسة الأمنية المثلى هي التي يكون فيها تطبيق الآليات الواقية قد تمت موازنته مقابل تخفيض الخطر المتوقع (عبدالمطلب ،٢٠٠٦: ص ٤١١) .

التوصيات والنتائج :

وهذه بعض التوصيات حول الاستخدامات غير المشروعة عبر شبكة الإنترنت وتقديم بعض الحلول والمقترحات التي من شأنها أن تساعد في التقليل من خطر هذه الاستخدامات والعمل على مواجهة هذا التهديد والوقاية منه ، وستكون على المستوى العربي من جهة ، والمستوى العالمي من الجهة الأخرى .

توصيات على المستوى العربي وهي :

- العمل على وضع استراتيجية واضحة المعالم من قبل المختصين والباحثين ، وتهدف إلى الاستخدام الأمثل والآمن للإنترنت .
- زيادة التعاون في مجال التبادل التقني والفني والقضائي بين الجهات المختصة .
- تفعيل دور المؤسسات التعليمية والجهات التأهيلية في مكافحة الجريمة الإلكترونية والعمل على إضافة برامج جديدة من شأنها أن تقلل من هذه الجرائم .
- فرض إجراءات أمنية إلزامية في القطاعات الحكومية الإلكترونية ، تمنع من التسلل إليها واستخدامها بأي طريقة لمصلحة الجريمة .
- العمل على تحسين النظم التشريعية وتحديثها ، وتقديم نصوص صريحة وواضحة حول جرائم الإنترنت ومساسها بأمن الدولة من الداخل أو الخارج .
- وضع قانون شامل للإنترنت بحيث يبين جرائم الإنترنت ويجرمها ويعاقب مستخدميها ، بالإضافة إلى أنه يعطي الحق لبعض الجهات المختصة أن يقوم بتفتيشها وضبط معلماتها ومراقبتها وفقا للشروط الخاصة بهذه الإجراءات .
- إعادة تأهيل الجهات ذات الصلة القانونية من قضاة ومحققين وخبراء من خلال تدريبهم على كيفية التعامل مع الجرائم الإلكترونية وكيفية الكشف عنها واستنباط الأدلة في إثباتها ، وليتناسب هذا التأهيل مع التطور السريع في عالم الإنترنت . حيث إن هذه الجرائم تختلف كثيرا عن الجرائم التقليدية .
- العمل على مراقبة هذه الشبكة وحجب بعض المواقع التي من شأنها أن تبث مثل هذه الجرائم وكذلك حجب المواقع التي لا تتناسب مع مجتمعاتنا المحافظة ، وتتولى هذه المهمة جهات خاصة من قبل الدولة .
- تشكيل لجنة مختصة تشرف على الإنترنت ، من شأنها تطويره وتقديم ما هو أفضل في هذا المجال . وكذلك يكون من شأنها أن تعد التقارير الإحصائية واستقبال المقترحات ومتابعة الشكاوى

وتقديمها للجهات المختصة ، بالإضافة إلى تحديد بعض المفاهيم والمصطلحات التي تسهل عملية كشف الجرائم وتجنبها .

- العمل على زيادة الوعي لدى مستخدمي الإنترنت بعقد دورات تدريبية أو بيان أخطار الجريمة الإلكترونية ومعاقبة فاعليها .

توصيات على المستوى العالمي :

- التنسيق والتعاون وتبادل المعلومات والخبرات بين الأجهزة ذات الصلة بمكافحة الجريمة في كل أنحاء العالم .
- إعادة تأهيل وتدريب الدول التي مازالت متخلفة في مجالات تقنية المعلومات ومكافحة الجريمة الإلكترونية وذلك بالاستفادة من آخر ما توصلت إليه الدول المتقدمة في هذا المجال .
- دراسة مبادئ وأهداف وفكر الجماعات الإرهابية وخاصة التي تستخدم الإنترنت وسيلة لتنفيذ الإرهاب وذلك للتحريض منهم وتبين أهدافهم للعالم على وجه الحقيقة لتجنبهم والابتعاد عنهم .
- إنشاء منظمة عالمية تشارك فيها جميع الدول ، تكون بمثابة الضابط لشبكة الإنترنت في العالم ومن شأن هذه المنظمة تقديم الإحصاءات والاقتراحات والشكاوى إلى الجهات المختصة لمتابعتها وكذلك دراسة كل ما هو جديد في شبكة الإنترنت للتقليل من الجرائم الإلكترونية .
- البحث مع الجماعات الإرهابية ودراسة دوافعهم والتفاوض معهم لإيجاد الحلول السلمية البديلة عن الجرائم الإرهابية .

الخاتمة :

إن شبكة الإنترنت تتطور بسرعة هائلة لتدخل في كل المجالات دون قيود أو حدود ، لتعطي كما هائلا من المعلومات في شتى الميادين (علمية ، اجتماعية ، اقتصادية ، عسكرية ...) ، وحيث إن استخدامها متاح للجميع فقد أصبحت أيضا بعد أن كانت وما زالت وسيلة معلوماتية مميزة ، أصبحت وسيلة أو أداة لتنفيذ ما يعرف بالجريمة الإلكترونية وما تحمله الكلمة من معنى سواء كان ذلك عن طريق الإرهاب أو التجسس الإلكتروني أو القرصنة وغيرها .

وبالتالي أصبح من الضروري وضع حلول وقوانين وأنظمة واستراتيجيات من شأنها أن تحد من هذا الاستخدام الغير مشروع لهذه الشبكة المعلوماتية على المستويين العربي والعالمي.

المراجع :

أولا – المراجع العربية :

- أبو الحجاج ، أسامة . دليلك الشخصي إلى عالم الإنترنت . القاهرة : نهضة مصر .
- الألف ، محمد . مكافحة جرائم الإرهاب عبر الإنترنت ، ١٩٩٨م.
- البداينة ، ذياب . جرائم الحاسب والإنترنت ، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها ، أكاديمية نايف العربية للعلوم الأمنية ، تونس ، ١٤٢٠هـ (٩٣-١٢٤) .
- البداينة ، ذياب . (١٩٨٨م) . الأمن الوطني في عصر المعلومات . الجزيرة ، ٩٤٢١ .
- البداينة ، ذياب. التطبيقات الاجتماعية للإنترنت ، ورقة قدمت في الدورة التدريبية حول شبكة الإنترنت من منظور أمني ، أكاديمية نايف العربية للعلوم الأمنية ، ١٩٩٩م بيروت ، لبنان .
- الجلاف ، عيسى سالم . ثقافة الإنترنت وأثرها في الشباب . الشارقة ، ٢٠٠٦م.
- الجنيدي ، ماهر أ . النصر للأقوى والأذكى والقذر ، مجلة إنترنت العالم العربي ، نوفمبر، ١٩٩٩م ٣٦ .
- الجنيدي ، ماهر ب. رائحة الماريجوانا تنبعث من أوكار إنترنت ، مجلة انترنت العالم العربي ، نوفمبر ١٩٩٩م ، ٣٩-٤٠ .
- خالد ، محمد بن سعود بن . الإنترنت في المملكة العربية السعودية، الانتشار والاستخدامات،١٤٢٤هـ ص ٤٧ ٤٨.
- داود ، حسن طاهر. جرائم نظم المعلومات . الرياض : أكاديمية نايف العربية للعلوم الأمنية ، ١٤٢٠هـ .
- داود ، حسن طاهر . الحاسب وأمن المعلومات . الرياض : الإدارة العامة ، ١٤٢١هـ .
- الدناني ، عبد الملك . الوظيفة الإعلامية لشبكة الإنترنت، دراسة لمعرفة استخداماتها في مجال الإعلام، ط١، بيروت، دار الراتب الجامعية، ١٤٢٠هـ، ص٤٣.
- روجرز ، إفريت م. "الأفكار المستحدثة وكيف تنتشر"، ترجمة سامي ناشد، (ب ط) القاهرة، عالم الكتب، ص٨٤.
- الزومان ،عبد العزيز . شبكة الإنترنت، مجلة العلوم والتقنية، السنة ١٦، العدد ٦٤، شوال ١٤٢٣هـ، ص٥.
- السيد ، سمير . محاضرات في شبكة المعلومات العالمية . القاهرة : مكتبة عين شمس ، ١٩٩٧م .
- سالم ،فادي . عالم الإنترنت السفلي نشر في مجلة الإنترنت العالم العربي عدد نوفمبر، ١٩٩٩م ص ٢٨
- سيمبسون، الان . الإنترنت، استعد، انطلق، (ب ط) بيروت، مركز التعريب والترجمة، الدار العربية للعلوم، ١٩٩٩م، ص١٣.

- السنو ، مي العبد الله . الاتصال في عصر العولمة، الدور والتحديات الجديدة، ط٢،بيروت، دار النهضة العربية، ص ١٤٦.
- سالم ،فادي . مقالة منشورة في مجلة العالم العربي ، عدد الألفية الثالثة يناير ٢٠٠٠ ص ٢٨ وما بعدها .
- شاهين ، بهاء . شبكة إنترنت، ط١، القاهرة، الدار العربية لعلوم الحاسب، ١٩٩٦م، ص١٢.
- عبد المطلب ، ممدوح عبدالحميد " استراتيجيات الشرطة لمكافحة الإرهاب " من إصدارات مركز بحوث شرطة الشارقة –الشارقة٢٠٠٢ ص ٨٦ – ٩٥ .
- عبد المطلب ، ممدوح عبد الحميد . المهددات الأمنية لاستخدام الإنترنت . الشارقة ،٢٠٠٦م.
- عبد المطلب ، ممدوح عبد الحميد . جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية : الجريمة عبر الإنترنت . الشارقة : مكتبة دار الحقوق ،٢٠٠١م.
- عقل ، مارسيل . الإرهاب المعلوماتي شبح مرعب تعجز عن تحديد مكانه وزمانه ، ٢٠٠٤م.

htt/://www.alwatan.com.sa/daily/2004-07-21/readers.htm

- عمر ،فدوى فاروق . استخدام شبكة الإنترنت في إدارة مؤسسات التعليم العالي في المملكة العربية السعودية، ط١، (بدون ناشر) ١٤٢٤هـ،ص ص١٧- ١٨.
- الفنتوخ ، عبد القادر . الإنترنت للمستخدم العربي . الرياض : مكتبة العبيكان، ١٤٢١هـ ، .
- محمد ، عادل ريان . جرائم الحاسب الآلي وأمن البيانات ، العربي ، العدد ٤٤٠ ، ١٩٩٥م، ٧٣-٧٧ .
- موقع بوابة عجيب (٢٠٠١/٣/٢٥م)

http://it.ageeb.com/viewarticle=1662&category=34

- موقع بوابة عجيب (٢٠٠١/٨/٨م)

http://it.ageeb.com/viewarticle.asp?article=1976&category=17

- ألهاجري ، إياس . تاريخ الإنترنت في المملكة العربية السعودية، ط١، الرياض، بدون ناشر، ١٤٢٥هـ، ص ٥٣.
- اليوسف ، عبد الله عبد العزيز . التقنية والجرائم المستحدثة ، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها ، أكاديمية نايف العربية للعلوم الأمنية ، تونس ، ١٤٢٠هـ (١٩٥-٢٣٣)
- مجلة مفتاح الإنترنت، دار الشبكة العربية للنشر والتوزيع، صفحة عالم الإنترنت، العدد ٤٠، بدون تاريخ، ص ٧.
- مجلة الرسالة الثقافية، العدد الثاني، ذو الحجة ١٤٢٤هـ، ص ٤٤.
- مرآة الجامعة، صحيفة أسبوعية تصدر عن كلية الدعوة والإعلام بجامعة الإمام محمد بن سعود الإسلامية، صفحة تقنيات، العدد ٣٤٣، السنة ٢٢، بتاريخ ١٣/٢/ ١٤٢٥هـ، ص ١٣

ثانيا – المراجع الأجنبية :

- NUA internet Surveys. (1998,June) . How Many Online ? [Online] . Available: http://ww.nua.ie/surveys/howmayonline/index.html [26.10.2000] .
- 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 .
- www.internet-studies.net/a%20short%20history%20of%20the%20internet/2.html
- http:www.mondex.ca mondex Canada
- http:www.ustreas.gov fincen fatfe98.htmi