الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة

الدكتورة: ليتيم فتيحة
كلية الحقوق و العلوم السياسية
- جامعة عنابة -

الدكتورة: ليتيم نادية
كلية الحقوق و العلوم السياسية
- جامعة سكيكدة -

ملخص:

إنَّ بروز مفهوم الحكومة الإلكترونية، وانتشار تقنيات المعلوماتية في كلِّ قطاع من قطاعات الأنشطة البشرية، وتغلغلها المستمر فيها، بات يؤكِّد أهمية موضوع الأمن المعلوماتي الوطني لها، بوصفه الأداة الفعَّالة لضمان حماية تُخُوم الحكومة الإلكترونية، وضمان نجاح تطبيقها على أرض الواقع، هذا من جهة.

من جهة أخرى، فإنَّ تطور المعرفة لدى مستخدمي الحاسوب بشتَّى مستوياتهم، وانتشار نظم الشبكات، وسيادة شبكة الإنترنت، أضحى يشكِّل تهديدًا إضافيًا؛ بسبب امتلاك زمرة منتخبة من هؤلاء المستخدمين خبرة رصينة، ورغبة في استكشاف الجوانب الخفيَّة منَ المواقع الإلكترونية، الأمر الذي يسوِّغ لهم محاولة اختراق نُظُم الشبكات المتخصصة،أو ما يطلق عليها بالقرصنة الإلكترونية، والتي أصبحت اليوم شبح يتهدد العالم، وهاجسا أمنيا يتحدى قيام الحكومة الإلكترونية.

ومن هنا، فإن الأمر يستدعي ضرورة تأمين البيانات والمعلومات، لبعث الثقة والأمان في التعامل، في البيئة الرقمية المفتوحة التي نعيشها اليوم، والتي تُعدً المعلومات من أهم ركائزها ومقوماتها.

Résumé :

L'émergence de la notion de e-gouvernement, et la prolifération des technologies de l'informatique dans tous les secteurs des activités humaines souligne l'importance de la question de la sécurité de l'information, comme un outil puissant pour assurer l’existence de l’e- gouvernement.

Cependant, le développement de la connaissance des utilisateurs d'ordinateurs, et la prolifération des réseaux d'Internet sont devenus une menace supplémentaire, en raison des tentatives de pénétrer illégalement dans les sites et systèmes des réseaux spécialisés , ou ce qu’on appelle «le piratage électronique», qui est devenu aujourd'hui la plus grande menace qui affronte le gouvernement électronique.

La question appelle aujourd’hui à la nécessité de sécuriser les données, et de protéger la sécurité de l'information du gouvernement de la menace du piratage, pour assurer un climat de confiance dans l'environnement numérique ouvert.

مقدمة:

يشهد العالم منذ منتصف القرن العشرين ثورة جديدة، اصطلح على تسميتها بالثورة المعلوماتية، وذلك إشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن.[1] وقد كان لهذه الثورة تأثيراتها على الحكومات التي حاولت الاستفادة منها، ووضع خطط وطنية لتطويرها واستثمارها على أكمل وجه، من أجل مواكبة العصر وانجازاته المتسارعة في جميع المجالات. وقد تجسد ذلك أساسا عبر مشاريع الانتقال من شكلها التقليدي المألوف، إلى شكل الحكومة الإلكترونية ".Gouvernement Electronique"

إلا أنَّ بروز مفهوم الحكومة الإلكترونيَّة، وانتشار تقنيات المعلوماتية في كلِّ قطاع من قطاعات الأنشطة البشرية، وتغلغلها المستمر فيها، بات يؤكِّد أهمية موضوع الأمن المعلوماتي الوطني لها، بوصفه الأداة الفَعَّالة لضمان حماية تُخُوم الحكومة الإلكترونية، وضمان نجاح تطبيقها على أرض الواقع، هذا من جهة. من جهة أخرى، فإنَّ تطور المعرفة لدى مستخدمي الحاسوب بشتَّى مستوياتهم، وانتشار نظم الشبكات، وسيادة شبكة الإنترنت، أضحى يشكِّل تهديدًا إضافيًّا؛ بسبب امتلاك زمرة منتخبة من هؤلاء المستخدمين خبرة رصينة، ورغبة في استكشاف الجوانب الخفيَّة منَ المواقع الإلكترونية، الأمر الذي يسوّغ لهم محاولة اختراق نُظُم الشبكات المتخصصة،[2] أو ما يطلق عليها بالقرصنة الإلكترونية.

وقد انتشرت في السنوات الأخيرة ظاهرة القرصنة، وتفاقمت، حيث لم تعد شبكة الإنترنت مجرد أداة إيجابية للحصول على المعلومات، بل أصبحت تشكل خطورة كبيرة لكل المستخدمين.[3] **فهل فكرت يوماً ما يمكن أن يحصل إذا ما تم اختراق أنظمة الحكومة الإلكترونية؟ هل تأملت بمقدار الخسارة التي يمكن أن تلحق بمفهوم النموذج الإلكترو-حكومي من جراء ذلك؟**[4]

لقد أصبحت القرصنة الإلكترونية اليوم شبح يتهدد العالم، وهاجسا أمنيا يتحدى قيام الحكومة الإلكترونية، فالأمر يستدعي ضرورة تامين البيانات والمعلومات، لبعث الثقة والأمان في التعامل، في البيئة الرقمية المفتوحة التي نعيشها اليوم، والتي تُعدَّ المعلومات من أهم ركائزها ومقوماتها. **فكيف يمكن حماية الأمن المعلوماتي للحكومة من خطر القرصنة حينما يتم الانتقال بها إلى الفضاء الإكتروني؟**

ويتفرع عن هذه الإشكالية الرئيسية جملة من التساؤلات الفرعية، يذكر من بينها:

- ما المقصود بالأمن المعلوماتي للحكومة الإلكترونية؟ وما هي عناصره؟

- ما هي القرصنة؟ وما مدى خطورتها على أمن الحكومة الإلكترونية عموما والحكومات العربية خصوصا؟

- ما هي التقنيات والأساليب الحديثة في مكافحة القرصنة؟

وللإجابة على الإشكالية الرئيسية وتساؤلاتها الفرعية، سوف يتم تقسيم هذه الدراسة إلى ثلاثة محاور أساسية:

أولا: مفهوم الأمن المعلوماتي للحكومة الإلكترونية.

ثانيا: تأثير القرصنة على الأمن المعلوماتي للحكومة الإلكترونية.

ثالثا: وسائل حماية الأمن المعلوماتي للحكومة الإلكترونية من خطر القرصنة.

أولا: مفهوم الأمن المعلوماتي للحكومة الإلكترونية:

يقتضي تحديد مفهوم الأمن المعلوماتي للحكومة الإلكترونية، تحديد تعريفه وتبيين عناصره هذا من جهة، ودراسة مدى أهميته من جهة أخرى، وذلك على النحو التالي:

1.تعريف الأمن المعلوماتي:

يقصد **بأمن المعلومات** من زاوية أكاديمية، العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها. ومن زاوية تقنية، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات، ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية، التي تستهدف المعلومات ونظمها.[5]

أما **المعلومات** فما هي سوى حقائق وأفكار، يتبادلها الناس في حياتهم العادية عبر وسائل الاتصال المختلفة، ومن خلال مراكز ونظم المعلومات المختلفة في المجتمع والإنسان. فالمعلومة هي إذن تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير. وتتطلب المعلومة بطبيعتها وجود وسط تخزن فيه.[6]

ومن خلال التعريف السابق، نجد أن **عناصر الأمن المعلوماتي** تتلخص في توفير أمن العناصر الأربعة التالية:

أ.السرية أو الموثوقية: *Confidentialité*

وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

ب. التكاملية وسلامة المحتوى: Intégrité

أي انه لابد من التأكد من أن المحتوى لم يتم العبث به؛ أي انه لم يتم تدمير أي جزء من أجزاءه في أي مرحلة من مراحله، عن طريق القرصنة أو الدخول غير المشروع عليه، من أي من العابثين الذين يقومون بالدخول إلى محتوى المعلومات لتدميره سواء كان تدمير كلي أو جزئي.[7]

ج. استمرارية توفر المعلومات أو الخدمة : Availability

ويقصد بها عملية التأكد من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وان مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.

د.عدم إنكار التصرف المرتبط بالمعلومات: Non Répudiation

أي ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها، إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين. بمعنى أنه يتوجب عدم إنكار العميل أن التصرف الذي أجراه على الموقع، كطلب الشراء، قد صدر عنه، أو إنكار الموقع نفسه أنه تعاقد مع العميل في شان ما.[8]

2. أهمية حماية الأمن المعلوماتي للحكومة الإلكترونية:

تشتمل أنظمة الحكومة الإلكترونية على كميات ضخمة من المعلومات، منها ما هو العام والمتاح للجمهور، ومنها ما هو الخاص بالحكومة وحدها، ومنها ما هو خاص بالمواطن الواحد أو المؤسسة الواحدة. وتتدرج الحراجة الأمنية لتلك المعلومات عبر مستويات عدة، تبدأ بمستوى "دون الحرج" إلى مستوى "الحراجة القصوى". وينبغي اتخاذ التدابير الاحترازية حسب مستويات الحراجة، وعدم المبالغة في حماية الأصول العامة الخاصة بالجمهور، وبالتالي فقدان الشفافية الحكومية، وعدم الاستهتار بالأصول الحرجة وتعريض أمن البلاد الإلكتروني للخطر. ويوضح المخطط التالي هرم حراجة المعلومات في الحكومة الإلكترونية:

ونستطيع أن نسرد بعض الأصول المعلوماتية الحرجة فيما يلي:

- خطط الدولة وملفاتها الأمنية والمخابراتية؛
- تشكيلات الدولة العسكرية وكيفية تسليح جيشها؛
- أجندات الحكومة السياسية ومحاضر اجتماعاتها؛
- ملفات المواطنين الصحية، القضائية، الأمنية....الخ؛
- الملفات القضائية والجنائية؛ وملفات المؤسسات التجارية وبياناتها المالية والاقتصادية؛
- قواعد بيانات الهوية الرقمية وكلمات السر وأدوات الدخول؛ وقواعد البيانات المالية والاقتصادية.

فمن الواضح إذن، أن الحكومة الإلكترونية يجب أن توازن بين درجة حراجة المعلومات وكلفة تشغيل أنظمة حماية متطورة ومعقدة، فمن غير الضروري على سبيل المثال اعتماد نفس المعايير الأمنية لحماية ملفات مخابراتية وأخرى تجارية أو صحية. وينبغي أن لا يقع مدراء الأمن الإلكتروني في فخ الهستيريا الأمنية المعلوماتية، بحيث ينسفون مبدأ الشفافية الحكومية كما ذكرنا سابقا. وعلى هذا الأساس، من الممكن أن يتم تصنيف وتجميع كافة البيانات والمعلومات والإجراءات الإلكترو-حكومية، ضمن طبقات الهرم السابق واعتماد معايير مقبولة من كافة الأطراف.[9]

ثانيا: تأثير القرصنة على الأمن المعلوماتي للحكومة الإلكترونية:

تتطلب دراسة تأثير القرصنة على الأمن المعلوماتي للحكومة الإلكترونية، تحديد مفهوم القرصنة وتاريخ نشأتها، وتبيين كيفية القيام بها، وكذا التطرق إلى وسائل وأساليب القرصنة المستخدمة في اختراق الأمن الإلكتروني والمخاطر المترتبة من جراء ذلك.

1. تحـديد تـعريف القـرصنة وتـاريخ نشـأتها:

يشير مفهوم القرصنة الإلكترونية إلى استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة، تستهدف التحايل على أنظمة المعالجة الآلية للبيانات، لكشف البيانات الحساسة (المصنفة) أو تغييرها والتأثير على سلامتها أو حتى إتلافها. [10] عبارة أخرى، القرصنة ما هي سوى عملية دخول غير مصرح به، إلى أجهزة الغير وشبكاتهم الإلكترونية؛ أي أن توجه هجمات إلى معلومات الكمبيوتر أو خدماته، بقصد المساس بالسرية أو المساس بسلامة المحتوى والتكاملية، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها. فهدف هذا النمط الإجرامي هو نظام الكمبيوتر، وبشكل خاص المعلومات المخزنة داخله. فالقرصنة إذن تعني الوصول بطريقة غير مشروعة من خلال ثغرات في نظام الحماية الخاص بالهدف. [11]

ويقوم بعملية القرصنة أشخاص هواة أو محترفين، تم تعريفهم كالتالي: "أشخاص لهم القدرة على التعامل مع أنظمة الحاسب الآلي والشبكات، بحيث تمون لهم القدرة على تخطي أي إجراءات أو أنظمة حماية، اتخذت لحماية تلك الحاسبات أو الشبكات." وهؤلاء المخترقون يتم تصنيفهم إلى نوعين: أولهما هم **الهاكرز** " *HAKERS* " وهم الأشخاص الذين لهم القدرة الفائقة على اختراق الأجهزة والشبكات، أيا كانت إجراءات وبرامج الحماية التي تم اتخاذها. إلا أنهم لا يقومون بأي من الإجراءات التي تؤدي من تم إلى الإضرار نتيجة اختراق جهازه أو شبكته. أما **الكراكز** " *CRACKERS*" فهؤلاء يطلق عليهم المخربين، وهم يتشابهون مع الهاكرز في قدرتهم الفائقة على الاختراق وتخطي إجراءات وبرامج الحماية، إلا أنهم يقومون بالعبث بالبيانات والمعلومات المخزنة على تلك الحسابات والشبكات. [12]

وتعود بداية القرصنة إلى الستينات، إذ ارتبط ظهورها مع ظهور أولى الحواسيب. إلا أن أول عملية قرصنة قد سجلت في عام 1878، بإحدى شركات الهاتف المحلية الأمريكية. ويعتبر الخبراء الفترة من 1980 إلى 1989 العصر الذهبي للقرصنة. [13]

وتجدر الإشارة إلى أن أشهر حروب النت على الإطلاق هي " حرب الهاكرز العظمى" التي دارت رحاها بين عامي 1990 و1994 بين فريقين من الهاكرز المحترفين، حيث سعى كل فريق لاختراق حواسيب الآخر. [14] ما شهد عام 2000 أول حرب إلكترونية دولية بين العرب والمسلمين ضد اليهود، وكانت نتيجتها اختراق وتعطيل الكثير من المواقع الإسرائيلية. كما شهدت الهند مصيرا مماثلا من قبل

الهاكرز الباكستانيين. وكذلك الحرب الأمريكية الصينية عام 2001، بسبب أزمة طائرة التجسس الأمريكية في الصين، والتي راح ضحيتها الكثير من المواقع والشبكات. [15] ولعل أشهر القراصنة على الإطلاق هو الأمريكي كيفن ميتنيك، الذي يُعتبر أشهر هاكر في التاريخ. وكذا قرصان أطلق على نفسه " The Menetor،" والذي قام بنشر دراسة شهيرة بعد أن تم اعتقاله، أصبحت تعرف باسم "بيان الهاكر" وهو بيان رسمي لأهداف ووجهات نظر القرصان، نشرت في المجلة الإلكترونية " Phrack." ولا تزال الدراسة تعتبر أشهر ما كتب عن قرصنة الحاسوب، وكثيرا ما تستخدم لتبين طريقة تفكير وعمل القرصان.

2. كيفية خرق الأمن المعلوماتي للحكومة الإلكترونية عن طريق القرصنة:

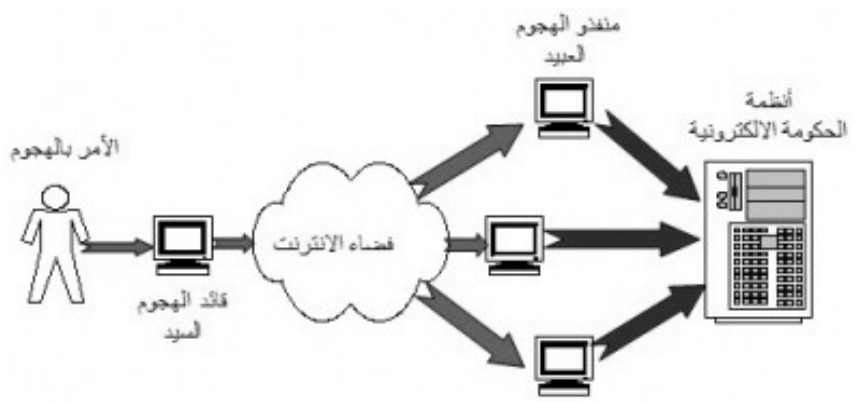
لمحاولة خرق الأمن المعلوماتي للحكومة الإلكترونية، تستخدم معظم برامج القرصنة أو الاختراق نوعين من الملفات الأول يسمى " CLIENT.EXE "، والثاني ".SERVER.EXE " وكلاهما يندرجان تحت اسم " TROJAN." حيث يعمل الملف الأول على فتح ثغرة " PORT " في الحاسب المستهدف، ليمكن الملف الثاني من الدخول إلى الحاسب من خلال هذه الثغرة. والمقصود بالثغرة هنا كل برنامج اختراق يعتمد على رقم منفذ خاص به، حيث أن برنامج " NET BUS" على سبيل المثال، يستخدم المنفذ (1 2 3 4 5) للدخول من خلاله. وعليه فإن عملية الاختراق مبنية على فكرة السيطرة عن بعد، وهذه العملية لا تتم إلا من خلال الملفين المذكورين آنفا. [16]

والحقيقة أن هناك طرق شائعة في إجراء عملية القرصنة، لخرق امن الحكومة الإلكترونية، من اشهرها: القرصنة باستخدام ملفات "**أحصنة طروادة**" "Trojan Horses Program،" ويتم بإرسال برنامج التجسس هذا من قبل المستفيد إلى جهاز الضحية، ليكون حلقة الوصل بين جهاز الضحية والمخترق أو المستفيد. ويتم إرسال هذا البرنامج بأكثر من طريقة، منها البريد الإلكتروني؛ حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر. كما قد يرسل عن طريق برنامج المحادثة أو الدردشة، أو عن طريق إنزال بعض البرامج من أحد المواقع غير الموثوق بها. وبمجرد زرع برنامج التجسس، يقوم بفتح منفذ الاتصال أو بوابة داخل الجهاز المصاب، وهذا المنفذ يمكن المستفيد من الاختراق بواسطة برامج متخصصة. [17]

ويعتبر برنامج حصان طروادة من البرامج الخطرة على الإطلاق، التي تستخدم في عمليات القرصنة واختراق أجهزة الحاسبات الآلية، نظرا لتمتعه بعدة مميزات تجعل منه الأقدر على عملية الاختراق، دون القدرة على كشفه وتتبعه والقضاء عليه، لذلك فقد اكتسب هذا البرنامج شهرة كبيرة في مجال اختراق أجهزة الحاسبات الآلية. وقد صمم هذا البرنامج في البداية بغرض حسن ومفيد، وهو معرفة ما يقوم به الأبناء على جهاز الكمبيوتر في غياب الوالدين، أو معرفة ما يقوم به الموظفين على

جهاز الكمبيوتر في غياب المدراء، إلا أنه تم تطوير هذا البرنامج بعد ذلك تطويرا سيئا. وتكمن خطورة برنامج حصان طروادة في كونه يتيح للمخترق أن يحصل على كلمة سر الدخول على الجهاز؛ بمعنى أنه يتيح للدخيل أن يتمكن من الدخول على الجهاز بطريقة لا تثير أي ريبة أو شك، فلا يستطيع صاحب الجهاز من ملاحظة وجود دخيل يتمكن من الدخول على جهازه في غيبته. [18]

وتكمن خطورة القرصنة أكثر عندما لا تستطيع أجهزة الأمن الإلكتروني اكتشاف مصدر الاختراق أو القرصنة، وهو ما يطلق عليه عادة باسم **الهجوم السيد**، وهو ما يوضحه المخطط التالي:



يقوم هذا النوع من الهجوم الإلكتروني على مبدأ توزيع الأدوار بين البرنامج قائد الهجوم (Master Attacker) والبرامج المنفذة للهجوم *(Slave Attackers)*؛ إذ يقوم الشخص الآمر بالهجوم بإعداد برنامج رئيسي يرسل إشارة الهجوم لبرامج فرعية، موجودة على العديد من الأنظمة المربوطة بالإنترنت؛ بحيث يظهر لوحدات الأمن الإلكتروني في الدولة بأن الهجوم صادر من نقاط تواجد الأنظمة الفرعية، في حين أن الهجوم الإلكتروني الفعلي يكون قد تم عبر البرنامج الرئيس وبإشارة من الشخص المسؤول. ولسوء الحظ لن تتمكن أجهزة الأمن الإلكتروني من تعقب المهاجم الفعلي، الذي يكون قد قام بعملية تضليل إلكترونية قد توقع الحكومة الإلكترونية في فخ اتهام أشخاص غير معنيين كلياً بالهجوم، بل كانوا أيضا جزء من الضحية. وعلى سبيل المثال فقد يعمد إرهابيو المعلومات إلى زرع أنظمة الهجوم الفرعية (العبيد) في مقاهي الإنترنت في الدولة، ويقومون بإيقاظها من أمكنة جغرافية متباعدة كلياً، وحين يتم تعقب مصادر الهجوم فسوف تصل أجهزة الأمن إلى تلك المقاهي وتنقطع الحلقة تمام [19]

3. وسائل وأساليب القرصنة في خرق الأمن المعلوماتي:

تتعدد وسائل وأساليب القرصنة في اختراق الأمن المعلوماتي للمواقع الإلكترونية، إلا أنها في مجملها تهدف إلى مهاجمة هذه المواقع وتحقيق نفع معين للمهاجم من وراء ذلك، وفي بعض الأحيان لا يكون هناك نفع للمهاجم سوى تعريض الموقع الضحية للخطر والضرر. ومن أهم هذه الأساليب والطرق ما يلي:

أ. الفيروسات: "*virus* "

الفيروسات هي إحدى أنواع البرامج الآلية، إلا أن الأوامر المكتوبة في هذه البرامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته. [20] (24) فهي برامج قد تم تصميمها لإلحاق الضرر بنظام الحاسب، عن طريق ربط نفسه بالبرامج الأخرى، وكذلك القدرة على إعادة تكرار نفسه؛ بحيث يتوالد ويتكاثر؛ مما يتيح له فرصة الانتشار داخل جهاز الحاسب في أكثر من مكان في الذاكرة؛ ليدمر البرامج والبيانات الموجودة في ذاكرة الجهاز. (25) [21] وتكمن خطورة الإصابة بالفيروس في أنه يؤدي إلى تعطيل عمل البرامج أو تقليل سرعته، أو إصابة الجزء الخاص بتشغيل جهاز الكمبيوتر، مما يؤدي إلى إيقاف عمل الجهاز، أو قد يؤدي الفيروس إلى مسح منطقة جدول التقسيم، وهو ذلك الفهرس الذي يحتوي على أسماء الملفات وأماكن وجودها على القرص الصلب [22] (26)

ويتكون برنامج الفيروس بشكل عام من أربعة أجزاء رئيسة هي:

- **آلية التكرار:** وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه؛

- **آلية التخفي:** وهو الجزء الذي يجعل الفيروس قادراً على الاختفاء، ويمكن أن يتضمن تشفيراً لمنع البرامج الماسحة التي تبحث عن نموذج الفيروس من اكتشافه؛

- **آلية التنشيط:** وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يتمكن المستثمر من تحديد مكانه ومسحه، كاستخدام ساعة توقيت الساعة في الكمبيوتر، أو الانتظار لتنفيذ برنامج ما عدداً معيناً من المرات؛

- **آلية التنفيذ:** وهو الجزء الذي ينفذ الفيروس عندما يتم تنشيطه، ويكون مجرد رسالة على الشاشة أو مسح بعض الملفات. [23] (27)

وتجدر الإشارة إلى أنه توجد العديد من أنواع الفيروسات كفيروسات **"الديدان"** " *Worms* " وهي عبارة عن برنامج صغير، يستخدم شبكة الحاسب الآلي والثغرات الأمنية لبعض البرامج والتطبيقات، وعندما يجد هذه الثغرة يقوم باستنساخ نفسه في ذلك الجهاز. [24] (28)فهذه الديدان لها خاصية سرعة الانتشار والتوالد وصعوبة التخلص منها، نظرا لقدرتها الفائقة على التلون

والتناسخ والمراوغة.[25] وكذا فيروسات **"حصان طروادة"** "*Trojan horse*" وهي برامج توحي للمستخدم بأنها تقوم بعمل معين بينما هي في حقيقة الأمر تقوم بعمل آخر، وتكون ضارة على الأغلب. وتتميز عن الفيروسات بكونها غير قادرة على إنتاج واستنساخ نفسها؛[26] إذ تقوم بعمل واحد هو إتلاف القرص الصلب أو فتح بعض المنافذ، للسماح للمخترقين بالتحكم في الجهاز الصلب أو سرقة البيانات منه.[27]

ب. الإغـراق بالـرسـائل:

يقصد بطريقة الإغراق بالبريد الإلكتروني تلك الطريقة التي تعني إرسال كم هائل من الرسائل، عبر البريد الإلكتروني لأجهزة الحاسبات الآلية، المراد العمل على تعطيلها وتوقفها عن العمل. وتلك الرسائل التي لا تعني شيئا على الإطلاق قد تكون محملة بملفات كبيرة الحجم، لمجرد التأثير على الجهاز، نظرا لصغر المساحة المحددة للبريد الإلكتروني في معظم الأحيان. وتصل لجهاز الحاسب الآلي مرة واحدة، وفي وقت واحد تقريبا، مما تعمل على توقفه على العمل على الفور، نظرا لما تسببه من ملأ منافذ الاتصال وكذا ملأ قوائم الانتظار. وبمجرد توقف تلك الأجهزة عن العمل، تنقطع بالتالي الخدمة التي تؤديها تلك الأجهزة.[28]

ج. خـداع بروتوكـول الانترنت: " IP Spoofing"

ويتم ذلك بالتخفي واستغلال بروتوكولات النقل، بأن ينتحل المخترق صفة مستخدم آخر مخول بالاستخدام، ويقوم بتزوير العنوان المرفق مع حزمة البيانات المرسلة، ويظهر للنظام وبروتوكولات النقل على أنه عنوان صحيح مرسل من داخل الشبكة، وبذلك يسمح النظام لحزمة البيانات بالمرور باعتبارها حزمة مشروعة.[29]

4. مخـاطر القرصـنة على الأمـن المعلوماتي للحكومة الإلكتـرونية:

من خلال استعراض وسائل وأساليب القرصنة السابق ذكرها، يمكن تلخيص التأثيرات الضارة للقرصنة وخطورتها على الأمن المعلوماتي للحكومة الإلكترونية فيما يلي:

أ. تدمير المواقع: مثلما هو الحال عند ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص بالمعتدي إلى الموقع، كما سبق وأشرنا. وفي الواقع، هناك أسباب مساعدة للقرصنة في تدمير المواقع، منها : ضعف الكلمات السرية المستخدمة؛ حيث نجد أن بعض مستخدمي شبكة الإنترنت يجد أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمها، مما يسهل عملية كسرها أو تخمينها من قبل المخترق. ومن الأسباب أيضا عدم وضع برامج حماية كافية لحماية الموقع من الاختراق والتدمير.

ناهيك عن عدم القيام بالتحديث المستمر لنظام التشغيل، والذي يساعد في كثير من الأحيان على اكتشاف المزيد من الثغرات الأمنية.

ب. تشويه المواقع: يوجد تشابه كبير، بين ما يحصل في العالم الافتراضي من عمليات تشويه مواقع ويب " *Defacement* " وبين ما يحدث على أرض الواقع عندما يتم إنزال علم دولة معينة من السفينة، ورفع علم القراصنة مكانه؛ حيث أن عملية التشويه، في أغلب الأحيان، ليست سوى تغيير الصفحة الرئيسية للموقع بصفحة أخرى، يعلن المخترق فيها انتصاره على نظام مزود ويب والإجراءات الأمنية للشبكة. ويقصد من ورائها إبراز قدراته التقنية، وإعلان تحدّيه للمشرفين على نظم مزودات ويب. وتتضمن الصفحة الجديدة أحياناً، رسالة يرغب الشخص الذي قام بعملية التشويه إيصالها للعالم. وقد تتضمن هذه الرسالة اعتراضاً منه على حالة سياسية أو اجتماعية، أو صرخة يريد إيصالها، إلى كل من يزور هذا الموقع! [30]

ج. العبث بالبيانات: وذلك بتغيير البيانات أو إنشاء بيانات وهمية، في مراحل الإدخال أو الإخراج أو التخزين. [31]

د. الأخطار المادية للقرصنة: يترتب على القرصنة خسائر مادية جسيمة تتكبدها الحكومات الإلكترونية، فقد قدرت على سبيل المثال إحدى شركات أمن المعلومات الأمريكية أن دقيقة واحدة يقضيها المتسلل في نظام ما، تؤدي إلى استدعاء خبير أمن يقضي 34 ساعة على الأقل لسد الثغرة التي دخل منها المتسلل، وإصلاح الأعطال التي أحدثها، مما يكلف ما لا يقل عن 22 ألف دولار أمريكي. [32]

ثالثا. وسائل حماية الأمن المعلوماتي للحكومة الإلكترونية من خطر القرصنة:

تتعدد وتتنوع الوسائل التي تستخدمها الحكومة الإلكترونية لحماية أمنها المعلوماتي، من وسائل تأمين بشرية وتقنية وتكنولوجية، وأخرى قانونية وأمنية وتوعوية.

1. وسائل التامين البشرية والتقنية والتكنولوجية لحماية أمن الحكومة الإلكترونية:

وتتمثل فيما يلي:

أ.تامين العنصر البشري:

تبدأ عمليات تامين المعلومات في الحكومة الإلكترونية، بالعنصر البشري، واضحة في عناصر المراقبة، فيتم التحري عن الأفراد العاملين فيها واستمرار متابعتهم وضمان ولائهم للمؤسسة التي يعملون بها، وضمان عدم إغرائهم، وذلك لضمان سرية المعلومات التي يعملون عليها، على أن لا يتم من خلالهم تبادل أي نوع من المعلومات، بل يتم إبلاغهم فقط عن المعلومات من خلال رئاستهم المباشرة في العمل، ويعطى للمرؤوسين الجزء الخاص بهم من هذه المعلومات. [33] كما أنه يمكن تامين

العنصر البشري باستخدام مجموعة من الوسائل المتعلقة بتعريف شخص المستخدم، وموثوقية الاستخدام ومشروعيته، وهي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة، من قبل الشخص المخول بهذا الاستخدام "*Identification et Authentification*". وتضم هذه الوسائل البطاقات الذكية المستخدمة للتعريف ووسائل التعريف البيولوجية، التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي.[34] إذ تستطيع هذه التقنيات الأمنية المعتمدة على **التحقق الحيوي أو البيولوجي** "*Biometrics* " تسجيل معلومات عن بصمات الأصابع، والوجوه، والأصوات، وقزحية وشبكية العين، والتوقيع اليدوي، وغيرها من الخصائص الفيزيائية، وأن تعمل كحارس لنظام معين، وتسمح بمرورك من بوابة معينة، أو أن تمنعك من المرور، بناء على انطباق خصائصك الفيزيائية مع المعلومات المخزنة في قاعدة البيانات.[35] لهذا نجد أن نظم المعلومات في وسائل المقاييس الحيوية تعتبر وسيلة سريعة ودقيقة.

هذا إضافة إلى استخدام **كلمات السر** بأنواعها، ويستحسن أن تكون كلمات المرور معقدة وديناميكية: إذ من الضروري أن تكون كلمات السر تطابق الحد الأدنى لمواصفات الأمن والسرية، بحيث تكون طويلة كفاية، ولا تستخدم الكلمات المفتاحية، أو أسماء العلم أو الحيوانات، أو الكلمات التي يحتمل وجودها في معاجم اللغة، ويمكن زيادة تعقيد هذه الكلمات بجعلها تتغير اوتوماتيكياً مع مرور الوقت عليها.[36]

ب. وسـائل التـامين الـفنية والتكنـولوجية:

توازن الوسائل الفنية والتكنولوجية بين التقليل من خطر القرصنة والخسائر المترتبة على هذه الاختراقات، وبين المعلومات المراد حمايتها وأهميتها وتكلفة هذه الحماية. ومن الوسائل الفنية لهذه الحماية:

- جـدران النـار:

الجدران النارية هي مجرد أدوات بسيطة تعمل كمنفذ للأنترنث؛ بكلمات أخرى كحراس على طرف الشبكة. وقد تم استخدام أولى الجدران النارية لتحقيق الأمن في أوائل التسعينات.[37] وعلى الرغم من أن جدران النار لا تعد علاجا لجميع أمن المعلومات مع شبكة الانترنت، إلا أنها ضرورية لأي استراتيجية متبعة، فهي حاجز بين شبكتين. إذ تقوم برمجيات جدران النار بفحص رزم البيانات القادمة والخارجة، اعتمادا على مجموعة القواعد التي يضعها المشرف على الشبكة، للسماح لهذه الرزم بالمرور، أو لحجبها ومنعها من الوصول إلى الشبكة الموثوقة الداخلية.[38]

- محـاكاة أسـاليب الهجـوم الإلـكتروني:

يسمى هذا الأسلوب في بعض الأحيان بالمناورات الأمنية الإلكترونية، وتعمل خلالها أجهزة الأمن الإلكتروني على القيام بهجوم تجريبي غير ضار على أنظمة إدارات الدولة المختلفة، للتحقق من صلابتها ومقاومتها. وقد يتم هذا الهجوم بدون سابق إنذار للتأكد من فعالية أجهزة الحماية، ومستوى تطبيق الإدارات الحكومية لمعايير الأمن الإلكتروني.[39]

- تشفير المعلومات المنقولة والمحفوظة: [40]

لا يمكن غض النظر عن أمن وسرية المعلومات، التي تنتقل من طرف إلى آخر عبر شبكة الانترنت، وتركها عرضة لعيون المتنصتين والقراصنة، فمن الواجب اعتماد تقنيات تشفير ***"Cryptage"*** عالية؛ بحيث تظهر تلك المعلومات بصورة مبهمة تماماً لكل من يحاول التنصت عليها عبر الشبكة السلكية أو اللاسلكية، وينبغي اتخاذ نفس الإجراءات بالنسبة للمعلومات الحساسة المحفوظة في الأجهزة، بحيث يتم حفظها وهي مشفرة ويعد التشفير من وسائل حفظ سرية المعلومات في نطاق الأنظمة الإلكترونية، لا سيما في الحكومة الإلكترونية وتطبيقاتها. ويهدف التشفير إلى منع الغير من التقاط الرسائل أو المعلومات، ومن تم منع وصولها أو وصولها مشوهة إلى الطرف الآخر.[41]

وتعتمد تكنولوجيا التشفير الحديثة على النظرية التالية: تمتلك كل جهة أو فرد مفتاحين لتشفير وفك تشفير البيانات: المفتاح الأول وهو المفتاح الخاص، ويكون فقط بحوزة الجهة المخولة. والمفتاح الثاني وهو المفتاح العام، ويتم نشره على الانترنت أو على شبكة الحكومة الإلكترونية، من أجل استخدامه من قبل الجهات الأخرى لتشفير الملفات والمعلومات المراد إيصالها إلى الطرف الآخر. فعلى سبيل المثال، من أجل تشفير المعلومات المرسلة من قبل المواطن إلى دائرة الآليات من أجل تسجيل سيارته، فإن المواطن يستخدم المفتاح العام الخاص بدائرة الآليات لتشفير المعلومات قبل إرسالها، وتستخدم الدائرة مفتاحها الخاص لفك تشفير المعلومات بعد استقبالها.[42]

- استخدام برامج متخصصة ضد القرصنة:

توجد العديد من البرامج المستخدمة لمنع القرصنة؛ كتزويد قاعدة البيانات بعدد كبير من أسماء **أحصنة طروادة**؛ حيث يتم عمل مسح كامل لكافة الملفات الموجودة بجهاز المستخدم، ومطابقتها مع الموجود بقاعدة البيانات تلك للتعرف على الملفات المطابقة.[43] وكذا استخدام **طريقة طبق العسل**؛ وذلك لخداع القراصنة والإيقاع بهم، عن طريق توجيه المخترق أو القرصان إلى نظام معلومات ليس ذي أهمية ومتصل بأجهزة الأمن والتنبيه، وهذا النظام معمول به في نظم المعلومات العسكرية.[44] بالإضافة إلى استخدام **برامج خاصة لمكافحة الفيروسات**؛ وذلك من خلال فحصها للبريد الإلكتروني القادم، وكذا محافظتها على قواعد البيانات، كما تراقب البرامج الموجودة بالشبكة والقادمة إليها، كما تقوم أيضا بحجب البرامج سيئة السلوك وتسمح للبقية بالمرور.[45]

2. وسـائـل الحـمـاية الأمنية والقـانونية:

تتمثل وسائل الحماية الأمنية والقانونية أساسا في ضرورة **تطوير اتفاقيات الحكومة الإلكترونية الأمنية الدولية**؛ إذ لا يوجد دولة في العالم لا تملك اتفاقات أمنية ثنائية أو جماعية مع الدول الخارجية، ومن المفيد أن يتم تطوير تلك الاتفاقات الأمنية، لكي تشمل قضايا ومواضيع الأمن الإلكتروني وأوجه التعاون المحتملة. وعلى سبيل المثال: قد تتعاون حكومة دولة ما مع حكومات خارجية، لمنع الاعتداء الإلكتروني الصادر من أراضي تلك الدول وعبر شبكاتها. وفي المقابل، من الممكن أن يتم تبادل الخبرات الأمنية الإلكترونية مع تلك الحكومات. كما ينبغي على الحكومة أن تضع **العقوبات الرادعة لمرتكبي جريمة القرصنة**؛ بحيث تقوم بإرهابهم قبل أن يفكروا بإرهابها، ومحاولة الاعتداء إلكترونياً عليها، وفي هذا المجال سيأتي الدور الحيوي للهيئات التشريعية في الدولة من أجل سن القوانين الرادعة المناسبة.

3. وسـائل الحـماية التـوعوية:

لا يمكن اعتماد سياسات الدفاع الإلكترونية المذكورة سابقا، لتجنب الأخطار الناتجة عن القرصنة، من دون وعي كامل وشامل لهذا الموضوع الخطير. إذ من المهم، بل من الضروري، أن تقوم الحكومة الإلكترونية بحملة توعية عامة حول أمن البلاد الإلكتروني، تشمل رأس الدولة وصولاً إلى موظفيها وجمهور المواطنين، وتشرح لهم المخاطر الأمنية الإلكترونية وكيفية تفاديها، وما هي الإجراءات التي قامت بها الحكومة في هذا المجال. كما من الممكن إصدار نشرة إعلامية (مجلة، جريدة،.....) شهرية خاصة بهذا الموضوع.

ولما كان موضوع الأمن الإلكتروني يمس أمن البلاد بشكل عام، فمن المهم أن تقوم الحكومة بإجراءات وقائية تتناسب مع ذلك الموضوع، منها ما هو على المستوى التنظيمي والهيكلي؛ كعدم إعطاء مسؤولية الأمن الإلكتروني لمجموعة من الأشخاص داخل الدولة كجزء إضافي من مهامهم. وكذا ضرورة إنشاء تشكيلات خاصة بالأمن الإلكتروني، قد تكون تابعة لأجهزة الدولة الأمنية؛ بحيث يكون تطوير الأمن الإلكتروني ورسم سياسات الدفاع والهجوم الإلكتروني في صلب مهامها. وقد نذكر على سبيل المثال إنشاء الحكومة لوحدة الأمن الإلكتروني، أو وحدة للرقابة الأمنية الإلكترونية تتكفل بالتأكد من أن جميع إدارات الدولة تقوم بتنفيذ إجراءات الوقاية الأمنية، المقررة والمرسومة من قبل الدولة.[46]

خـاتـمة:

لا يمكن لأي مشروع حكومة إلكترونية أن يزدهر وينجح بدون معالجة الأخطار المطروحة والجوانب المحيطة بها ، وربما من الأفضل للحكومة البقاء في فضائها المادي والواقعي وعدم الشروع

بدخول الفضاء الإلكترو-حكومي، في حال لم تتسلح بأدوات الدفاع الإلكتروني المناسبة. ذلك أن الحاسب الآمن 100 % هو الحاسب المغلق غير المتصل بالشبكة، الموضوع في خزينة تيتانيوم، مدفونة في قبو خرساني بقاع البحر، محاط بمجموعة من الحراس مدفوع لهم بسخاء؛ أي أن الكمبيوتر الآمن على نحو مطلق هو فقط الكمبيوتر الذي لم يوصل بعد بمصدر الكهرباء، وما يزال داخل الصندوق، لم يستعمل بعد. وبالتالي فإن الأمر يستدعي بحق الاهتمام بالأمن المعلوماتي لقيام حكومة إلكترونية على أسس متينة وقوية.

ولا تزال هناك عقبات كثيرة تعيق تحقيق الأمن المعلوماتي العربي، بما فيها الجزائري، ومن تم قيام الحكومات الإلكترونية العربية، يذكر منها: نقص الكفاءات العلمية، وكذلك عدم الثقة بشركات الحماية، والخوف من أن تقوم تلك الشركات نفسها بتسريب المعلومات التي تقوم بحمايتها. ومن الطريف أن بعض شركات الحماية ذاتها تتعرّض لما يسمى بالقرصنة أو الإرهاب المعلوماتي.

ورغم أن تقنيات الاتصالات باتت في متناول أغلب الدول العربية،إلا أنها لا تزال تفتقر إلى الحماية الذاتية، فهي دائماً تستعين بالشركات الأجنبية من أجل توفير سبل الحماية كالجدار الناري مثلاً. إلا أنه لم يتوفر بعد لدينا نحن العرب ما نخاف عليه على الشبكة العالمية من معلومات إلا القليل، فأسرار التكنولوجية العربية في الصناعات الثقيلة، سواء المدنية أو العسكرية، ليست هدفاً لدى قراصنة المعلوماتية لسبب بسيط هو أنه لا نملك هذه التكنولوجية، فنحن لا نملك أسلحة التدمير الشامل التي من شأنها أن تكون أسرارها هدفاً.[47]

إن الأمن المعلوماتي العربي ضرورة ملحة يفرضها الواقع لقيام حكومات إلكترونية عربية، ونحن نعترف أننا لم نصل بعد إلى المستوى الأمني المطلوب، إما للتكلفة الباهظة التي يتطلبها نظام الحماية وإما لقلة الخبرات والكفاءات في هذا المجال. إلا أنه إذا لم يكن لدينا ما نخفيه أو نخاف عليه، فلا يعني ذلك أننا لا نحتاج إلى الأمن المعلوماتي، فنحن نتقدم بخطوات واسعة في مجال المعلوماتية، ولا شك أننا بحاجة إلى حماية ما لدينا من مخاطر القرصنة أو الإرهاب المعلوماتي.

هوامش:

1 - نهلا عبد القادر المومني، **الجرائم المعلوماتية**، الأردن، دار الثقافة للنشر والتوزيع، 2008، ص 13.

2- حسن مظفر الرزّو، **الأطر المستقبلية لإعداد ملاكات الأمن المعلوماتي**، الألوكة،2009/04/6، /http://www.alukah.net/Culture/0/5426

3- **مواجهة أضرار القرصنة الإلكترونية**، جريدة المساء، الجزائر، 2009/12/12.

4- **المخاطر الالكترونية المحيطة بالحكومة**، مركز دراسات الحكومة الإلكترونية، لبنان، 25 ماي 2009، http://www.egovconcepts.com/channels/security/48-2009-05-25-09-54-07.html

5 - خالد ممدوح إبراهيم، **امن المعلومات الإلكترونية**، الإسكندرية، الدار الجامعية، 2008، ص 27.

6- يتوجب التفرقة بين **المعلومات والبيانات**، فالبيانات تعبر عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام، التي لا علاقة بين بعضها البعض. أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات. فالبيانات " *Data* " هي **المدخلات *In Put*** *إلى* جهاز الكمبيوتر بهدف تشغيلها، ومعالجتها داخل الجهاز والحصول على **المخرجات *Out Put*** في صورة معلومات ***Informations*** . أنظر: خالد ممدوح إبراهيم، **أمن الجريمة الإلكترونية**، الإسكندرية، الدار الجامعية، 2008، ص ص 28، 29.

7 - منير محمد الجنبيهي، ممدوح محمد الجنبيهي، **أمن المعلومات الإلكترونية**، الإسكندرية، دار الفكر الجامعي، 2006، ص .13

8- صفية أحمد أبو بكر، **استخدام *Ipsec* كوسيلة لحماية الشبكات من الهجمات الفعالة**، المؤتمر الدولي حول أمن المعلومات " نحو تعامل رقمي آمن"، مسقط، 2005، ص 216.

9- **الأصول الحكومية المعلوماتية الحرجة**، مركز دراسات الحكومة الإلكترونية، لبنان، 2009، *http://www.egovconcepts.com/channels/security/93-2009-06-07-16-08-32.html*

10- **القرصنة ثمن باهظ يدفعة مستخدمو الانترنت**، إيلاف، 24 /2009/09، *#http://www.elaph.com/Web/Technology/2009/9/486426.htm*

11- جميل زكريا محمود، **ورقة في الجريمة المعلوماتية وأساليب التامين**، المؤتمر الدولي لأمن المعلومات الإلكترونية: "معا نحو تعامل رقمي آمن،" سلطنة عمان، 2005، ص147.

12 - منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق، ص .28

13- **القرصنة الإلكترونية.. مفهوم له تاريخ**، الفريق العربي للأمن والحماية المعلوماتية، 2009، *http://www.atsdp.com/forums/909-a.html*

14- محمد محمود عمارة، **تاريخ القرصنة الإلكترونية بين العبقرية وانتهاك الخصوصية**، *مجلة الوعي الإسلامي*، الكويت، وزارة الأوقاف والشئون الإسلامية، العدد 531، 2010، *http://alwaei.com/topics/current/article_new.php?sdd=1384&issue=530*

15- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق، ص. ص.30، .31

16- نفس المرجع ، ص. ص. 33-.34

17- جميل زكريا محمود، مرجع سابق، ص. .148

18 - منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق، ص. ص. 36-.37

19- **هجوم السيد العبيد**، مركز دراسات الحكومة الإلكترونية، لبنان، 2009، *http://www.egovconcepts.com/channels/security/94-2009-06-07-16-13-13.htm*

20- نادية أمين محمد علي، **الفيروسات وطرق الوقاية منها كأمن البيانات**، المؤتمر الدولي لأمن المعلومات الإلكترونية: معا نحو تعامل رقمي آمن، سلطنة عمان، 2005، ص 200.

21 - محمد مصطفى عبد العزيز، **أمن المعلومات في وجه القرصنة.. معركة لا تنتهي**، الفريق العربي للأمن والحماية المعلوماتية، *http://www.atsdp.com/forums/195-a.html*

22- نادية أمين محمد علي، مرجع سابق، ص. 202.

23-رفعت شميس، **الأمن المعلوماتي بين القرصنة والإرهاب الإلكتروني**، موسوعة دهشة، *http://www.dahsha.com/viewarticle.php?id=5355*

24- نادية أمين محمد علي، مرجع سابق، ص. 205.

25 - منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق، ص. .61

26- رفعت شميس، مرجع سابق.

27 - نادية أمين محمد علي، مرجع سابق، ص. 205.

28 - منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق، ص. ص. 46-.47

29- صفية أحمد ابو بكر، مرجع سابق، ص. 218.

30- **القرصنة الإلكترونية**، منتدى نبض المعاني، 2010، *http://www.nabdh-alm3ani.net/nabdhat/t33913.html*

31 - صفية أحمد أبو بكر، مرجع سابق، ص. 218.

32 - نفس المرجع، ص. .215

33- جميل زكريا محمود، مرجع سابق، ص. .135

34 - خالد ممدوح إبراهيم، مرجع سابق، ص .39

35- رفعت شميس، مرجع سابق.

36- **مبادئ حماية معلومات الحكومة**، مركز دراسات الحكومة الإلكترونية، لبنان، 2009، *http://www.egovconcepts.com/channels/security/68-2009-05-26-07-03-56.html*

37- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق، ص. 65.

38 - جميل زكريا محمود، مرجع سابق، ص. .145

39- **مبادئ حماية معلومات الحكومة**، مرجع سابق.

40 - آخر ما استحدث في مجال التشفير هو **تقنية التشفير الكمي "*Quantum Cryptography*"** وهي تقنية تستخدم مبدأ من مبادئ علم الفيزياء الكمية، في عملية نقل البيانات من موقع إلى آخر بأسلوب آمن 100% ، ومثل ذلك يجعل من المستحيل على أي متنصت معرفة محتويات الرسالة المرسلة، إلا بتغير المحتوى وهذا جرس إنذار فوري.

41 - عبد الفتاح بيومي حجازي، **التجارة الإلكترونية: في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت**، الإسكندرية، دار الفكر الجامعي، 2006، ص. ص. 259، 260.

42- **مبادئ حماية معلومات الحكومة**، مرجع سابق.

43- جميل زكريا محمود، مرجع سابق، ص. 150.

44- عبد الفتاح بيومي حجازي، مرجع سابق، ص. 275.

45 - جميل زكريا محمود، مرجع سابق، ص. 147.

46- **مبادئ حماية معلومات الحكومة**، مرجع سابق.