التلوث المعلوماتي في بيئة العمل الصحفي الالكتروني (الجريمة الالكترونية نموذجا) دراسة حالة

بتول عبد العزيز رشيد

الجامعة العراقية/ كلية الاعلام / قسم الصحافة الاذاعية والتلفزيونية

المقدمة

يمكن القول اننا نعيش في عصر تكنلوجيا الاتصال وسرعة الوصول الى المعلومة فالعالم يتسارع لاقتناء وتطوير احدث الاجهزة وما تمخضت عنه اجهزة الاتصال الحديثة من فوائد ايجابية لا يمكن نكرانها او تجنبها ولكن في الوقت ذاته كانت الاثار السلبية قد برزت وتمحورت لتأخذ جانبا مهما في وضعها ضمن اولى اولويات الباحثين والاكاديميين في حقول المعرفة والعلوم ومنها الاعلام والاتصال.

وتعد شبكة الحواسيب العالمية (الانترنت) اهم وسيلة من وسائل الحصول على المعلومات والاخبار والقضايا التي تشغل الراي العام العالمي. وباستطاعتها ان تحول هذا الكم الهائل من المعلومات الى بيانات الكترونية قابلة للتعامل مع الشبكة العالمية للحواسب (الانترنت) وهي متعددة الاستخدامات فهي شبكة اتصال – ووسيلة اعلام –ومكتبة افتراضية – وتساهم في التعليم عن بعد وزادت اهميتها بزيادة استخداماتها. فنرى أننا نعيش عصر المعلوماتية.

«وهذه النظرة المحددة بالتفاعلية بين مجتمع ما وتطور وسائل الاعلام فيه، لا يعفينا هذا الاختصار من القول وجود تقاطع والاقتراب من مذهب الميديولوجيا الذي هو صيغة الجمع أي علوم الاعلام لا بصفته المفرد وخصوصا ان الاعلام هو المحور المعاصر الذي تتقاطع فيه مجمل العلوم الانسانية الاخرى، فاذا كان هدف الميديولوجيا توضيح سلطات الكلمة في رحلتها الطويلة فان لوسائل الاعلام الحديثة في نقلها وارسالها الدور الاكبر في تحديد هذه السلطة وهي مذهبا فلسفيا متكاملا تبلور على يد فيلسوف فرنسي مرموق مثل ريجيس دوبريه Regis Debras رائد الميديولوجيا أو علم الاعلام الذي باشر بتناوله في محاضرته الجامعية في فرنسا بنشره مفصلا في العام ٢٠٠٠»[١].

ويشتق مصطلح الميديولوجيا لغويا من (ميديو) أي الكلية والجمع للأشياء وتعني تقنيا وسائل الاعلام والانتشار والنقل في اوسع معانيها وتعني (لوجيا) (Logie) علما محددا ياتي نقيضا للاستبدادية التعددية (Multi) أو الجزئية (Micro) التين سيطرتا على الفكر البشري في الربع الاخير من القرن الماضي والتي ساهمتا في الحؤول دون اي جهد منظور يمكثف، غير ان الميديولوجيا تدور حول تطور اللغات والافكار والمعتقدات الاساطير الخاصة بكل انسان معاصر ومدى ارتباطها بطرائق انتقالية من الكتابة الى العلم المرئي المسموع أو لغات ولهجات الاولاد في الساحات والازقة الى شاشات التلفزة وتقودنا هذه النظرية الى الاعلام وثقافة المعلوماتية. التي تجلت باوسع معانيها[١].

مع الثورة المعلوماتية والعصر المعلوماتي ونمو التبادل العلمي والتقني والثقافي بين الدول، تتوفر ظروف ملائمة أكثر إما للحرب النفسية الحديثة، او الحرب المعلوماتية والتعتيم المعلوماتي والإرهاب المعلوماتي، وإما للاستخدام السلمي للمعلومات الذي يسهم في نضال الشعوب العادل من أجل العدالة والسلم الديمقراطي والتقدم الاجتماعي حيث إن المعلوماتية الحديثة واختراعات التقنية المعاصرة ذات القوة التدميرية يمكن أن تشكل خطراً هائلاً إذا لم تكن تحت إشراف أُناس ذوي ضمير وشعور بالمسؤولية وذوي ثقافة أيضاً.. وصولا الى التلوث المعلوماتي أو الجرائم الالكترونية بأدق وصف جرائم تطال المعرفة، الاستخدام، الثقة، الامن، الربح والمال، السمعة، الاعتبار، ومع هذا كله فهي لا تطال حقيقة غير المعلومات، لكن المعلومات، بأشكالها المتباينة في البيئة الرقمية ، تصبح شيئا فشيئا المعرفة، ووسيلة الاستخدام وهدفه، وهي الثقة، وهي الربح والمال، وهي مادة الاعتبار والسمعة. ان جرائم الكمبيوتر بحق هي جرائم العصر الرقمي[٢].

كما ان الفاتورة الاجمالية لجرائم تقنية المعلومات عالميا وعربيا في ٢٠١١ وحده تقدر بحوالي ٣٨٨ مليار دولار امريكي اما التكلفة النقدية المباشرة فتقدر بحوالي ١١١٤ مليار دولار[٣].

المبحث الاول
الاطار المنهجي للبحث

اولا- اهمية الدراسة.

تبرز أهمية البحث باعتباره من البحوث التطبيقية في مجال بيئة النظام المعلوماتي الصحفي التي تكون متاحة ضمن استخدام الحاسوب او الانترنت ولاسيما في المواقع الالكترونية الصحفية بعد ان برزت الشبكة العنكبوتية العالمية كاهم وسيلة جديدة للإعلام والاتصال. علما ان هذه الدراسة تتزامن مع بروز العديد من الظواهر الجديدة ومنها التلوث المعلوماتي التي كانت من نتاجات صناعة تكنلوجيا الاتصال وقد اتاحت هذه التقنية التكنلوجية من ذوي النفوس الضعيفة في ارتكاب العديد من الجرائم الالكترونية ومنها جرائم التسلل الى نظام الحاسب الالي لالحاق الضرر بالمعلومات المخزنة فيه او سرقتها او نشر الفيروسات فيها لذلك جاء هذا البحث ليسد جزءا من النقص الحاصل في هذا النوع من الدراسات وليقدم إضافة جديدة للمعرفة العلمية. وان ماحفز الباحثة التصدي للدراسة هو الإحساس بأهمية الجانب المهني واتجاه المجتمع الاعلامي (الصحفيين) الى تقنيات تكنلوجيا الاتصال في عملية انتاج المعلومة الصحافية.

وخاصة موضوع دراستنا يدور حول العاملين والصحفيين العاملين في المجال الالكتروني.

ثانيا- مشكلة البحث.

تدور مشكلة البحث حول التساؤلات الآتية:

١. ما هو التلوث المعلوماتي واشكاله.
٢. ما هي الجريمة الالكترونية وعلاقتها بالصحفيين العاملين في بيئة العمل الالكتروني.
٣. ما هي الاضرار المتحققة من التعرض الى انواع الجرائم الالكترونية في بيئة العمل الصحفي الالكتروني.
٤. ما مدى استخدام العاملين في المؤسسات الإعلامية (الصحفية) الالكترونية للبرامج المضادة للفيروسات التي تصيب الحاسب الالي.

ثالثا- أهداف الدراسة.

تهدف الدراسة الى:

١. ابراز موضوع التلوث المعلوماتي في المواقع الالكترونية الاعلامية العراقية وتسليط الضوء على العديد من الظواهر التي لازمت التطور المعلوماتي واثرت بشكل او باخر على سلامة العاملين في المجال الصحفي الالكتروني.
٢. الكشف عن شكل اخر من الملوثات الا وهو الجريمة الالكترونية ومدى اثرها على عمل الصحفين العاملين في البيئة المعلوماتية.
٣. الحاجة الى توعية الصحفين العاملين على الانترنت الى هذا الخطر.
٤. الكشف عن استخدام أساليب عمل حديثة، لتحقيق ولو قدر من الامان المعلوماتي للحفاظ. على سلامة الصحف او المواقع من الهجمات الالكترونية.

رابعا- منهج الدراسة:

اعتمدت الباحثة منهج (دراسة حالة) اذ يتناسب مع اغراض البحث "ويدرس الوحدات سواء اكانت صغيرة او كبيرة «ويقوم على التعمق في دراسة المعلومات بمرحلة معينة من تاريخ هذه الوحدة او دراسة جميع المراحل التي مرت بها و الكشف عن العوامل التي تؤثر في الوحدة المدروسة ثم الوصول الى اعمامات علمية متعلقة بها وبغيرها من الوحدات المشابهة»[٤].

مستعينة بذلك بالمنهج المسحي بهدف تصوير الواقع التطبيقي الفعلي للصحفيين العاملين في المواقع الالكترونية الاعلامية العراقية «و بالرغم من إن منهج المسح يلعب دورا وصفيا، إلا انه يمكن أن يودي دورا تفسيريا بشرح الأحداث أو الظواهر التي تدرس»[٥].

لذلك تم الاعتماد على وصف الظاهرة وتتبع علاقتها عن طريق جمع المعلومات عن البحث واللجوء إلى عرض النتائج بأسلوب كمي على وفق طبيعية مشكلة البحث.

خامسا - إجراءات البحث وعينته :

اعتمدت الباحثة على إجراءات عديدة على المستوى النظري والميداني، فعلى المستوى النظري تم الاستعانة بالطريقة المكتبية في جمع البيانات والمعلومات النظرية الخاصة بالبحث وتنظيمها وفق منهجية علمية منظمة .. أما على المستوى الميداني. فقد أعدت استمارة استبيان بعد القيام بدراسة استطلاع أولية للوقوف عند إجابات علمية لتساؤلات البحث وذلك بوضع المحاور الرئيسة في شكل أسئلة خاصة بكل محور وقد تضمنت الاستمارة (١٧) سؤالا فضلا عن اسئلة فرعية مضمنة وجهت إلى المحررين في (المواقع الاعلامية العراقية)، والذين تم اختيارهم بطريقة الحصر الشامل لمحررين يعملون في بيئة الكترونية ولأنهم يمثلون الصحفيين المهنيين المتعاملين بشكل مباشر على اجهزة الحواسيب فضلا باعتمادهم على الشبكة العالمية (الانترنت).و ينتمون لمواقع اعلامية عراقية تختلف في اتجاهاتها وسياساتها وتمثل كل اطياف الشعب العراقي. فوصل عدد المبحوثين الى (٢٤) محرر الكتروني وقد بلغت عدد الاستمارات الموزعة (٢٤) استمارة خضعت للتحليل.

سادسا- حدود البحث:

وتمثلت في:

١. المجال البشري: المحررين الالكترونيين في المواقع الاعلامية العراقية وبواقع:
   أ- (٥) مبحوثين في وكالة الانباء العراقية.
   ب- (٤) مبحوثين في قناة النجف.
   ت- (٣) مبحوثين في قناة الرشيد.
   ث- (٢) مبحوثين في قناة الديوان.
   ج- (٤) في قناة الحرية.

ح- (١) الموقع الرسمي للهيئة الاعلامية للمكتب الشهيد الصدر.

خ- (٥) وكالة انباء الاعلام العراقي.

٢. المجال المكاني:

أ- وكالة الانباء العراقية.

ب- قناة النجف.

ت- قناة الرشيد.

ث- قناة الديوان.

ج- قناة الحرية.

ح- الموقع الرسمي للهيئة الاعلامية للمكتب الشهيد الصدر.

خ- وكالة انباء الاعلام العراقي.

٣. المجال الزماني: يمتد من تاريخ ١-٩-٢٠١٣ لغاية ١-١٢-٢٠١٣ وهي المدة التي تم بها توزيع استمارات الاستبيان وتحليل النتائج.

ثامنا- الثبات والصدق.

إتفق الخبراء على أن المقياس أو(الأداة) يتسم بالصدق أو الصلاحية(validity) متى كان صالحاً لتحقيق الهدف الذي أُعِدَ من إجله وأن يقيس بالفعل ما ينبغي أن يُقاس[٦].

وقد تم اختبار محتوى الاستمارة عن طريق الصدق الظاهري وذلك بعرض الاستمارة على عدد من الخبراء والمتخصصين في مجال الصحافة الالكترونية لمعرفة أرائهم والأخذ بوجهات نظرهم* وقد تم إجراء التعديلات اللازمة للأسئلة استنادا إلى إرشادات وتوجيهات الخبراء.

ويعتبر الثبات والصدق بمثابة الجسر الذي يربط بين المفاهيم والاجراءات المنهجية والاحصائية التي تختبر هذه المفاهيم والنظريات وهما ضروريان لتحقيق احدى خصائص البحث العلمي الاساسية وهي القابلية للتعميم[٥].

ولإختبار ثبات المقياس(Reliability) فان أنسب الإختبارات هي التي تتم بطريقة إعادة الإختبار أو تعدد القائمين بالإختبار على مادة التحليل نفسها وتعليمات الترميز وقواعده نفسها. وقد تمت أعادت التحليل بعد مضي اسبوعين على التحليل الاول. وقد وجدت الباحثة اختلافات طفيفة بين نتائج التحليل الأول ونتائج التحليل الثاني.

تاسعا- الدراسات السابقة:

تعتبر هذه الدراسة من الدراسات الاستكشافية وتفتقر المكتبة العربية الى الدراسات في موضوع التلوث المعلوماتي وبالأخص الجريمة الالكترونية في المجال الاعلامي الا ان اكثر الدراسات التي تناولت هذا الموضوع من الجانب القانوني والتشريعي ومن هنا جاءت فكرة البحث هذه.

وقد كان كتاب عبد الملك الدناني من الدراسات التي عنيت لبحث عن الوظيفة الاعلامية لشبكة الانترنت وهي دراسة مسحية في رصد وسائل الاعلام اليمنية المشتركة في الانترنت وقد اجريت هذه الدراسة ٢٠٠٣ اي مطلع الاستخدام الصحفي للانترنت وقد استفادت الباحثة من هذه الدراسة قدر تعلق الامر بتصميم الاستبانة فقط.

وكانت دراسة يونس عرب وهي بالأصل ورقة عمل بعنوان صور الجرائم الالكترونية حيث تناولت مفهوم الجريمة الالكترونية من وجهة النظر القانونية والتشريعية

فضلا عن دراسة راشد بشير ابراهيم ،التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على امارة ابو ظبي وقد استفادت الباحثة من هذه الدراسة قدر تعلق الامر بانواع الجرائم الالكترونية واشكال الفيروسات التي تخترق الحواسيب الالكترونية

الا ان هذه الدراسة حاولت ان تحدد مؤشرات خطيرة تواجه الصحفيين العاملين في البيئة الالكترونية وتشكل تحديا خطيرا للامن الوطني والدولي باعتبارها الظاهرة الاجرامية المتصاعدة في ظل ثورة المعلومات الحاسوبية.

عاشرا- تحديد المصطلحات:

١- الانترنت (اسم) وهي شبكة منفتحة غير منظمة تؤمن الارتباط بين شبكات معلوماتية على الصعيد العالمي وهي تشكل مكانا للتبادل والتلاقي والحوار والحرية والتربية للعديد من الشعوب مع ذلك قد تنقل هذه الشبكة مضامين صادقة وغير صادقة. ويرى البعض انها النموذج الاولي لقناة المعلومات فائقة السرعة[٧].

٢- المعلوماتية او علم المعلومات.

العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها واختزانها واسترجاعها وتفسيرها وبثها وتحويلها واستخدامها.

فضلا عن الاهتمام بدراسة اساليب معالجة المعلومات كالنظم المعلوماتية ونظم البرمجة وبعبارة مختصرة فان المعلوماتية هي معالجة الالية للمعلومات اما تقنيات المعلومات فتعني التزاوج والالتحام بين التقنيات النظم المعلوماتية والاتصالات والاستعمال المتزايد للالكترونيات في جميع المجالات(٨).

٣- الجريمة الالكترونية.

لقد تعددت تعريفات الجريمة الالكترونية ويمكن ان نعرفها اقرب الى نطاق البحوث الاعلامية وهي نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه " كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات(٢).

٤- التلوث المعلوماتي.

ان الحفاظ على شبكة المعلومات من التلوث بالنصوص والمشاهدة المسيئة للمجتمع يشكل هما مشتركا لجميع مستخدمي الشبكة وهم بذلك يتحملون المسؤولية الاخلاقية للحفاظ على الشبكة نظيفة ومفيدة للجميع(٩).

٥-جرائم الانترنيتInternet Crime أو جرائم المعلوماتية Information Crime. والتي هي فعل إجرامي أو سلوك غير مشروع وغير مسموح به، في محاولةٍ للوصول لبيانات سرية مخزونةٍ داخل الحاسوب، وغير مسموح بالإطلاع عليها ونقلها ونسخها أو حذفها. أو تدمير بيانات وحواسيب الغير بواسطة الفيروسات، والاعتداء على حرية الأشخاص واستغلالهم(١٠).

٦-البرنامج.

هي الأساس الذي تعمل من خلاله الأجهزة (Hardware) خلاف الأجهزة (Software) البرمجية لتحويلها إلى شئ مفيد يقوم بوظائف عدة مثل أنظمة التشغيل وهي من أكبر الأمثلة على البرمجيات. وعلى الرغم من أن البرمجيات (بنوعيها برمجيات النظام وبرمجيات التطبيق) كانت موجودة قبل الإنترنت والبرمجيات هي من أكثر المنتجات الرقمية حاجة للحماية الا انها الأكثر عرضة للقرصنة. مما أدى إلى ظهور فئة تستهدف عمل الجرائم بمختلف أنواعها(١١).

٧- القراصنة crackers-*

يقصد بالقراصنة الاشخاص الذين يقدمون على استخدام او نسخ غير مشروع لنظم التشغيل او البرامج المختلفة للحاسب الالي المحمية بموجب قوانين حق المؤلف سواء بالاستفادة منها شخصيا او تجاريا تحقيقا لأهداف او ميول اجرامية(١٢).

٨- قرصنة برامج الحاسوب.

عرفت بانها الاستيلاء على ملك الغير عن طريق النهب او السرقة دون الجوء الى العنف او الترهيب او التهويل او القتل ولا يدخل في نطاق القرصنة الالكترونية استيلاء الفاعل على المكونات المادية المستخدمة في الحاسب أي ان الفاعل رغم حصوله على البرامج والبيانات الالكترونية المملوكة للغير الا انه لا يخرجها في الوقت ذاته من حيازة ذلك الغير ولا يحول بالتالي بينه وبين الانتفاع بها[١٣].

٩- الاختراق.

وهو جريمة التسلل الى نظام الحاسب الالي لالحاق الضرر بالمعلومات المخزنة فيه او سرقتها او نشر الفيروسات فيها[١٤].

١٠- فيروس الحاسب الالي.

هو عبارة عن برنامج كتب بإحدى لغات البرمجة، اعده مبرمجون متخصصون وهو قادر على التوالد والتناسخ ويستطيع الدخول الى البرامج ويتفوق على نظم التشغيل ويصل الى المكونات المادية مثل الذاكرة الرئيسية او القرص الصلب ويهدف الفيروس الى الولوج للبرامج وتخريبها والانتشار فيها بقوة كما له خاصية الاختفاء والظهور ويضرب بمجرد كتابة كلمة او اصدار امر او حتى بمجرد فتح البرنامج الحامل للفيروس او الرسالة البريدية مما يؤدي الى اصابة الجهاز ومسح محتوياته او العبث بالملفات المخزنة[١٢].

١١- المتسللونHackers:

هم اشخاص برعوا في استخدام الحاسب الالي وبرامجه ولديهم فضول وحب استكشاف يدفعهم للدخول الى اجهزة الحاسب الالي للآخرين بطرق غير مشروعة وبدافع التطفل او التحدي واثبات المقدرة على اختراق نظم امن الشبكات وفي الغلب فان افعالهم هذه لا تحمل ميولا اجرامية او نوايا تخريبية [١٢].

١٢- المحرر الالكتروني من يقوم بالتحرير او المساعدة في تحرير المواقع الاعلامية الالكترونية مهما كان شكلها ومكانها[١٥].

المبحث الثاني

اولا – مفهوم التلوث المعلوماتي :

ان المتتبع للتطور التاريخي لمصادر المعلومات، يجد ان الصحف اليومية وصفحات الكتب والإذاعات هي مصدر المعلومات الرئيسي في الماضي، اما الصور الحالية لمصادر المعلومات تبني ذهناً مشوشاً، فليست كل صور التكنولوجيا تؤدي إلى التطور فالإفراط في حجم المعلومات المتاحة يمثل مشكلة اذ ليس بسبب كميتها الزائدة عن الحد وإنما لكونها بلا مضمون [١٦].

وتوجه الى المجتمع ككل عندها يمكن ان نطلق عليه مجتمع المعلومات أو ما يسمى المجتمع ما بعد الصناعي وهو الذي يعتمد في تطوره بشكل رئيسي على المعلومات والحواسيب وشبكات الاتصال المختلفة وهي ادوات اساسية للتغيير في كافة جوانب المجتمع السياسية والاقتصادية والتجارية والصحية والاعلامية وذلك في سبيل انتاج وتطبيق المعرفة [٩] وخصوصا ان الاعلام هو المحور المعاصر الذي تتقاطع فيه مجمل العلوم الانسانية الاخرى[١].

أما مايك داش وهو استشاري إداري في صناعة التكنولوجيا المتقدمة فقد عبر عن التلوث المعلوماتي حيث، اكتشف أنه متعرض لطوفان من الملوثات المعلوماتية، وقضى عامين كاملين في تطوير استراتيجيه لوضع حد لهذه البيانات المسمومة، وكانت نتيجة بحثه انه اكتشف أن هناك حجماً مروعاً من المعلومات يأتي تحت شعارين الأول: أنت تحتاج إلى شيء ينقصك، والثاني: إذا اشتريت هذا الشيء سيصلح لك الشيء الآخر[١٦].

ثانيا- اشكال التلوث المعلوماتي:

يمكن القول ان مصطلح التلوث المعلوماتي قد بدا بالظهور في الدراسات النظرية نتيجة لتأثير التغييرات السريعة والقوية لثورة تكنلوجيا المعلومات وتكنلوجيا الاتصالات علما مع ان هناك اشكال للتلوث المعلوماتي ويمكن حصرها خدمة للأغراض الدراسة:

١. ان المعلومات بحد ذاتها والموجودة على شبكة الانترنت وما تتعرض له من أخطار وتحريف وتنوع المصادر في الشبكة وكثرتها وتعددها والملوثات الكثيرة التي تؤثر في ثقافة وتربية المجتمعات والتغييرات التي طرأت على المفاهيم والقيم الإنسانية[١٦].

٢.التلوث الالكتروني.

وهو أحدث صيحة في مجال التلوث المعلوماتي، وهو ينتج عن المجالات التي تنتج حول الأجهزة الالكترونية ابتداء من الجرس الكهربي والمذياع والتليفزيون، وانتهاء إلى الأقمار الصناعية والهاتف النقال، حيث يحفل الفضاء حولنا بالموجات الراديوية والموجات الكهرومغناطيسية وغيرها(١٧).

واوضحت احدى الدراسات المصرية في هذا المجال ان هناك عددا من المخاطر الصحية المحيطة بالصحفيين والعاملين في المؤسسات الصحفية المصرية وخاصة المتعاملين منهم مع تكنلوجيا الحاسب الالي (VDU Visual Display Units).

أو شاشات العرض المرئي بحيث تنقسم هذه المخاطر الى ثلاث مجموعات المشكلات المتعلقة بالأجهزة العضلية والعظمية من جراء وضعية الجلوس. والمشكلات المتعلقة بمخاطر الاشعاع وتسبب الارهاق والزغللة والرؤية المزدوجة والمشكلات النفسية وذلك بسبب ان الحاسبات تقوم بتحجيم العلاقات بين الزملاء(١٨).

وخاصة بعد انتشار آلاف الأقمار الصناعية حول الأرض هو تلوث غير مرئي، صامت ، ليس له رائحة أو مذاق هو الملوّث الكامل (perfect pollutant) وهو المسبّب الرئيسي لأغلب المشاكل الصحية في العالم الحديث(١٧).

٣. ان الاتجاه السائد في منطقتنا العربية والاسلامية ينحو باتجاه التوسع في مفهوم التلوث المعلوماتي ويتبنى تصنيفات موسعة تشمل اشكال الافعال والسلوك المخلة بالآداب العامة والقيم الاخلاقية كافة.

وما يمكن إن نلاحظه من خلال ما ينشر عبر شبكة الانترنت من مواقف وافكار تشكل اعتداء على المعتقدات والمقدسات الدينية وما يبث من افلام فاضحة تنتهك القيم الاخلاقية والآداب العامة وخير دليل هلى ذلك ما نشر مؤخرا من صور مسيئة لرسولنا محمد عليه الصلاة والسلام بصحيفة دنماركية وبث عبر شبكة الانترنت، وما تبعه من جدل وخلاف حول معاقبة الجهة التي صدر عنها هذا الفعل(١٢).

حيث تشير الدراسات الاعلامية الحديثة الى انه ينبغي ان يكون تعامل المجتمع الاسلامي مع ظاهرة الاعلام الفضائي تعاملا واقعيا ومسؤولا يدرك حقيقة واقعة وكيفية احسان توظيفه ويغير الصورة التي عليها واقع استخدامات القنوات الفضائية العربية والعالمية حيث لم تحسن الصورة العربية ولا الصورة الاسلامية(١٩).

٤. ظاهرة تشويه اللغات وذلك سواء اكان ذلك من خلال استخدام اللهجات العامية للتعبير عن الذات او كتابة اللغة العربية بأحرف اللغة الانجليزية بشكل ركيك يدمر المعنى ويشوه اللغة مثل ما هو موجود حاليا على صفحات الفي سبوك اذ يقول احدهم للاخر:

Aa m3ioom 2bn 3mi...mr 3lek eshi mn

فيرد الاخر

Hhhhhh Walla ya eben 5alte akwa men heak

هذا هو نموذج من نماذج التلوث المعلوماتي الحاصل حاليا على شبكة الانترنت وتطبيقات التواصل الاجتماعي خاصة بين الاجيال الناشئة التي وجدت نفسها تكبر وتكتسب ثقافتها في خضم تلك التطورات المتسارعة بشكل مذهل(٢٠).

وهذا يعني ايجاد فرضية قائمة على اننا نشهد ميلاد لغة جديدة وعربية ترعاها وسائل الاعلام الكثيرة والحديثة والسريعة وذلك على انقاض العربية القديمة التي تنهار باستسلام خفي ومن دون مقاومة فتذكرنا بادبيات الصراع بين الفصحى والعامية ومعها تنهار الوشائج السلطوية التي تربط اساليب العربية بالأمس مع اساليب الصحافة العربية المعاصرة(١).

٥.النفايات التكنلوجية.

لقد أدى التطور التكنولوجي السريع والعولمة إلى إنتاج كميات كبيرة من الأجهزة الإلكترونية والكهربائية بشكل يكاد أن يكون يومياً مثل أجهزة الكومبيوتر والهواتف النقالة وما إلى ذلك، هذه الأجهزة تتحول إلى نفايات إلكترونية تضر بالبيئة وبالصحة العامة عندما يتمّ التخلص منها، وما يثير الانتباه هو أن الدول الغنية وعلى رأسها الولايات المتحدة الأميركية تعمد إلى تصدير هذه الأجهزة البالية إلى الدول الفقيرة أو إلى دول العالم الثالث بحجة المساعدة.

والهند الآن تتصدر دول العالم بتكنولوجيا المعلومات، لكن هذه الصورة الجميلة لثورة تكنولوجيا المعلومات حوّلت الهند إلى مقبرة لفضلات إلكترونية، التي لا تخلو من المواد السامة الضارة بالبشر والبيئة(٢١).

ثالثا- التلوث المعلوماتي والجريمة الالكترونية.

ومع تنامي ظاهرة العدوان على البيئة المعلوماتية ظهر ما يسمى بالتلوث المعلوماتي والذي يشكّل الوجه القبيح للتقنية الحديثة فالجرائم المتحققة عن هذا العدوان تتميز عن الجرائم العادية بسرعتها الفائقة وتأثيرها المدمّر، وقدرة مرتكبيها على الإفلات من الملاحقة والعقاب في

ظل افتقاد كثير من الدول أنظمة قانونية قادرة على التعامل مع هذا العدوان والجرائم الناجمة عنه. [٢١] وإن مصطلح التلوث البيئي المعلوماتي هو الاسم الاخر للجرائم الالكترونية[٢٢].

ومع صعوبة الاتفاق على مفهوم محدد لجريمة تقنية المعلومات بسبب اختلاف المفاهيم والقيم الاجتماعية والاخلاقية بين المجتمعات[١٢] يمكن ان نشير ان الجريمة الالكترونية هي في الحقيقة عملية اتلاف او تخريب الهدف منها حذف 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 الكتروني[٢٣]. وأصبحت الجرائم المعلوماتية تشكّل تهديداً وتحديا خطيرا للامن الوطني والدولي باعتبارها الظاهرة الاجرامية المتصاعدة في ظل ثورة المعلومات الحاسوبية [١٦] ومن خلال ارتباط هذه الجرائم بوسائل التقنية الحديثة والنظر الى هذه الوسائل بوصفها وعاء للمعلوماتية قد يتم الاعتداء عليه مباشرة للاضرار بهذه المعلومات والتأثير فيها[٨].

لقد اتاحت الانترنت للتكنلوجيين الموهوبين والجماعات الغاضبة ونوعيات مختلفة من المتهربين من القوانين الاستفادة من صعوبة التحكم بالمعلومات لتحقيق اهداف سياسية واجتماعية وتجارية واعلامية[٢٤].

مظاهر الجريمة الالكترونية على الانترنت

تعد الجريمة الالكترونية من أخطر الجرائم وألد ملوث في شبكة الانترنت (١٦) وبشكل عام، يمكن تحديد أبرز المظاهر التي يمكن أن تتحرّك فيها ومن خلالها بعض صور الجريمة على شبكة الإنترنت.

أ: الجرائم الماسة بالمعطيات الشخصية او البيانات المتصلة بالحياة الخاصة.

وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة وهو ما يعرف بموضوع (الخصوصية) (٢) ومن اشهر هذه الوسائل ما يعرف برسائل (كوكيز COOKIES) ببساطة هي عبارة عن برنامج ينتقل الى نظام المستخدم بمجرد دخوله للموقع وتتمكن من تسجيل بيانات تخص المستخدم ، وتتم عن طريق استدراج الزائر الى مواقع مختلفة ولدى دخوله يتم من خلال رسائل الكوكيز تتبعه ومعرفة ميوله وبالتالي ارسال الرسائل الالكترونية اليه (٢٥).

وفي كثير من الأحيان تكون سرقة المعلومات الشخصية التي تخص البطاقة عبر موقع على الانترنت مخصص للشراء مثلا ، عندما يكون هذا الموقع غير آمن يسرق القرصان رقم البطاقة ويستخدمها للاغراضه المختلفة وينتحل شخصية المستخدم الحقيقي (صاحب البطاقة). اكتشفت الكثير من محاولات نسخ بطاقات الائتمان والصراف عن طريق ما يسمى: **(Skimming)(١٦).

ب: الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه وتسمى ايضا الجريمة الثقافية (Cultural Crime)

١- جرائم قرصنة البرمجيات.

Software Piracy: هي عملية نسخ أو تقليد لبرامج أحدى الشركات العالمية على اسطوانات وبيعها للناس بسعر أقل. بدون دفع ثمنها للشركة أو الشخص الذي قام بتصنيعها (٢٦) وتشير التقديرات الى ان هناك حوالي ٣٠٠ مليار صفحة على الاقل يتم اعادة انتاجها من خلال الة نسخة واحدة كل سنة على مستوى العالم ويشمل هذا النسخ الصحف والمجلات والنوت الموسيقية (٢٥) فالحل البديل لقرصنة البرمجيات هو استخدام البرمجيات الحرة . وهي البديل الأمثل للبرمجيات المقرصنة إن لم تود ان تدفع ثمن البرامج الأصلية. وهي برمجيات يمكن استخدامها والتعديل او إعادة توزيعها مجانا بدون أي مقابل مادي بشرط عدم نسبها لأحد غير صاحبها الأصلي. ويوجد برمجيات حرة المصدر ذات مستوى عالي من الكفاءة و يوجد أيضًا بديل حر المصدر لكل البرامج التي يقوم المستخدمين بقرصنتها فمثلا بدل من نظام تشغيل وندو ز يوجد نظام تشغيل لينكس و بدلا من حزمة الأوفيس يوجد حزمة الأوبن أوفيس و بدل من متصفح انترنت اكسبلورر يوجد متصفح فاير فوكس و بدل من برنامج الأدوب فوتوشوب يوجد برنامج جيمب، فهذه هي فكرة البرمجيات حرة المصدر (١٦).

ويمثل اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي) لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج (٢). فقد نظرت المحاكم البريطانية في دعوى رفعتها جمعيات مكافحة القرصنة في امريكيا وبريطانيا ضد مجموعة ميرور الصحف العائدة لروبرت ماكسويل اذ تم الكشف على ٩٠% من البرامج الالية المستعملة في اجهزتها الشخصية وتبين انها مزورة وطالبوا امام المحكمة محو الاسطوانات ودفع تعويض يتجاوز ٢٥٠ الف دولار علما بان ماكسويل كان يشجع على اعتماد القرصنة (٢٥).

٢- جريمة نسخ المؤلفات العلمية و الأدبية بالطرق الالكترونية المستحدثة (٢٦).
ومنها التعدي على القنوات الفضائية المشفرة وإتاحتها عن طريق الانترنت عن طريق تقنية.
(soft copy)(٢٧) اذ تقدم اتحاد الناشرين العرب ببلاغ لادارة مكافحة جرائم الحاسبات وشبكات المعلومات بوزارة الداخلية عن وجود موقع اليكتروني يقوم بنسخ الكتب التي تصدرها عدد من دور النشر المصرية واللبنانية وتبين ان مؤسسة صوت القلم العربي الاعلامية تبث موقع مول الكتاب العربي المعروف باسم «المعرض الاليكتروني الاول للناشرين والمؤلفين الذي يبث من محافظة المنوفية لقيامه بالتعدي حقوق الناشرين المصريين والعرب بتسويق وترويج النسخ الورقية والاليكترونية لكتبهم على موقعه دون اذن كتابي أو شفهي منهم مما سبب خسائر مالية فادحة» (٢٨).

ت: الجرائم التي تستهدف الأشخاص:

وهي الجرائم التي من الممكن أن يصل بها الى قتل الأشخاص بالحاسوب عن طريق تعرضهم التهديد بالقتل(٢٩).

ج: الجريمة الجنسية (Sexual crime).

ويقصد بها الجرائم التي تتم من خلال استخدام الحاسوب او الانترنت عن طريق ايصالها الى المتلقي من دون ان يكون هناك اعتداء على النظام المعلوماتي ومن هذه الجرائم انشاء المواقع الاباحية واستغلال القاصرين جنسيا وعرضها من الصور وفديو وحوارات في تداول الجميع وحتى الاطفال ومن هذه الجرائم كذلك محاولة ابتزاز بعض الاشخاص بنشر الشائعات عنهم وتشويه سمعتهم اذا لم يرضخوا او لم يدفعوا مقابلا ماديا وقد يكون الهدف هو الانتقام (٨) ويخترق الحاسوب عن طريق (فيروس الجنس) وهو يمثل مجموعة من الصور الجنسية مثيرة للغرائز لجلب انتباه القائم على النظام واثناء ذلك ينسخ البرنامج نفسه ويمسح جدول توزيع الملفات (٢٥) هذا النوع من الجريمة يمكن أن يتمثل بإحدى الصور التالية:

- الابتزاز: من أشهر حوادث الابتزاز عندما يقوم احد الشباب باختراق جهاز احد الفتيات أو الاستيلاء عليه و به مجموعة من صورها، وإجبارها على الخروج معه وإلا سيفضحها بما يملكه من صور.
- التغرير والاستدراج: في العادة تتواجد هذه الصورة عندما يتعرف احد الشبان على إحدى الفتيات في الشات أو في برامج المحادثة ويكوّن علاقة معها ثم يستدرجها بالكلام المعسول ويوهمها

بالزواج لكي تثق به ومن ثم يقوم بتهديدها وفضيحتها بما يملكه من صور أو تسجيلات لصوتها إن لم تستجيب لطلباته(٢).

د: جرائم التزوير Forgery والاحتيال.

وتشمل تزوير البريد الالكتروني (E-Mail Forgery Electronic Mail Forgery) وتزوير الوثائق والسجلات Document/Record Forgery و تزوير الهوية Identity Forgery (٢).

وتتم عملية التزوير بالدخول الى قاعدة البيانات وتعديل البيانات الموجودة بها أو اضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك (٢٥).

واستخدام اساليب احتيالية للتنكر الالكتروني فمثلا الاضافة كصديق للمجني عليه وما ان تتم الموافقة يقوم بالتحصيل على نسخة من كل خصوصياته المسجلة على حسابه الخاص (معلومات، صور، مقاطع فيديو، قائمة اصدقاء) ثم استخدامها على نحو غير مشروع كالتشهير والابتزاز أو انشاء حساب جديد منتحلا صفة المجني عليه (٢٨).

هـ: سرقة وقت الانترنت خدمات الكمبيوتر Theft of Computer Services.

وهو استخدام من قبل شخص غير مصرح به لساعات (hacking) ان سرقة وقت الانترنت يأتي في إطار القرصنة للإنترنت المدفوعة من قبل شخص آخر، فالقرصان يصل إلى كلمة المرور للوصول إلى الانترنت اما عن طريق القرصنة أو عن طريق وسائل غير قانونية، فيصل إلى الانترنت من دون علم أو معرفة الشخص (Internet Identity Theft) الآخر. ونعرف أن الوقت تمت سرقته من قبل أي قرصان عندما ينتهي شحن الوقت ونحتاج إلى تعبئتها أو شحنها مع العلم أن الشخص لا يستخدمها بكثرة !! حيث أن (Internet Identity Theft) أن السارق يصل إلى كلمة المرور للوصول إلى الانترنت عن طريق جهاز الكمبيوتر- مما لا نعرف عنه- أنه يقوم بجمع جميع أنواع المعلومات ويخزنها في الملفات المخفية على القرص الصلب. وهذه الملفات تقوم بتخزين المعلومات مثل تسجيل الدخول وكلمات السر، والأسماء والعناوين وحتى أرقام بطاقات الائتمان. ويمكن الحصول على هذه المعلومات بطريقتين: إما عن طريق الاستيلاء عليها أثناء انتقالها انتقالا غير آمن بين الأجهزة عبر الشبكة، أو عن طريق تثبيت برامج ضارة على جهاز الكمبيوتر الخاص بك (مثل برامج التجسس) التي من شانها أن تجمع كل شئ تحتاج إليه تلقائيا واعادتها إلى الجهاز مرة أخرى(١١).

و: تجارة المخدرات باستخدام الانترنت.

ان المخاوف من استخدام الانترنت لا تقتصر على ارتكاب الانترنت في ارتكاب الجريمة بل تساهم بعض المواقع في انحراف الشباب وذلك من خلال انشاء مواقع الالكترونية بقصد الاتجار بالمخدرات او المؤثرات العقلية او الترويج لها او تعاطيها او سهل التعامل فيها او تعاقد او تعامل او تفاوض بقصد ابرام الصفقات المتعلقة بالاتجار بها باي شكل من الاشكال(٣٠).

ز: الجريمة السياسية والاقتصادية (Political and economic crime).

• تستخدم المجموعات الإرهابية حالياً تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية. وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق، وبث الأخبار المغلوطة، وتوظيف بعض صغار السن، وتحويل بعض الأموال في سبيل تحقيق أهدافهم.

• في الولايات المتحدة الأمريكية يقوم الإرهابيون باستخدام الإنترنت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية.

• الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجانا.

• نشر الأفكار الخاطئة بين الشباب كالإرهاب والإدمان والزنا لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى(٢٦).

• وتنفيذ عمليات ارهابية تحت مسميات وهمية او تسهيل الاتصال بقيادات واعضاء الجماعات الارهابية والترويج للأعمال الارهابية و افكارها او نشر عمليات تصنيع و اعداد وتنفيذ الاجهزة المتفجرة او الحارقة او اية ادوات او مواد تستخدم في التخطيط او التنفيذ للأعمال الارهابية وان الجرائم الارهابية(٣٠).

• اختراق المواقع الالكترونية لمجموعة من المؤسسات وخاصة ذات الصبغة الاقتصادية ،الأمر الذي لطالما تسبب في تشفير الحسابات المعلوماتية و النقدية لمجموعة من المصارف.

• رسائل البريد الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج مع الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي؛ وتشفير الأرقام السرية لعدة وسائط بنكية حديثة والتي نجد في مقدمتها البطائق البنكية الالكترونية التي لطالما تعرضت للسطو

الالكتروني من طرف محترفين في الاجرام الالكتروني مما تفقد معه ثقة المرتفق بالمعاملات المصرفية والبنكية[٢٧].

ح- جرائم انتحال الشخصية.

وهي تقسم الى قسمين:

انتحال شخصية الفرد والهدف منها الاستيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية مثلا الاستيلاء على معلومات اختيارية من الضحية فهناك جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية والذي يتطلب بطبيعة الحال الافصاح عن بعض المعلومات الشخصية كالاسم والعنوان والاهم رقم بطاقة الائتمان لضم المبلغ الرمزي الى الجهة الخيرية[٢٥].

انتحال شخصية الموقع فهو الاشد خطورة واكثر صعوبة في اكتشافه ويتم الاتصال بها من خلال الاتصال الامن حيث تتم العملية من خلال اختراق المجرم لاحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي الى توجيه اي شخص الى موقعه بمجرد كتابة اسم الموقع الممشهور[٢٥].

رابعا : بعض أهم وسائل الجرائم الإلكترونية :وتشمل اتجاهين:

اولا: هجمات المعلومات: وتشمل النسخ غير المصرَّح به للبيانات والمعلومات والأوامر والبرمجيات وغيرها، وتحليل الاتصالات، والقيام بعمل قنوات مخفيّة، تمهيداً لهجوم لاحق أو تخزين معلومات غير مشروعة.

ثانيا-هجمات البرمجيات: وتشمل:

١- المصائد أو الأبواب الخلفية (أي اختلاس الثغرات)، :backdoors.

وهي ثغرة تترك عن عمد من مصمم النظام؛ للتسلل إلى النظام عند الحاجة، وتجدر الإشارة إلى أن كل البرامج والنظم التي تنتجها الولايات المتحدة الأمريكية تحتوي على أبواب خلفية تستخدمها عند الحاجة، وهو ما يمكن هيئات وأركان حرب المعلومات من التجوال الحر داخل أي نظام لأي دولة أجنبية[٣١].

السرقة أو اختلاس المعلومة، أو الاستخدام اللحظي ويقصد به سرقة منفعة الحاسب الالي اي استخدامه لأغراض شخصية أو تجارية بدون علم مالكه أو حائزه القانوني وذلك مثلا لتحرير بطاقات مخصصة لأعمال الخير أو لنسخ العاب الفيديو لاستعمالهم الشخصي أو لمعرفة زبائن الشركة أو المؤسسة أو الخدمات التي تقدمها[٣٢] استخدام البرمجيات الخبيثة، كالفيروسات، وهي

تدخل الى الحاسوب بشكل شرعي وكأنها برامج عادية محمولة برفقة برامج اخرى يتم تحميلها الى الحاسوب يعتبرها النظام وكأنها احد برامج التطبيق التي تم تحميله وعند تنفيذ التطبيق يبدا الفيروس نشاطه التخريبي حسب طريقة تصميمه(٣٣).

ومن اشهر الفيروسات الموجهة ضد الحواسيب والشبكات المعلوماتية:

١. فيروس الابطاء ويتمثل عمل هذا الفيروس في ابطاء عمل جهاز الحاسوب بصورة تدريجية تمهيدا لايقافه عن العمل(٣٤).
٢. فيروس (Melissa) ويعتبر من فيروسات احصنة طروادة التي تعني انها تنتقل من خلال التحاقها باحد الملفات مختفية وراءه فهذا الفيروس انتشر من خلال تخفي في شكل مستند (Word) مرسل عبر البريد الالكتروني وقد ادى الى تعطيل العديد من ملفات الانترنت والبريد الالكتروني(٣٣).
٣. والدودة الإلكترونية، الديدان:WORMS

وهي فئة من الفايروسات مبدا عملها قائم على التأثير على النظام بجعله يصدر اوامر خاطئة أو مضللة لمكونات وعناصر هذا الحاسوب بعد ان يحجم دور النظام(٣٣).

٢- الرقائق:chipping تماما مثلما يمكن للبرامج والنظم software أن تحتوي على وظائف غير معروفة أو متوقعة، فمن الممكن أن تحتوي بعض الرقائق على مثل تلك الوظائف، والمصانع الأمريكية تنتج الملايين من تلك الرقائق، وهم سادة العالم في هذه الصناعة الدقيقة؛ حيث يمكن للدوائر المجمعة IC's التي تشكل هذه الرقائق أن تحتوي على وظائف إضافية أثناء تصنيعها، لا تعمل في الظروف العادية، إلا أنها قد تعلن العصيان في توقيت معين، أو بالاتصال بها عن بعد؛ حيث يمكن أن تستجيب لتردد معين لبعض موجات الراديو، فتشل الحياة في مجتمع أو دولة ما(٣١).

٣- القنابل المنطقية او الموقوتة Time Bombs logie Bombs-

وهي عبارة عن برنامج يصمم للدخول الى النظام المعلوماتي وينتشر بداخله بحيث تبقى ساكنة وغير فعالة مدة قد تصل الى اشهر او اعوام وقد تنشط بتاريخ معين كاول يناير او ابريل او نتيجة ظرف منطقي كتغيير امر ما او محو اسم او ادخال او معالجة معلومة بحيث تعمل على تدمير النظام كليا او جزئيا(١٢).

٤- والماكينات والميكروبات فائقة الصغر: ويطلق عليهاNano machines and Microbes ، وهي على عكس الفيروسات التي تصيب برامج ونظم المعلومات، يمكنها إصابة عتاد النظام

نفسه ..hardware فالـ Nano machines عبارة عن robots فائقة الصغر (أصغر من صغار النمل مثلا) قد تنتشر في مبنى نظام معلوماتي في دولة معادية أو منافسة؛ حيث تتفشى في الردهات والمكاتب حتى تجد حاسبًا آليا، وتدلف إليه من خلال الفتحات الموجودة به، وتقوم بإتلاف الدوائر الإلكترونية به.

أما الميكروبات؛ فمن المعروف أن بعضًا منها يتغذى على الزيت، فماذا لو تم تحويرها جينيًّا لتتغذى على عنصر الـ silizium المكون الهام في الدوائر الإلكترونية؟ إن هذا يعني تدمير وإتلاف الدوائر الإلكترونية بأي معمل به حاسبات آلية أو حاسب خادم server لموقع على الإنترنت، أو مبنى هام أو حساس يدار بالكمبيوتر، أو حتى مدينة بأسرها عن طريق إتلاف دوائر التحكم الإلكترونية فيها، والتي تقوم على مرافقها الحيوية[١٢].

٥- عمليات الاغراق بالرسائل الاليكترونية: وذلك من اجل اجهاد نظم تشغيل تلك الاجهزة والشبكات والحاق الضرر بها وتعطيلها عن العمل او تدميرها[٢٨].

٦- ومدافع hero، وقنابل Emp، أما المدافع؛ فهي عبارة عن مدافع تطلق موجات راديو مركزة وعالية الطاقة والترددhigh energy radio frequency ، والتي يمكنها تعطيل وإتلاف أي هدف إلكتروني، وقد يتراوح الضرر من ضرر متوسط بغلق شبكة حاسب مثلا أو إعادة تشغيله بشكل دوري، فلا يمكن استغلاله، أو ضرر بالغ بإعطاب العتاد الخاص بالحاسب أو الشبكة بشكل لا يمكن بعده إصلاح الحاسب أو الشبكة.

أما قنابل EMP فهي تشبه المدافع غير أنها تستخدم نبضات إلكترو مغناطيسية ElectroMagnetic Pulse؛ حيث يمكن التسلل إلى مواقع العدو الإلكترونية الحساسة والهامة، وإلقاء هذه القنابل، التي سوف تتلف كل الحواسب والشبكات في دائرة انفجارها غير المدوي أو المشتعل، وهي وإن كانت أصغر حجما من مدافعHERF، إلا أنها أوسع وأبعد أثرا؛ حيث لا اختيار لهدف مع القنبلة، بينما قذيفة مدفع HERF تنتقي هدفها. والنوع الأخير من أسلحة حرب المعلومات يستخدم في الأغراض العسكرية[٣١].

ويجمع بين هذه الأنواع أنها برمجيات ضارة تستخدم للتدمير أو التعطيل، وإن كان بعضها يستخدم في الأغراض العسكرية[١٦].

ويمكن ان تخترق الحاسب الالي من خلال ارسال ملف تجسس يقوم بتمكين المخترق من الدخول وهذا الملف يخترق الموقع باحد الطرق وهي[١٤]:

ترسل عن طريق البريد الالكتروني عن طريق استقبال ملفات عند استخدام برامج المحادثة باستعمال قرص مرن مصاب بملف التجسس وعند تشغيله يصاب الحاسب الالي بهذا الملف بتحميل برامج أو ملف عن طريق الشبكة العالمية للمعلومات من مواقع غير موثوق بها ومن برامج التجسس تسمى (تروجن أو باتش) ترسل من قبل المخترق وتختبى في ملفات النظام.

خامسا: أعراض اصابة الحاسوب بالفيروس: وتتمثل فيما ياتي:

- بطء تشغيل الجهاز.
- توقف النظام عن العمل.
- نقص شديد في سعة الذاكرة المؤقتة.
- ظهور حروف غريبة الضغط على مفاتيح معينة.
- تغير في حجم الملفات و عددها.
- عرض رسالة خطأ فجائية و غير عادية.
- تشغيل القرص أكثر من المعتاد.
- سماع صوت صفارة: مع ظهور رسومات على الشاشة مصحوبة بتوقف الجهاز.

الأضرار التي تسببها الفيروسات في اجهزة الحواسيب

- تدمير شبكات الاتصالات و الحسابات.
- إتلاف بعض أجزاء من الدوائر المتكاملة وتدميرها تماما.
- تقليل سرعة وكفاءة عمل وحدة التشغيل المرئية المعروفة باسم الميكروبروسيسور.
- تقليل سرعة عمل وحدات الطباعة والأقراص المرنة والصلبة.
- إتلاف البيانات المسجلة على قواعد البيانات (بتغير في بعض البيانات – حذف بعض البيانات – تبديل بعض السجلات).
- إدخال بيانات مضللة أو بيانات رسمية وغير موجودة أصلا في السجلات الأساسية.

أما بالنسبة للأنواع الحميدة والتي لا تسبب أضرارا فهي برمجيات تعطي نوعا من الدعابة والفكاهة للمستخدم مثل ظهور عبارات مسلية على الشاشة من وقت لآخر – عزف قطعة موسيقية هادئة – ظهور بعض الرسومات مثل الأزهار وشجرة الكريسماس – ظهور صور لبعض المعاليم الأثرية الشهيرة ومشاهير الفنانين ولاعبي كرة القدم[٣٥].

برامج مكافحة الفيروسات

يمكن للصحفيين العاملين على الحاسب الالي من مكافحة الفيروسات – سواء من الاصابة بها أو باكتشاف وجودها – وخاصة اذا المخترقين اذا يئسوا من اكتشاف كلمة السر الخاصة بالموقع الخاص، فانهم يتجهون الى محاولة اختراق الحاسب الالي يمكن تنظيف الجهاز من ملفات التجسس بزيارة موقع:

htt://housecall.antivirus.com/pc.-housecall/start-corp.asp

ففي هذا الموقع يمكنك ان تتأكد من خلو الجهاز الذي تعمل عليه من الفيروسات وملفات التجسس(١٤).

وأفضل طرق الحماية من هذا النوع:

تأمين متصفح الويب.

حماية المعلومات الحساسة والخاصة.

حذف محفوظات المواقع على الإنترنت.

حذف ذاكرة التخزين المؤقتة الخاصة بك على الجهاز.

افراغ سلة المحذوفات(١١).

سادسا: الشروط الواجب توافرها من اجل الحماية من الجريمة الالكترونية.

يمكن أن نقوم باتخاذ إجراءات وقائية، ويجب أن تكون جزء من العمل على الإنترنت:

١. على مشغلي الانترنت تجنب الكشف عن أي معلومات تتعلق بهم، مثل بطاقات الهوية، أو الهوية على موقع الإنترنت أو غيرها.

٢. عدم إرسال الصور عبر الإنترنت أثناء التحدث مع الغرباء.

٣. حفظ نسخة احتياطية من الملفات والمجلدات، بحيث أنه لو فقدت بيانات أو معلومات نتيجة لابتلائها بالفيروسات، يكون هناك نسخة منها.

٤. عدم أستخدم بطاقة الائتمان الخاصة في حالة عدم التأكد من أن الموقع آمن، فهذا الاحتياط قد تحمي من التحايل(٣٦).

٥-ستخدام برامج حماية اليكترونية اصلية (غير منسوخة) Internet Security وتحديثها بصفة مستمرة وذلك لحماية الحاسب الالي من اي فيروسات واردة عبر شبكة الانترنت أو اي ميديا اخرى يتعامل معها(٢٨).

٦- ضرورة وضع ارقام سرية على الملفات الهامة حتى لا يستطيع فتحها اي شخص مع ضرورة تغيير الرقم السري بصورة دورية حتى لا يصبح قابل للاختراق[٣٧].

اما كلمات المرور (password) ضرورة ان تكون معقدة ومكونة (حروف، ارقام حروف خاصة)[٢٨] ولتجاوز هذه الاشكالية ينبغي الجمع بين المعرفة التقنية والعملية المتوفرة لدى خبراء اجهزة الحاسب الالي ونظم تقنية المعلومات من جهة وبين المعرفة المهنية والقانونية من جهة اخرى[١٢] وقد حاولت بعض المدن أو الاحياء في الولايات المتحدة حل هذه المشكلة (التلوث المعلوماتي) وخاصة فيما يخص موضوع استغلال بعض المشتركين حرية الانترنت المفتوحة، وذلك عبر تأسيس شبكات مغلقة تتصل مع الانترنت عبر بوابات يمكن التحكم بها جيدا كما حاولت جهات اخرى حل المشكلة بانشاء مواقع لتقييم المضمون الفكري والاخلاقي على الشبكة بما يتيح الوصول الى المعلومات الجيدة مباشرة دون التعرض للمرور عبر مواقع غير مرغوب بها، على اعتبار انها مسؤولية اخلاقية وقانونية كبيرة من اجل العمل على حماية الشبكة[٩].

اولا: بيئة العمل الصحفي الالكتروني وسلامته من الجرائم الالكترونية.

ان التطبيقات التي يمكن انجازها باستخدام الحاسبات الرقمية لا يمكن حصرها اذ تمثل ضرورة حتمية مع سرعة تحول صناعة الصحافة الى انظمة النشر المكتبي[١٨]. وقد اتضح دخول التكنلوجيا في تطوير اساليب اداء عمليات الانتاج بما في ذلك الانتاج الاعلامي بل ان اجهزة الاعلام تعد من بين اولى المجالات التي انتفعت من التطور التكنلوجي بشكل واسع[٣٨]. وبرزت الشبكة العنكبوتية العالمية كاهم وسيلة جديدة لنشر المعلومات منذ ظهور التلفاز اذ انها تتيح للمراسلن الصحفيين الوصول الى المعلومات من جميع انحاء العالم على الفور كما تتيح للمراسلين الصحفيين ايجاد معلومات من مصادر لم يكونوا ليجدوها سابقا وتسمح للصحفيين ان يكونوا اكثر شمولية واكثر دقة واكثر اكتمالا وتسمح للناس ان ينشروا معلومات لجمهور دولي بطريقة فعالة من حيث التكلفة والكفاءة ان الشبكة العنكبوتية العالمية تعمل على تغيير مهنة الصحافة تغييرا جذريا [٣٩].

فبلنسبة للصحفيين المحترفين والمنظمات الاخبارية فانهم يستخدمون الشبكات الاجتماعية والاكثر شعبية مثل تويتر أو الفيسبوك وهذه الادواة بوصفها نقطة بداية ممتازة لتطوير الاخبار الصحفية والبحث عن ابطال محتملين لنصوص تثير الاهتمام من الناحية الانسانية[١٥].

ومع ان مجتمع الانترنت الرحب فتح افاقا واسعة امام التدفق الهائل للمعلومات والصحفيين في العالم اجمع حيث يقدم الخدمات الاخبارية عن طريق البريد الالكتروني E-MAIL

– والشبكة العنكبوت العملاقة والمعروفة ومحركات البحث والتخاطب عبر الانترنت والمجموعات الاخبارية والتجارة الالكترونية وبروتوكول نقل الملفات وتمكن هذه الخدمة المستخدم من نسخ الملفات من جهاز حاسوب الى جهاز اخر[٣٤].

ورغم المزايا العديدة التي تتمتع بها التكنلوجيا الجديدة وتمثل اضافة مهمة لصناعة النشر بصفة خاصة وبذلك فان هذه التكنلوجيا الحاسبات والاتصالات ودخولها الى دور الصحف قد ادى الى وجود العديد من الضغوط الجديدة على الصحفيين والعاملين بهذه الدور وهو ما ادى بدوره الى عديد من التاثيرات الصحية السلبية لتكنلوجيا الصحافة[١٨].

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. وهنا يحسن بنا التنويه بأن التخريب الذي يمكن أن تتعرض له نظم المعلومات تختلف صوره و تتعدد أشكاله والأضرار التي قد تنتج عنه، لذا فإن الوسائل الدفاعية تختلف بإختلاف تلك الإدوات التخريبية وطبيعة الأضرار التي قد تحدثها. الحرب المعلوماتية [٢٣].
وظهرت مصطلحات جديدة في عالم الامن المعلوماتي والحاسب الالي والانترنت مثل:
.Crackers – Hackers

فهؤلاء المخربون او القراصنة او المتطفلون يدخلون على الانظمة والبرامج والمواقع والشبكات والحاسبات دون تصريح ويسببون إضرارا للهدف. وهناك امثلة حية عن عمليات التسلل والتخريب التقني، فقد اقدمت مجموعة من القراصنة الاسرائيليئون على اختراق موقع صحيفة (غالف نيوز) وتخريبه على الشبكة الدولية للمعلومات الانترنت، وقاموا بإزالة الموقع ورفع العلم الاسرائيلئ مقرونا بعبارة (تحيا اسرائيل) وقد بينت التحقيقات التي قامت بها مجموعة من خبراء الكومبيوتر في الصحيفة من خلال مواقع عدة في الولايات المتحدة الامريكية ان مصدر التخريب هو مجموعة من الحاسبات الالكترونية بالدولة العبرية مرتبطة بمزود الخدمة (ننفجن) ويستخدم القراصنة عادة عددا من الاساليب التقنية في التخريب منها تشويه المواقع، اختراق النظم، حملات تشويه المعلومات واستخدام الفيروسات او حصان طروادة لشن حروبهم على الشبكة [٤٠].

وتحت عنوان كتبت جريدة الاخبار العراقية (الجيش السوري الالكتروني) يخترق صحيفة (ديلي تلغراف) البريطانية كما واعلن عن اختراقه صفحة وكالة الاسوشيتدبرس على موقع تويتر ونشر اخبار كاذبة يعلن مسؤوليته عن اشاعة (تفجير البيت الابيض) ويخترق موقع صحيفة

(فاينانشيال تايمز) البريطانة وترك الجيش السوري الالكتروني بصمته على الحسابات المخترقة من خلال الوسم #SEA.

كما تم نشر مقطع فيديو (لارهابيين يقومون باعدام بعض المدنيين) بحسب تعبير المخترقين وقد حذفت هذه التغريدات بعد استعادة الحسابات وذكر موقع Business Insider.

ان الهجمة الالكترونية شملت اختراق حسابات الصحيفة على تويتر والخاصة بالاخبار والرياضة والكوميديا والكتب وغيرها من الحسابات . اضافة الى اختراق الصفحة الرسمية للصحيفة على الفيسبوك ويأتي هذا الاختراق ضمن سلسلة هجمات الكترونية نفذها افراد «الجيش السوري الالكتروني» على عدة جهات اعلامية غربية احتجاجا على التلفيق الاعلامي الموجه ضد سورية بحسب تعبيرهم. لهذه الاسباب يتعاظم الاهتمام بامن المعلومات الالكترونية وسلامتها[٤١].

ومن الهجمات الالكترونية الاعلامية ففي عام ٢٠٠٧ تعرضت استونيا لهجوم حجب الخدمة على المستوى الوطني، ادى الى إن يبقى البلد كله مفصولا عن الانترنت على مدار اسبوع ،فاثر ذلك في الشبكات الحكومية وشبكات الاتصالات والدوائر المالية والاعلامية[١٢].

وفي تشرين الاول عام ١٩٨٥استطاعت احد الصحف الاسبوعية الباريسية من اختراق نظام الحماية للحاسوب الخاص بلجنة الطاقة النووية الفرنسية كانت الغاي هي اختبار قوة النظام ولكن الصحيفة خرجت بمعلومات غاية في السرية والاهمية عن مشروع سلاح الليزر الذي يجري تطويره لحساب وزارة الدفاع الفرنسية وكذلك عن مشروع اخر يتعلق بمنطقة التجارب النووية الفرنسية في المحيط الهادي وقد اكتفت الصحيفة بنشر العبارات الرئيسية العريضة عن بعض المعلومات دون الخوض في التفاصيل وقد بينت بانها توصلت الى هذه المعلومات الغاية في الاهمية بواسطة حاسوب شخصي وبمساعدة احد العاملين في مركز المعلومات الخاصة باللجنة النووية الفرنسية ،حيث زودها بالكلمات السرية مقابل رشوة دفعت له[٣٣].

وبذلك لا يمكن ان ننكر صعوبة تحديد الخط الفاصل في هذا الموضوع اذ طالما كانت لسلع العامة والمزايا الاخرى خاضعة لسيطرة الحكومة على الانترنت فهي تعد بمثابة امور ضرورية لنجاح الانترنت ولن تستطيع اي جهة ان تقدم ذلك عمليا الا الحكومات الاقليمية التقليدية ،ولا يمكن للفوضى وهي غياب القوة الالزامية للحكومة ان تستمر حيث على الرغم من مشاكل الحكومات الديمقراطية فانها ما زالت النظام الافضل في التاريخ ومع وجود صحافة حرة وانتخابات نزيهة وقضاء مستقل وبالتالي فان نجاح الانترنت في التقليل من اضرار التلوث المعلوماتي يعتمد على استقرار الدول[٢٤].

سابعا: ضرورة التعاون الدولي.

لذلك لابد من ان يكون هناك تعاون دولي يتفق مع طبيعة هذه الجرائم والتي تتميز بطابع خاص يقتضي ان تكون هناك اجراءات تحقيقية سريعة ويسمح هذا التعاون الدولي بسهولة الاتصال المباشر بين اجهزة الشرطة في الدول المختلفة وذلك عن طريق انشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالانترنت والحاسوب وتعميمها والدولة بمفردها لا تستطيع القضاء على هذه الجرائم لانها عابرة للحدود لذلك فان الحاجة ملحة الى تعاون وتنسيق العمل ومكافحة هذه الجرائم وقد تبلور هذا النوع من التعاون الدولي في انشاء المنظمة الدولية للشرطة الجنائية (الانتربول) Interpol وتتولى هذه المنظمة اقامة العلاقات بين دول المنظمة وتبادل المعلومات بين السلطات والتحقيق فيما يتعلق بجرائم المعلوماتية ومنها جرائم الانترنت وقد انشا المجلس الاوربي في عام ١٩٩١ شرطة اوربية تختص بملاحقة الجرائم العابرة للحدود[٤٢].

الاطار العملي وتحليل البيانات لمظاهر الجريمة الالكترونية على الانترنت

جدول (١)

يبين اتجاهات معرفة المبحوثين لمعنى التلوث المعلوماتي واشكاله

الاجابة	التكرار	النسبة المئوية
نعم	١٨	%٧٥
كلا	١٦	%٢٥
المجموع	٢٤	%١٠٠

يتبين من جدول (١) ان ٧٥% من المحررين العاملين على اجهزة الحاسوب والمتصلة بالانترنت على دراية تامة بمعنى التلوث المعلوماتي في حين ان نسبة ٢٥% من المبحوثين لم يكونوا على علم بوجود معنى للتلوث المعلوماتي ويمكن ان يتم ايعاز السبب الى ان التقنية الحديثة والتكنلوجيا الراهنة غير مضرة وهذا يستدعي الانتباه حتى لو كانت نسبة قليلة من المحررين الصحفيين .

جدول (٢)

يبين اشكال التلوث المعلوماتي التي يتعرض لها المبحوثين قيد الدراسة

(سمح للمبحوثين باكثر من اختيار)

اشكال التلوث المعلوماتي	التكرار	النسبة
الملوثات التي تؤثر في ثقافة وتربية المجتمعات والتغييرات التي طرأت على المفاهيم والقيم الإنسانية.	٢٠	%٣٦
التعرض الى ما ينشر عبر شبكة الانترنت من مواقف وافكار تشكل اعتداء على المعتقدات والمقدسات الدينية.	٢٠	%٣٦
التعرض الى التلوث الالكتروني وما ينتج عنه من المجالات التي تحدث حول الأجهزة الالكترونية.	٨	%١٥
٤-التعرض الى استخدام اللهجات العامية للتعبير عن الذات او كتابة اللغة العربية باحرف اللغة الانجليزية.	٤	%٧
٥- استخدام النفايات التكنلوجية (الاجهزة البالية والمستملة من قبل الاخر).	٣	%٦
المجموع	٥٥	%١٠٠

وعن اشكال التلوث المعلوماتي فقد سمحت الباحثة لاختيار اكثر من شكل لمعرفة الانواع المعروفة لدى المحررين الالكترونيين علما ان كل الانواع تمثل هي اشكال للتلوث المعلوماتي واتضح من جدول (٢) ان الملوثات التي تؤثر في ثقافة وتربية المجتمعات والتغييرات التي طرأت على المفاهيم والقيم الإنسانية. التعرض الى ما ينشر عبر شبكة الانترنت من مواقف وافكار تشكل اعتداء على المعتقدات والمقدسات الدينية. قد حصلت على اعلى النسب من المبحوثين ٣٦% بينما التعرض الى التلوث الالكتروني وما ينتج عنه من المجالات التي تحدث حول الأجهزة الالكترونية. قد حصل على ١٥% التعرض الى استخدام اللهجات العامية للتعبير عن الذات او كتابة اللغة العربية باحرف اللغة الانجليزية. ٧% علما يعتبر من الملوثات الخطيرة جدا في راي الباحثة وهذا الخطر سيتعزز على المدى البعيد. واستخدام النفايات التكنلوجية (الاجهزة البالية والمستملة من قبل الاخر) قد حصل على اقل النسب ٦% علما ان جميع هذه الملوثات للبيئة وخطرة جدا على صحة الانسان.

جدول (٣)

يبين اتجاهات تعرض المبحوثين الى الجريمة الالكترونية.

الاجابة	التكرار	النسبة المئوية
نعم	١٦	%٦٧
كلا	٨	%٣٣
المجموع	٢٤	%١٠٠

من جدول (٣) يتضح ان المحررين الالكترونيين قد تعرضوا الى الجريمة الالكترونية وبنسبة ٦٧% وما تبقى من العينة اشاروا انهم لم يتعرضوا الى الجريمة الالكترونية وعلما ان المتبقين ومن خلال استعراض النتائج النهائية للبحث هم ايضا متعرضين الى الجريمة الالكترونية ولكن لا يعرفون المعنى أو غير مدركين ان الجريمة الالكترونية هي احى انواع التلوث المعلوماتي ومن اخطرها ويشكلون ٣٣%.

جدول (٤)

يبين اتجاهات تعرض المبحوثين الى الجرائم الماسة بالمعطيات الشخصية او البيانات المتصلة بالحياة الخاصة

الاجابة	التكرار	النسبة المئوية
نعم	٨	%٣٣
كلا	١٦	%٦٧
المجموع	٢٤	%١٠٠

من جدول (٤) يتضح ان الجرائم الماسة بالمعطيات الشخصية او البيانات المتصلة بالحياة الخاصة هي واحدة من الجرائم الالكترونية التي يتعرض لها المحررين العاملين على اجهزة الحواسيب الالكترونية وان نسبة٦٧% لم يتعرضوا الى هذا الاعتداء وبنسبة ٣٣% قد اشاروا بتعرضهم الى هذه الجريمة الالكترونية.

جدول (٥)

يبين اتجاهات المبحوثين حول تشكيل الاعتداء على جريمة يحاسب عليها القانون

الاجابة	التكرار	النسبة المئوية
نعم	١١	%٤٦
كلا	١٣	%٥٤
المجموع	٢٤	%١٠٠

وعن مدى معرفة المحررين الالكترونين ان هذا الاعتداء هل هو جريمة يحاسب عليها القانون ام لا فقد اشارت النسبة الاكبر بالنفي ٥٤% ونسبة قليلة اشارت بالإيجاب ٤٦% وهذه سابقة خطيرة كون هذه الثقافة قد تكون سائدة في المجتمع.

جدول (٦)

يبين مدى تعرض المبحوثين الى الجرائم الماسة بحقوق الملكية الفكرية والثقافية

الاجابة	التكرار	النسبة المئوية
نعم	١٦	%٦٧
كلا	٨	%٣٣
المجموع	٢٤	%١٠٠

في جدول (٦)

اما الجريمة الماسة بحقوق الملكية الفكرية والثقافية فقد اشارت نسبة ٦٧% انهم تعرضوا الى السرقة وان نسبة ٣٣% لم يتعرضوا الى هذا النوع من الاعتداء.

جدول (٧)

يبين المبحوثين الذين تعرضوا الى انواع الجرائم الماسة بحقوق الملكية الفكرية والثقافية

	التكرار	النسبة المئوية
جريمة سرقة المقالات الصحفية	١٦	%٦٩
جريمة نسخ المؤلفات العلمية او الأدبية	٥	%٣١
المجموع	١٦	%١٠٠

في جدول(٧) يتضح ان من تعرضوا الى جريمة سرقة المقالات الصحفية ٦٩% وان من تعرضوا الى جريمة نسخ المؤلفات العلمية او الأدبية وبنسبة ٣١% مما يعني هناك سرقات متاحة للجميع ولا يوجد من يراقب من قبل الحكومة أو هيئة أو منظمة دولية أو محلية

جدول (٨)

يبين مدى تعرض المبحوثين الى جريمة التهديد عبر الانترنت

الاجابة	التكرار	النسبة المئوية
نعم	١٦	%٦٧
كلا	٨	%٣٣
المجموع	٢٤	%١٠٠

في جدول (٨) يتضح الذين تعرضوا الى التهديد عبر الانترنيت ٦٧% اما من هم لم يتعرضوا الى هذا الاعتداء وبنسبة ٣٣% مما يعني ان العمل الصحافي يحمل الكثير من المخاطر وهناك من يتربص للصحفيين.

جدول (٩)

يبين انواع الجرائم التهديد عبر الانترنت

	التكرار	النسبة المئوية
التهديد بالقتل	١٣	%٨١
التهديد بالخطف	٢	%١٣
تفجير المنزل	١	%٦
المجموع	١٦	%١٠٠

من خلال قراءتنا للجدول (٩) يتضح ان الذين تعرضوا الى التهديد بالقتل ٨١% والذين تعرضوا الى التهديد بالخطف ١٣% اما التهديد بتفجير المنزل ٦% والحقيقة هذه نسب تنذر بالخطر الحقيقي في واقع الاعلام العراقي وقياسا كدراسة حالة مثل دراستنا هذه.

جدول (١٠)

يبين مدى تعرض المبحوثين الى الجريمة الجنسية الالكترونية عبر الانترنت

الاجابة	التكرار	النسبة المئوية
نعم	٦	%٢٥
كلا	١٨	%٧٥
المجموع	٢٤	%١٠٠

اما في الجدول (١٠) وعن تعرض المبحوثين الى الجريمة الجنسية عبر الانترنت فقد اشارت نسبة ٧٥% في حين نجد ان نسبة ٢٥% قد تعرضت الى ما يسمى بالجريمة الجنسية من المبحوثين.

جدول (١١)

يبين المبحوثين الذين تعرضوا الى انواع الجريمة الجنسية الالكترونية عبر الانترنت

الجريمة الجنسية الالكترونية	التكرار	النسبة المئوية
الابتزاز (نشر الشائعات وتشويه السمعة)	٤	%٦٧
نشر صور مزيفة ومحرفة	٢	%٣٣
التغرير والاستغلال بما يملكه المجرم من مستندات أو بيانات (صور أو تسجيل صوتي)	---	----
المجموع	٦	%١٠٠

يشير جدول (١١) الى النسبة الاكبر من المبحوثين قد تعرضوا الى جريمة الابتزاز (نشر الشائعات وتشويه السمعة) وبنسبة ٦٧% ونشر الصور المزيفة والمحرفة بنسبة ٣٣% اما جريمة التغرير والاستغلال بما يملكه المجرم من مستندات أو بيانات (صور أو تسجيل صوتي) لم يتم الاشارة لها من قبل المبحوثين وهذه تمثل الضعف في المجال الرقابي وهناك اعتداء مستمر وموجه الى الصحفيين العراقيين.

جدول (١٢)

يبين مدى تعرض المبحوثين الى جرائم التزوير الالكتروني

الاجابة	التكرار	النسبة المئوية
نعم	١٨	%٧٥
كلا	٦	%٢٥
المجموع	٢٤	%١٠٠

في جدول (١٢) يتعرض الى جريمة اخرى وهي التزوير الالكتروني فقد اشارت نسبة ٧٥% هم من تعرضوا الى هذه الجريمة وان نسبة ٢٥% لم يتعرضوا الى هذه الجريمة

جدول (١٣)

يبين المبحوثين الذين تعرضوا الى انواع جرائم التزوير الالكتروني

جرائم التزوير الالكتروني	التكرار	النسبة المئوية
تزوير البريد الالكتروني	١٥	%٨٣
وتزوير الوثائق والسجلات	٣	%١٧
تزوير الهوية	---	----
	١٨	%١٠٠

في جدول (١٣) يتضح هناك أنواعي من جرائم التزوير الالكتروني استطعنا رصد الصحفيين الذين تعرضوا الى هذه الجريمة فقد واتضح ان نسبة ٨٣% قد تعرضوا الى تزوير البريد الالكتروني الخاص. في حين نسبة ١٧% قد تعرضوا الى وتزوير الوثائق والسجلات ولم يتم الاشارة الى تزوير الهوية الشخصية للمبحوثين. وهذا يشير الى ايضا ضعف الوعي بخطورة تكنلوجيا الاتصال والتقنية الحديثة وما يتمخض عنها من جرائم ترتكب بحق الصحافيين.

جدول (١٤)

يبين مدى تعرض المبحوثين الى سرقة وقت الانترنت خدمات الكمبيوتر الخاصة

الاجابة	التكرار	النسبة المئوية
نعم	١٣	%٥٤
كلا	١١	%٤٦
المجموع	٢٤	%١٠٠

لقد اتضح من جدول (١٤) ان وقت الانترنت اي خدمات الانترنت المتاحة تتعرض الى السرقة من قبل الاخر وهو اعتداء بحد ذاته لانه خدمة مدفوعة الثمن وان نسبة ٥٤% قد اشارت انها تعرضت الى من يسرق هذا الوقت في حين اشارت نسبة ٤٦% انها لم تتعرض الى هذا الاعتداء.

جدول (١٥)

يبين مدى تعرض المبحوثين الى مواقع الكترونية تستخدم الانترنت لتجارة المخدرات

الاجابة	التكرار	النسبة المئوية
نعم	٥	%٢١
كلا	١٩	%٧٩
المجموع	٢٤	%١٠٠

لقد اشارت نسبة ٧٩% انها لم تتعرض الى المواقع التي تستخدم هذا النوع من الاتجار في حين اشارت نسبة منهم انها تتعرض الى مثل تلك المواقع وبنسبة ٢١% وتعتبر هذه المواقع بحد ذاتها تلوث الكتروني من الملوثات التي يجب مكافحتها ومن قبل الصحفيين انفسهم باعتبارها رسالة انسانية.

جدول (١٦)

يبين مدى تعرض المبحوثين الى الجريمة السياسية والاقتصادية الالكترونية

الاجابة	التكرار	النسبة المئوية
نعم	٨	%٣٣
كلا	١٦	%٦٧
المجموع	٢٤	%١٠٠

من جدول (١٦) يتضح من المبحوثين الذين لم يتعرضوا الى الجريمة السياسية والاقتصادية الالكترونية بنسبة ٦٧% وان نسبة ٣٣% قد تعرضوا الى هذا النوع من الاعتداء علما ان هناك انواع لهذه الجريمة كما هو موضح في جدول (١٧).

جدول (١٧)

يبين <u>المبحوثين</u> الذين تعرضوا الى انواع الجريمة السياسية والاقتصادية الالكترونية

انواع الجريمة السياسية والاقتصادية الالكترونية	التكرار	النسبة المؤية
بث الأخبار المغلوطة على موقعك الالكتروني	٦	%٧٥
اغراق موقعك الالكتروني برسائل البريد الواردة من مصادر مجهولة	٢	%٢٥
اختراق موقعك الالكتروني ونشر تنفيذ عمليات ارهابية	---	----
المجموع	٨	%١٠٠

يتضح من هذا الجدول ان نسبة ٧٥% قد تعرضوا الى بث الأخبار المغلوطة على الموقع الالكتروني وهي نسبة كبيرة قياسا الى النوع الاخر من الاعتداء والمتمثل باغراق الموقع الالكتروني برسائل البريد الواردة من مصادر مجهولة وحصدت نسبة ٢٥% اما اختراق موقع الالكتروني ونشر تنفيذ عمليات ارهابية لم تشر مجموعة المبحوثين ان هناك من تعرض الى هذا النوع من الاعتداء.

جدول (١٨)

يبين مدى تعرض المبحوثين الى جريمة انتحال شخصية من قبل شخص اخر للقيام بممارسات غير مشروعة

الاجابة	التكرار	النسبة المئوية
نعم	١٣	%٥٤
كلا	١١	%٤٦
المجموع	٢٤	%١٠٠

يتضح من جدول (١٨) ان من المبحوثين قد تعرض الى جريمة انتحال الشخصية وبنسبة ٥٤% وهناك من لم يتعرض الى هذا النوع من الجرائم وبنسبة ٤٦% وهي من الجرائم التي تعرض سمعة المحررين الصحفيين الى الخطر علما اذا كانت هذه الممارسات غير مشروعة.

جدول (١٩)

يبين عدد المرات التي تم فيها اختراق الحاسوب الشخصي للمبحوثين

الاجابة	التكرار	النسبة المئوية
ولا مرة	١٣	%٥٤
مرة واحدة	٩	%٣٨
مرتين	٢	%٨
اكثر من ثلاث مرات	---	-----
المجموع	٢٤	%١٠٠

وعن سؤال المبحوثين عدد المرات التي تم فيها اختراق الحاسوب الشخصي اتضحت نسبة ٥٤% لم يتم الاختراق ولا مرة وبنسبة ٣٨% مرة واحدة تم فيها الاختراق وبنسبة ٨% مرتين وبشكل عام لوحظ وجود اختراق يتعرض له المحررين العاملين على اجهزة الحواسيب الالكترونية

جدول (٢٠)

يبين عدد المرات التي تمت بها سرقة البريد الالكتروني للمبحوثين

الاجابة	التكرار	النسبة المئوية
ولا مرة	٨	%٣٣
مرة واحدة	٧	%٢٩
مرتين	٦	%٢٥
اكثر من ثلاث مرات	٣	%١٣
المجموع	٢٤	%١٠٠

اما عن جريمة سرقة البريد الالكتروني لوحظ ان نسبة ٣٣% لم يتم بها سرقة البريد الالكتروني ولا مرة في حين ان العينة التي خضعت الى التحليل قد تمت بها سرقة البريد الالكتروني ولكن بنسب متفاوتة وبالشكل الاتي بنسبة ٢٩% مرة واحدة و٢٥% مرتين و ١٣% اكثر من ثلاث مرات وبصورة عامة تشير النتائج الى وجود اختراق واعتداء واضح يتعرض لها المبحوثين.

جدول (٢١)

يبين عدد المرات التي تم فيها اختراق الموقع الالكتروني الاخباري الذي يعمل فيه المبحوثين

الاجابة	التكرار	النسبة المئوية
ولا مرة	١٠	%٤٢
مرة واحدة	٦	%٢٥
مرتين	٨	%٣٣
اكثر من ثلاث مرات	---	-----
المجموع	٢٤	%١٠٠

اما عن الاختراق الموقع الالكتروني الذي يعمل به الصحفي المحرر الالكتروني اشارت نسبة ٤٢% انها لم تتعرض الى الاختراق بينما نسبة ٢٥% قد تعرضت مرة واحدة الى الاختراق ونسبة ٣٣% تعرضت مرتين للاختراق وتوعز الباحثة الى ان هناك خطر حقيقي وصل الى مدى

بعيد يتعرض اليه الصحفيين العراقيين من خلال التماس المباشر عبر الانترنت مع الاخر الذي يقوم بعمليات الاعتداء.

جدول (٢٢)

يبين مدى استخدام المبحوثين الى برامج الحماية من الفيروسات وتحديثه بشكل دوري

الاجابة	التكرار	النسبة المئوية
نعم	٢٣	%٩٦
كلا	١	%٤
المجموع	٢٤	%١٠٠

وعن طرق المعالجة في جدول (١٩) توجهت الباحثة بالسؤال عن مدى استخدام البرامج المتوفرة في الاسواق للحماية من الفايروسات فقد اشارت نسبة كبيرة قياسا من عدد المبحوثين انها تستخدم هذه البرامج وبنسبة ٩٦% في حين نسبة ٤% قد اشارت بعدم استخدامها وهذا يفسر وجود اهمال من قبل بعض المبحوثين بشان اقتناء هذه البرامج أو ما يصدر عنها من النسخ المحدثة استخدام برامج حماية اليكترونية اصلية (غير منسوخة) Internet Security وتحديثها بصفة مستمرة وذلك لحماية الحاسب الالي من اي فيروسات واردة عبر شبكة الانترنت أو اي ميديا اخرى يتعامل معها.

جدول (٢٣)

يبين مدى اتخاذ المبحوثين الى الاجراءات وقائية للحفاظ على البيانات من السرقة والتلف

الاجابة	التكرار	النسبة المئوية
نعم	٢٠	%٨٣
كلا	٤	%١٧
المجموع	٢٤	%١٠٠

من جدول (٢٠) اتضح نسبة من المبحوثين ٨٣% يتخذون اجراءات حماية من الفايروسات وان النسبة الاقل هم لا يتخذون اجراءت بديلة وبنسبة ١٧% وبعد سؤالهم عن السبب اتضحت اسباب غير منطقية في راي الباحثة ومنها لا توجد اجراءات بديلة أو عدم استخدام

الادوات والاجهزة الناقلة للفايروسات مثل(الفلاش) والسبب يعزوا الى ان هناك عدم وجود دراية من قبل المحررين العاملين على اجهزة الحواسيب المتصلة بالانترنيت.

اهم النتائج

١. ايد ٧٥% من المحررين العاملين على اجهزة الحاسوب والمتصلة بالانترنت على دراية تامة بمعنى التلوث المعلوماتي في حين ان نسبة ٢٥% من المبحوثين لم يكونوا على علم بوجود معنى للتلوث المعلوماتي وبذلك يشكلون الجهل التام بوجود هذا النوع من الملوثات في بيئة العمل الصحفي.

٢. لقد اقر وبنسبة ٦٧% من المبحوثين وجود الجريمة الالكترونية وتعتبر من الملوثات المعلوماتية وما نسبته ٣٣% هم ايضا متعرضين الى الجريمة الالكترونية ولكن لا يعرفون المعنى أو غير مدركين ان الجريمة الالكترونية هي احى انواع التلوث المعلوماتي ومن اخطرها.

٣. لقد تبين من خلال نتائج البحث ان هناك سرقة للبريد الالكتروني الخاص واختراق للحواسيب الشخصية واختراق للموقع الالكتروني الاخباري الذي يعمل فيه المبحوثين العاملين وبمختلف المواقع الاعلامية الالكترونية وبنسب مختلفة.

٤. اشارت نتائج التحليل النهائية ان المبحوثين قد تعرضوا لمختلف جرائم الانترنيت فقد تعرضت ٦٧%الى جرائم الماسة بقوق الملكية الفكرية وبواقع ٦٩% من هم تعرضوا الى سرقة المقالات الصحفية و ٣١%من هم تعرضوا الى نسخ المؤلفات العلمية والادبية من قبل مواقع اخرى بدون علم اصحابها.

٥. في حين اقر ٦٧% قد تعرضوا الى التهديد عبر الانترنت وبواقع ٨١% قد تم تهديدهم بالقتل و١٣% التهديد بالخطف ٦%ا لتهديد بتفجير المنزل.

٦. وقد اكد المبحوثين انهم تعرضوا الى جرائم ما يعرف بالجريمة الجنسية عبر الانترنت بواقع ٢٥%منهم ٦٧% الى جريمة الابتزاز ونشر الشائعات وتشويه السمعة .فضلا عن انواع الجرائم الاخرى التي تراوحت نسبها بين المرتفع جدا والمتوسط بالنسبة للتعرض الى الجرائم الالكترونية ومنها جرائم التزوير الالكتروني وجرائم التعرض الى المواقع الالكترونية لتجارة المخدرات وجرائم السياسية والاقتصادية الالكترونية التي حصدت ٧٥% في البث الاخبار

المغلوطة و٢٥% اغراق الموقع الالكتروني برسائل البريد الوارد من مصادر مجهولة فضلا عن جريمة انتحال الشخصية.

٧. اكد المبحوثون بان هناك طرق لمعالجة والتصدي الى الجرائم الالكترونية وبنسبة ٩٦% ومع ذلك فانهم عرضة لمثل هذه الهجمات عبر الانترنت . في حين نسبة ٤% قد اشارت بعدم استخدامها وهذا يفسر وجود اهمال من قبل بعض المبحوثين بهذا الشان. ضعف الجانب الرقابي في البيئة الالكترونية وتخلفها في الجانب القانوني لدرء اخطار الاعتداء على العاملين في الحقل الاعلامي الالكتروني وقلة الخبرة التقنية والعملية الجمع بين المعرفة التقنية والعملية المتوفرة لدى خبراء اجهزة الحاسب الالي ونظم تقنية المعلومات من جهة وبين المعرفة المهنية والقانونية من جهة اخرى.

التوصيات

١. ان مجتمعنا العربي يعيش في مواجهة صعبة تتمثل بتحديات التلوث المعلوماتي بكل اشكاله وانواعه ولعل اخطرها هي الجريمة الالكترونية ولذلك لابد من توحد الجهود العربية بكل طاقاتها من خلال صياغة استراتيجيات عربية موحدة وشاملة تتصدى لكل خطار اشكال التلوث المعلوماتي من خلال تطوير الصناعات التكنلوجية والصناعة المعلوماتية والثقافية والعمل على تسويقها وفق افضل الاطر العلمية الحديثة.

٢. تهيئة المهنيين والصحفيين العاملين في الحقل الالكتروني الى اساليب عمل حيثة تتصدى لكل اشكال التلوث المعلوماتي قبل الشروع والانخراط في الحياة المهنية.

٣. البدء الفوري باعداد الكوادر الصحفية وتهيئتهم ليكونوا ملمين بالتقنيات الحديثة والتي كل ماله علاقة باجهزة الحاسوب وما له علاقة بشبكة الانترنت.

٤. توفير برامج مكافحة الفايروسات وباسعار مناسبة تباع في جهات لها علاقة بالعمل الصحفي من اجل تحصين المهنة الصحفية من اشكال الجرائم الالكترونية.

٥. انشاء منظمة عربية معترف بها على الصعيد العالمي لها علاقات مع المنظمات غير الحكومة او منظمات تابعة الى الحكومات المحلية من اجل تنسيق الجهود للحد من مظاهر التلوث المعلوماتي ومنها بالأخص الجريمة الالكترونية.

الهوامش والمصادر

١. خوري، نسيم، الاعلام العربي وانهيار السلطات اللغوية، (بيروت: مركز دراسات الوحدة العربية،٢٠٠٥).

٢. عرب، يونس، صور الجرائم الالكترونية واتجاهات تبويبها، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، ٢-٤ نيسان/ ابريل، (سلطنة عمان: مسقط، ٢٠٠٦).

٣. غيطاس، جمال محمد، الامن المعلوماتي والجرائم الالكترونية ادوات جديدة للصراع، مركز الجزيرة للدراسات، ٢٩ شباط ٢٠١٢Jcforstudies@aljazeera.net.

٤. العتابي، جبر مجيد حميد، طرق البحث الاجتماعي، (وزارة التعليم العالي والبحث العلمي: لا جامعة الموصل،١٩٩١).

٥. الجمال، راسم محمد، مقدمة في مناهج البحث في الدراسات الاعلامية، (مركز جامعة القاهرة للتعليم المفتوح: مطبعة جامعة القاهرة،١٩٩٩).

٦. عبد الحميد محمد، البحث العلمي في الدراسات الإعلامية، (القاهرة، عالم الكتب للنشر والتوزيع والطباعة، ٢٠٠٧).

*الاساتذة الخبراء الدكتور اكرم فرج الربيعي اكاديمي وباحث وكاتب في مجال الاعلام والاتصال والدكتور رياض محمد كاظم اكاديمي وباحث في المجال الاعلامي.

٧. الحايك، اودين سلوم، مسؤولية مزودي خدمات الانترنت التقنية، (طرابلس- لبنان، المؤسسة الحديثة للكتاب، ٢٠٠٩).

٨. البقمي، ناصر بن محمد، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون الخليج العربية:(الامارات العربية المتحدة- ابو ظبي)، سلسلة محاضرات، مركز الامارات للدراسات والبحوث الاستراتيجية، ٢٠٠٨.

٩. عليان، ربحي مصطفى، مجتمع المعلومات والواقع العربي، (عمان، دار جرير للنشر والتوزيع، ٢٠٠٦).

١٠. هرمز، سهى بطرس: الجانب المظلم من التكنولوجيا المعلوماتية http://zowaa.org/about%20us.htm.

١١. المشتري، ديمة عبد العزيز، الجرائم الالكترونية ضد الملكية والمجتمع، مركز التميز للأمن المعلومات http://coeia.ksu.edu.sa.

* بعض المصطلحات معروفة باللغة الانكليزية عند التداول اكثر من اللغة العربية وقد عربت لأغراض البحث العلمي.

١٢. ابراهيم، راشد بشير، التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على امارة ابو ظبي: مجلة: تصدر عن مركز الامارات للدراسات والبحوث الاستراتيجية العدد ١٣١، ٢٠٠٨، ابو ظبي، الامارات العربية المتحدة.

١٣. الخلايلة، عايد رجا، المسؤولية التقصيرية الالكترونية: المسؤولية الناشئة عن اساءة استخدام اجهزة الحاسوب والانترنت: دراسة مقارنة، (الاردن– عمان، دار الثقافة، ٢٠٠٩).

١٤. الدخيل، ابو عبد الله عبد الرحمن بن محمد بن عبد الله، توصيف اختراق المواقع على الشبكة العالمية للمعلومات، وجهة نظر شرعية، (المملكة العربية السعودية: مكتبة الرشد، ٢٠٠٥).

١٥. حسنين شفيق، التدريب الاعلامي عبر الانترنت، (دار فكر وفن للطباعة والنشر والاعلان– بغداد ٢٠١١).

١٦. محمد، أحمد ،دراسة عن تلوث البيئة المعلوماتية على الموقع الالكتروني (نادي الاحياء العربي)
http://www.alarabiclub.org/index.php?p_name=member_details& 2006-07-06

١٧. التلوث الالكتروني وتأثيره على البيئة دراسة على الموقع الالكتروني -http://env .gro.com/vb/showthread.php?t=221

١٨. اللبان، شريف درويش– هشام عطية عبد المقصود: مقدمة في مناهج البحث الاعلامي (مصر: الدار العربية للنشر والتوزيع، ٢٠٠٨).

١٩. البدراني، فاضل، الاعلام صناعة العقول (بيروت: منتدى المعارف،٢٠١١).

٢٠. خالد ربايعة: تلوث المعلومات ،مقالة منشورة على الموقع الالكتروني .www.alqudsalraqmi.sp/atemplate.php?id

٢١. دراسة بعنوان تلوث المعلومات على الموقع الالكتروني.
http://www.mdarat.net/vb/showthread.php?t=23

٢٢. معتز كوكش، خبير في تقنية المعلومات والجرائم الالكترونية حوار اجرته قناة DM في برنامج صانعو القرار على الموقع الالكترونيWWW.face book.com

٢٣. إياس الهاجري: الحرب المعلوماتية http://www.minshawi.com على الموقع الالكتروني– يناير ٢٠٠٢م.
٢٤.سميث، جاك جولد و تيم و ومن يحكم الانترنت؟ اوهام عالم بلا حدود ،ترجمة فاطمة غنيم(هيئة ابو ظبي للثقافة والتراث ،المجمع الثقافي)٢٠٠٩.
٢٥.عياد، سامي علي حامد، الجرائم المعوماتية واجرام الانترنت (الاسكندرية، دار الفكر الجامعي)٢٠٠٦.
٢٦. **Skimming).
٢٧.ويعمل هذا الجهاز لتقديم نسخة من البطاقة التي يمكن استخدامها لأغراض احتيالية ، و في حالة عدم ضرورة وجود البطاقة يقوم بجمع المعلومات لاستعمالها على الانترنت وهي على نوعين نسخ بطاقات الائتمان في المقاهي والمطاعم، حيث يقدم المستخدم بطاقته الائتماني ة للنادل للدفع، ليأخذها النادل ويمررها في جهاز النسخ، ومن ثم يمررها في جهاز المطعم للدفع. وتسمى عملية تمرير البطاقة في الجهاز المذكور ب Skimming وتباع هذ ه الأجهزة على الإنترنت و في المزادات الإلكترونية بأسعار تتراو ح ب ين ٢٠٠ و ١٠٠٠ دولار .أميركي، أي أن انتشارها واسع جدا، وبمقدور أي قرصان الحصول عليها وتركيبها. (ATM) أما النوع الأخر: هو جهاز الكتروني صغير يعلق على بطاقة ائتمان أو محطة ماكينة الصراف الآلي عن طريق إضافة قطعة بنفس حجم ولون القطعة الموجودة لإدخال البطاقة ولكنها تحتوي على قارئ معلومات إضافي يقوم بنسخ المعلومات ونسخ البطاقة، وفي كل مرة يتم تمرير هذه البطاقة يقوم هذا الجهاز بجمع المعلومات وغالبا ما يكون متصل بكاميرا جانبية دقيقة للمراقبة عند عملية إدخال الرقم السري على لوحة المفاتيح وكذلك إرسا ل صور لا سلكية تصل إلى بعد ٢٠٠ متر تقريبا. (للمزيد اقرا المصدر) المشتري، ديمة عبد العزيز، الجرائم الالكترونية ضد الملكية والمجتمع، مركز التميز للامن المعلومات .http://coeia.ksu.edu.sa
٢٨.الجرائم الإلكترونية: الهيئة القومية للاتصالات: السودان، الخرطوم على الموقع الالكتروني .http://www.ntc.gov.sd/index.php?n
٢٩.العباس الوردي– مقال بعنوان الجريمة الالكتروني الثلاثاء ١٢ فبراير ٢٠١٣ – ١٢:٢٥على العنوان الالكتروني http://hespress.com/.

٣٠. الرشيدي، محمود، العنف في جرائم الانترنت، اهم القضايا: الحماية والتامين (القاهرة :الدار المصرية البنانية،٢٠١١).
٣١. ما هي الجريمة الالكترونية دراسة على الموقع الالكتروني http://ejabat.google.com/ejabat/thread?sort=wsmopts&tid=6b6e .9edd6835
٣٢. الزيدي، كاظم عبد جاسم، مكافحة الجرائم المعلوماتية في التشريع العراقي/ على الموقع الالكتروني./http://www.iraqja.iq/view.1813
٣٣. اشرف هيكل، اسلحة حرب المعلومات واستخداماتها، على الموقع الالكتروني .http://kenanaonline.com/users/ashrafhakal/posts/94428
٣٤. الشوابكة، محمد امين، جرائم الحاسوب والانترنت، الجريمة المعلوماتية (عمان، دار الثقافة،٢٠٠٩، ط٣).
٣٥. داود، سرحان سليمان، محمود عبد المنعم المشهداني، امن الحاسوب والمعلومات (الاردن- عمان، دار وائل للنشر، ٢٠٠١).
٣٦. نهلا عبد القادر، الجرائم المعلوماتية (الاردن- عمان، دار الثقافة، ٢٠١٠).
٣٧. الكشباطي، وليد، جرائم اختراق الأنظمة المعلوماتيّة الجمعة ١٢ حزيران (يونيو) ٢٠٠٩ http://www.chawkitabib.info/spip.php?rubrique73
٣٨. الحرقان، أشواق بنت حمد بن محمد، الجريمة الالكترونية أسبابها وطرق الحماية منها:
٣٩. center of excellence in information assurance على الموقع الالكتروني.
٤٠. http://coeia.ksu.edu.sa/%D8 مركز التميز لامن المعلومات.
٤١. عريان، امير الفونس: ورقة مقدمة للمؤتمر الثاني للمركز القومي للبحوث الاجتماعية والجنائية بعنوان الجرائم الالكترونية في البنوك وكيفية مواجهتها خلال الفترة ١٥-١٦ديسمبر ٢٠١٠ .http://coeia.ksu.edu.sa/%D8.
٤٢. الهيتي، هادي نعمان ،في فلسفة اللغة والاعلام (القاهرة: الدار الثقافية للنشر، ٢٠٠٦).
٤٣. راندي ريدريك- اليوت كينغ، ترجمة لميس البحيى، صحفيي الانترنت (الاردن: الاهلية للنشر والتوزيع،٢٠٠٩).
٤٤. الدليمي، عبد الرزاق محمد، الصحافة الالكترونية والتكنولوجيا الرقمية، (مصر: دار الثقافة للنشر والتوزيع،٢٠١١).

٤٥. جريدة الاخبار، خبر منشور في الصفحة الثالثة في جريدة الاخبار العراقية العدد ٢٦٣ الاربعاء ٢٠١٣-٥-٢٢.

٤٦. الطوالبة، علي حسن، التعاون القضائي الدولي في مجال مكافحة الجرائم الالكترونية، المركز الاعلامي الامني على الموقع الالكتروني:

http://www.policemc.gov.bh/reports/2012/February/7-2-2012/634642378126988013.p

الملاحق
الاستمارة التي خضعت للتحليل

السؤال الأول: هل تتعرض المعلومات التي تقدم عبر الانترنيت إلى تلوث معلوماتي وتحريف بكل أشكاله؟

١. نعم [ ].
٢. لا [ ].

إذا كانت الإجابة نعم إي من الملوثات تعرضت لها هذه المعلومات؟

١. الملوثات التي تؤثر في ثقافة وتربية المجتمعات والتغييرات التي طرأت على المفاهيم والقيم الإنسانية[ ].
٢. التعرض الى التلوث الالكتروني وما ينتج عنه من المجالات التي تحدث حول الأجهزة الالكترونية [ ].
٣. التعرض الى ما ينشر عبر شبكة الانترنت من مواقف وافكار تشكل اعتداء على المعتقدات والمقدسات الدينية [ ].
٤. التعرض الى استخدام اللهجات العامية للتعبير عن الذات او كتابة اللغة العربية بأحرف اللغة الانجليزية[ ].
٥. استخدام النفايات التكنلوجية (الاجهزة البالية والمستعملة من قبل الاخر) [ ].

السؤال الثاني: هل تعرضت إلى الجريمة الالكترونية؟

١. نعم [ ].
٢. لا [ ].

السؤال الثالث: هل تعرضت الى اعتداء يمس بالمعطيات الشخصية او البيانات المتصلة بالحياة الخاصة.

١. نعم [ ].
٢. لا [ ].

السؤال الرابع: هل يشكل هذا الاعتداء جريمة يحاسب عليها القانون؟

١. نعم [ ].
٢. لا [ ].

السؤال الخامس: هل تعرضت الى الجرائم الماسة بحقوق الملكية الفكرية والثقافية؟

١. نعم [ ].
٢. لا [ ].

اذا كانت الاجابة نعم اي نوع من الجرائم تعرضت لها؟

١. جريمة نسخ المؤلفات العلمية او الأدبية [ ].
٢. جريمة سرقة مقالاتك الصحفية [ ].
٣. أخرى تذكر.

السؤال السادس: هل تعرضت الى تهديد عبر الانترنت؟

١. نعم [ ].
٢. لا [ ].

اذا كانت الاجابة نعم أي نوع من التهديد تعرضت له؟

١. التهديد بالقتل [ ].
٢. التهديد بالخطف [ ].
٣. اخرى تذكر.

السؤال السابع: هل تعرضت الى الجريمة الجنسية الالكترونية عبر الانترنت؟

١. نعم [ ].
٢. لا [ ].

اذا كانت الاجابة نعم اي من هذه الجرائم تعرضت لها؟

١. الابتزاز (نشر الشائعات وتشويه السمعة) [ ].
٢. التغرير والاستغلال بما يملكه المجرم من مستندات أو بيانات (صور أو تسجيل صوتي) [ ]
٣. نشر صور مزيفة ومحرفة.

السؤال الثامن: هل تعرضت الى جرائم التزوير الالكتروني؟

١. نعم [ ].
٢. لا [ ].

اذا كانت الاجابة نعم اي من جرائم التزوير الالكترونية تعرضت لها؟

١. تزوير البريد الالكتروني [ ].
٢. وتزوير الوثائق والسجلات [ ].
٣. تزوير الهوية [ ].
٤. أخرى تذكر.

السؤال التاسع: هل تعرضت الى سرقة وقت الانترنت خدمات الكمبيوتر الخاصة بك؟

١. نعم [ ].
٢. لا [ ].

السؤال العاشر: هل تعرضت الى مواقع الكترونية تستخدم الانترنت لتجارة المخدرات؟

١. نعم[ ].
٢. لا[ ].

السؤال الحادي عشر: هل تعرضت الى الجريمة السياسية والاقتصادية الالكترونية؟

١. نعم [ ].
٢. لا [ ].

إذا كانت الإجابة نعم ما هي أنواع الجرائم الالكترونية التي تعرضت لها؟

١. بث الأخبار المغلوطة على موقعك الالكتروني [ ].
٢. اختراق موقعك الالكتروني ونشر تنفيذ عمليات ارهابية [ ].
٣. إغراق موقعك الالكتروني برسائل البريد الواردة من مصادر مجهولة [ ].
٤. أخرى تذكر.

السؤال الثاني عشر: هل تعرضت الى جريمة انتحال شخصية من قبل شخص اخر للقيام بممارسات غير مشروعة؟

١. نعم [ ].
٢. لا [ ].

السؤال الثالث عشر: كم عدد المرات التي تم فيها اختراق حاسوبك الشخصي؟

١. ولا مرة [ ].
٢. مرة واحدة [ ].
٣. مرتين [ ].
٤. اكثر من ثلاث مرات [ ].

السؤال الرابع عشر: كم عدد المرات التي تمت بها سرقة بريدك الالكتروني؟

١. ولا مرة [ ].
٢. مرة واحدة [ ].
٣. مرتين [ ].
٤. اكثر من ثلاث مرات [ ].

السؤال الخامس عشر: كم مرة تم فيها اختراق الموقع الالكتروني الاخباري الذي تعمل فيه؟

١. ولا مرة [ ].
٢. مرة واحدة [ ].
٣. مرتين [ ].
٤. أكثر من ثلاث مرات [ ].

السؤال السادس عشر: هل تستخدم برامج الحماية من الفيروسات وتحدثه بشكل دوري؟

١. نعم [ ].
٢. لا [ ].

السؤال السابع عشر: هل تتخذ اجراءات وقائية للحفاظ على البيانات من السرقة والتلف؟

١. نعم [ ].
٢. لا [ ].