

نموذج ماكمبر McCumber للأمن المعلوماتي (مدخل وثائقي)

McCumber model for information security
(documentary entry)

أ. بلال حجاز²
جامعة قسنطينة 2، الجزائر

د. سليمة سعدي¹
جامعة قسنطينة 2، الجزائر

تاريخ التقييم: 2020/04/20

تاريخ الإرسال: 2020/04/19

تاريخ القبول: 2020/05/25

Abstract:

المخلص:

This study aims to address the McCumber model for information security, which is one of the most important models developed to explain the elements related to information security, and this research is included in descriptive studies.

The study showed the importance of providing safety in electronic transactions, whether at the personal, institutional, and even national levels.

Keywords: Security, Risks, Information, System, McMember Model for Electronic Security.

تهدف هذه الدراسة إلى تناول نموذج ماكمبر McCumber للأمن المعلوماتي، وهو من أهم النماذج التي وضعت لشرح العناصر المتعلقة بأمن المعلومات، ويدخل هذا البحث ضمن الدراسات الوصفية.

بينت هذه الدراسة أهمية توفير الأمان في التعاملات الإلكترونية سواء على المستوى الشخصي أو المستوى المؤسسي وحتى على المستويات الوطنية.

الكلمات المفتاحية: أمن، مخاطر، معلومات، نظام، نموذج ماكمبر للأمن الإلكتروني.

saidi.salima2007@gmail.com

bilel.bib@gmail.com

¹ سليمة سعدي، جامعة عبد الحميد مهري قسنطينة 2، الجزائر.

² بلال حجاز، جامعة عبد الحميد مهري قسنطينة 2، الجزائر.

1- مقدمة

غدت المجتمعات في القرن الحادي والعشرين أسيرة لأساليب الخداع والتضليل المعلوماتي الناتج عن تطور الحاسبات الإلكترونية وتكنولوجيا المعلوماتية الحديثة خلال القرن العشرين. وهذا التطور الذي فرض على البشرية عالم جديد لم تشهده من قبل، حيث رافق سيل عارم من المعلومات الصحيحة والملففة والمضللة في وقت واحد، وانصبت كلها على العقول البشرية عبر قنوات وشبكات الاتصال المتطورة الحديثة، وترك هذا السيل العارم نتائج غير منتظرة في مختلف المجتمعات المتطورة والنامية على حد سواء. ودخلت المعلوماتية في صلب التفاعلات الاقتصادية والاجتماعية والسياسية بعمق، وغدت تمثل "ثورة معلوماتية" ثورة شاملة وضعت البشرية أمام تحديات أخطار الصراعات التي باتت تهدد الأجيال الصاعدة بعد أن أطبقت عليها الثورة المعلوماتية في الوقت الحاضر، ولا يعرف ما ينتظر الأجيال من أخطار مستقبلية. ورافقت الثورة المعلوماتية مفاهيم وقيم جديدة، وجاءت هذه الثورة بأفكار جديدة طالت جوهر الفرد وشخصيته، وبدأت تهتز معها القيم والتقاليد المتوارثة على وقع سيل المعلومات العالمية الصحيحة والملففة والمضللة والمخالفة للقوانين الوطنية المنهزمة عليه من كل حذب وصوب لأغراض تحريضية بحثة دون قيد أو حدود، وأظهرت المشكلة حالة من التنافس الفوضوي غير المتوازن بين كل ما هو إنساني وحضاري وثقافي ووطني وعالمي (البخاري محمد طشقند، 2016).

ففي تقرير صدر عن برنامج الأمم المتحدة الإنمائي عام 1999 بعنوان "عولمة ذات وجه إنساني Globalization with a Human Face" أكد التقرير على أنه على الرغم مما تقدمه العولمة من فرص هائلة للتقدم البشري في كافة المجالات، نظراً لسرعة انتقال المعرفة وانتقال التكنولوجيا الحديثة وحرية انتقال السلع والخدمات، فإنها في المقابل تقرض مخاطر هائلة على الأمن البشري في القرن الحادي والعشرين، وهذه المخاطر ستصيب الأفراد في الدول الغنية والفقيرة على حد سواء.

وسنحاول في هذا المقال إلقاء الضوء على أحد النماذج التي وضعت لشرح العناصر المتعلقة بأمن المعلومات ألا وهو نموذج ماكمبر **McCumber** للأمن المعلوماتي هو نتاج جهود العالم جون ماكمبر **McCumber** قدمها في شكل ملخص بحث عام 1991.

2- إشكالية الدراسة

في مجتمع الفضاء السيبري تحول العالم إلى بيت عنكبوت غير منظم الروابط عالم الشبكات والصفير والواحد، موصولة بطريقة افتراضية وفضائية فائقة السرعة، عالم توحدت فيه البنى التحتية المعلوماتية على المستويات الوطنية والإقليمية والدولية لتصبح بنية المعلومات كونية، عصر وصلت فيه التطورات الرئيسية كما وصفها "كاكو" في أعمدة العلم الثلاثة - المادة، الحياة، العقل - (الذرة، الـ: AND، الحاسب) إلى قمته، عصر أصبح الخيال العلمي واقعا بل أصبح من الصعب التفريق بين الواقع والخيال، واقع تغيرت فيه قواعد اللعبة السياسية عالم يتشكل ويعاد تشكيله بسرعة، عصر حروبه بلا جيوش بلا دماء استبدل الرصاص فيها بالبيانات فلم تعد الحكومات والدول فيه تخشى من بعضها بقدر خشيتها من المنظمات والأفراد والمجموعات، حيث أن العالم لم يعد يسير بالحروب أو بالطاقة أو بالمال، إنه يسير بالأحاد والأصفار الصغيرة، بالقليل من البيئات (BITS) إنها جميعا إلكترونات. هناك حرب في الخارج وهي لا تتعلق بمن يملك العتاد إنها تتعلق بمن يسيطر على المعلومات، ومما لاشك فيه أن التقنية الرقمية الحديثة قد أثرت بشكل

جذري على هوية وقيمة المعلومات، وبات من السهل اقتناء واختزال بل واختراق الأنساق المعلوماتية المختلفة، وأصبح من الممكن كسر الحواجز الأمنية التي تحمي المعلومة، خصوصاً بشكلها الرقمي الجديد،

إن هذه الوضعية التي يعيشها العالم جعلت كل الأفراد الفاعلة تتحرك كل على مستواها لإيجاد حل لهذه المعضلة مما خلق تساؤلات حول أهم التحورات والتحويلات التي طرأت على مسرح الجريمة والإجرام والكيفية التي يمكن من خلالها احتواء هذه الظاهرة أمنياً وتقنياً؟.

3- أهمية الدراسة

تكمن أهمية الدراسة من أهمية الموضوع الذي تعالجه ألا وهو أمن المعلومات الذي يكتسي أهمية كبيرة، كما تتجلى هذه الأهمية في كون هذا المجال يقوم بتأمين المعلومات وحمايتها من الأخطار التي تحيط بها، كما يقوم بتوفير الحماية والأمان للحواسيب والشبكات في الوقت الذي أصبح أمن المعلومات يلعب دوراً هاماً في حماية الأصول المعلوماتية، وبيانات المنظمات تضاعف عدد الحوادث الأمنية التي تتعرض لها المؤسسات والأغراض والحكومات، مثل تشويه المواقع، القرصنة وسرقة البيانات أو الاختراقات، وبذلك أصبح حماية وأمن المعلومات الحساسة والثمينة من أعقد الأمور التي تواجه كبار المسؤولين في القطاعات الحكومية والخاصة.

4- منهج الدراسة

نقصد بمنهج الدراسة الطريقة الموضوعية والمنطقية التي يتبعها الباحث لدراسة ظاهرة من الظواهر بغرض الإلمام بها وتحديد أسبابها ومعرفة أسبابها بقصد الوصول إلى أية نتيجة. ودون وجود منهج ينظمه يصبح البحث مجرد بيانات ومعلومات متتابعة لا يربطها منطق ولا فكر، وهي بذلك لا يمكن أن تحقق نتائج عامة يمكن تطبيقها (العابدي محمد عوض، 2005، ص 63). والمنهج المتبع في دراستنا هو المنهج الوصفي الوثائقي المعتمد على جمع المعلومات والبيانات اللازمة عن الظاهرة من المراجع والدراسات السابقة لوصف خصائصها ومميزاتها وصولاً إلى مجموعة من النتائج.

5- مدخل مفاهيمي حول الأمن والأمن المعلوماتي

1-5- مفهوم الأمن لغة واصطلاحاً

يعتبر مفهوم الأمن أحد المفاهيم التي تنتشعب دلالتها وتتسع مساحتها، ليشمل مضامين متعددة تتداخل مع شتى أنظمة الحياة، كما أن لفظ "الأمن" هو من الألفاظ ذات الدلالات الواضحة البينة، إذ تُعرف حقيقته عند النطق به، ولكن شدة وضوحه وكثرة استخدامه وكثرة تعريفاته واشتقاقاته، قد أضفت عليه شيئاً من الغموض، فاللفظ مشتق من أمن: مصدر أمن، أمن، يعيش في أمن: في طمأنينة ويُسّر، أمان، اطمئنان من بعد خوف، وقال ابن فارس: "الهمزة والميم والنون أصلان متقاربان: أحدهما الأمانة التي هي ضد الخيانة، ومعناها سكون القلب، والآخر التصديق (الحسين أحمد بن فارس بن زكريا، 1999، ص 133).

وحسب Cambridge online dictionary and thesaurus فإن مفردة الأمن تعني حماية الشخص، أو بناء أو منظمة أو دولة ضد التهديدات والجرائم من قبل دول أجنبية.

وأورد القاموس الفرنسي Larousse على الخط أن مفردة الأمن مشتقة من اللاتينية securitas، وهي تعني الوضعية أو الحالة التي يكون فيها شخص ما غير معرض أو في مأمن من أي خطر لا سيما الاعتداء الجسدي، والحوادث، السرقة أو التلف، كما أنه الشعور بالطمأنينة والأمان من الأذى (www.larousse.fr/dictionnaires/francais).

أما من الناحية الاصطلاحية، فالأمن هو حالة شعورية من الرضا النفسي الناشئ عن سيادة الحق والقانون، وضمان حقوق الفرد في المجتمع وحرية التفكير والتعبير وحفظ الكرامة الإنسانية، والتساوي في الفرص، كما يعنى الشعور الذي يسود الفرد أو الجماعة بإشباع الدوافع العضوية والنفسية، واطمئنان الجميع بزوال ما يهدده من مخاطر.

كما يعرف الأمن بأنه مجموع الجهود التي تصدر عن الفرد أو الجماعة لتحقيق حاجاتها الأساسية، أو للرد على العدوان عن كيانها ككل. إذن فهو الحالة التي يكون فيها الإنسان محمياً ضد، أو بعيداً عن خطر يهدده، أو هو إحساس يملك الإنسان بالتححرر من الخوف، كما أنه إحساس بالطمأنينة التي يشعر به الفرد، سواء بسبب غياب الأخطار التي تهدد وجوده، أو نتيجة لامتلاكه الوسائل الكفيلة بمواجهة تلك الأخطار حال ظهورها. فالأمن طمأنينة قلبية تسلم إلى السكون النفسي والرخاء القلبي، والأمانة طمأنينة والإيمان طمأنينة وتصديق وتسليم عن يقين(الزهراني هاشم بن محمد، 1425).

وفي معجم المعاني على الخط ذكر الأمن بعدة معاني منها (<http://www.almaany.com/>).

- **الأمن الداخلي:** ما يمس الوضع الداخلي بالبلاد وصيانتُه بالحفاظ على سيادة القانون.
- **الأمن الخارجي:** ما يمس حدود البلاد وحمايتها وسيادتها ضد أي اعتداء خارجي.
- **أمن الدولة:** جهاز إداري ملحق بوزارة الداخلية مهمته السهر على السلامة والأمن في البلاد.
- **الأمن العام:** النشاط الحكومي الذي يهدف إلى استقرار الأمن في البلاد.
- **الأمن القومي:** تأمين كيان الدولة والمجتمع ضد الأخطار التي تتهددها داخلياً وخارجياً وتأمين مصالحها وتهئية الظروف المناسبة اقتصادياً واجتماعياً لتحقيق التنمية الشاملة لكل فئات المجتمع.

2-5- ماهية أمن المعلومات

على ضوء التطورات المتسارعة في العالم والتي تؤثر في الإمكانيات والتقنيات المتقدمة المتاحة الرامية إلى حذف منظومات الحواسيب بغية السرقة أو تخريب المعلومات أو تدمير الحواسيب ومراكزها أدى إلى التفكير الجدي لتحديث الأساليب والإجراءات الدفاعية والوقائية وذلك تبعاً للإمكانيات المتوفرة، وهذا ما أدى إلى ظهور مجال أمن المعلومات التي سنتطرق إليه في العناصر التالية:



5-2-1- تعريف أمن المعلومات

تتعدد تعريفات أمن المعلومات وتتنوع حسب زاوية الرؤية، فمن الناحية الأكاديمية يعرف أمن المعلومات بأنه قضية تبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن الناحية التقنية، هو الوسائل والإجراءات اللازمة لتوفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن الناحية القانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهذا هو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (عرب يونس، 2011).

وتعرف توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة أمن أنظمة المعلومات بأنه "حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى أو تعديل المعلومات أثناء حفظها، معالجتها أو نقلها، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف، توثيق ومواجهة هذه التهديدات" (ألبيرتو إسكوديرو باسكال www.itrainonline.org/...Security/15_ar_mmtk_wireles).

ويغطي أمن المعلومات مجموعة الطرق والأساليب والأدوات المسؤولة عن حماية موارد نظام المعلومات وجعلها في متناول الأشخاص المصرح لهم عندما يحتاجون إليها، وحماية سلامة النظام والخدمات والمعلومات (ملفات بيانات، معرفة، رسائل...)، وضمان سلامتها من التغيير أو الإلغاء إلا من قبل الأشخاص المخولين الإداريين المسؤولين.

وعرف بأنه مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات، إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال. وهناك من عرفه بأنه مجموعة من التدابير الوقائية المستخدمة في المجالين الإداري والفني لحماية مصادر البيانات من أجهزة وبرمجيات وبيانات من التجاوزات أو التداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلسل أو الإجراءات الخاطئة المستخدمة من قبل إدارة المصادر المعلوماتية، فضلا عن إجراءات مواجهة الأخطار الناتجة عن الكوارث الطبيعية المحتملة التي تؤدي إلى فقدان بعض المصادر كلاً أو جزءاً، ومن ثم التأثير على نوع ومستوى الخدمة المقدمة (بدر أحمد أنور، 1997). كما عرف أمن المعلومات على أنه إجراءات خاصة تحول دون فقدان أو فساد البيانات أو استعمالها دون تفويض.

ومنه يمكن القول أن أمن المعلومات عبارة عن مجموع الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال الفني أو الوقائي لصيانة المعلومات وحمايتها من الدخلاء أو الاستعمال غير قانوني لها.

وهناك مصطلح آخر يستعمل كمرادف لأمن المعلومات وهو مصطلح ضمان المعلومات (Information Assurance IA) الذي يعبر عن "مجموعة الأعمال اللازمة لتأمين المعلومات وإدارة المخاطر المرتبطة باستخدام، معالجة، تخزين ونقل المعلومات، بالإضافة لتأمين الأنظمة والأجهزة المستخدمة والإجراءات اللازمة لتأمينها. كما يشير مصطلح ضمان المعلومات إلى ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزنة في أجهزة الحاسوب إضافة إلى الأجهزة

الملحقة وشبكات الاتصالات، والتصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزونة أو تلك التي ترمي إلى نقل أو تغيير أو تخريب المخزون المعلوماتي لهذه القواعد، وضمان توافر المعلومات عند اللزوم فقط للأشخاص المخولين بالوصول لها.

ويعتمد ضمان المعلومات على التقنيات والأجهزة المناسبة وأيضاً على الإجراءات الإدارية، وعلى الرغم من أن المصطلح برز في مجال المعلومات الرقمية إلا أنه يستخدم في مجال المعلومات بشكل عام سواء كانت رقمية أو غير رقمية، بكلمات أخرى، أمن المعلومات هو المصطلح الأعم والأكثر شمولاً في ما يتعلق بهذا المجال.

2-2-5 الفرق بين ضمان المعلومات وأمن المعلومات

إذا ضمان حماية المعلومات لا يتعلق فقط بتأمين المعلومات في حد ذاتها فحسب، بل بتأمين كافة الأنظمة المتعلقة بتداول المعلومات وتخزينها وتناقلها وتشارك محتوياتها، وأيضاً بالإجراءات الاستراتيجية لإدارة المخاطر المتعلقة بأمن المعلومات، بالتالي يقوم العاملون في مجال Information Assurance الواسع، بالإضافة لمواجهة الاختراقات الأمنية أو التطبيقات والبرمجيات المسيئة (كالفيروسات)، بإصدار سياسات المؤسسات المتعلقة بضمن المعلومات، كسياسة الخصوصية والمعايير ومقدار والالتزام بها، وأيضاً بإجراء التدقيق في استعدادات المؤسسة لقابلية استمرار العمل، قابلية التعافي بعد الكوارث والمقصود هنا كوارث الاختراقات الأمنية المتعلقة بالمعلومات وغيرها من المهام والأنشطة، وبالتالي يشمل العمل في مجال IA اختصاصات مختلفة كالحاسبة، كشف التزوير، علم التحقيق الجنائي، علوم الإدارة، هندسة الأنظمة وهندسة الأمان وعلم الجريمة، بالإضافة لعلوم الحاسب والشبكات الرقمية وغيرها من العلوم التقنية المتعلقة بالمعلومات ومعالجتها.

2-2-3 أهمية أمن المعلومات

لا شك أن لأمن المعلومات أهمية كبيرة، وتتجلى هذه الأهمية في كون هذا المجال يقوم بتأمين المعلومات وحمايتها من الأخطار التي تحيط بها، كما يقوم بتوفير الحماية والأمان للحواسيب والشبكات.

في الوقت الذي أصبح أمن المعلومات يلعب دوراً هاماً في حماية الأصول المعلوماتية وبيانات المنظمات، تضاعف عدد الحوادث الأمنية التي تتعرض لها المؤسسات والأغراض والحكومات، مثل تشويه المواقع، القرصنة وسرقة البيانات أو الاختراقات، وبذلك أصبح حماية وأمن المعلومات الحساسة والثمينة من أعقد الأمور التي تواجه كبار المسؤولين في القطاعات الحكومية والخاصة، ومصدر قلق كبير في كل من الحكومات وأصحاب الأعمال والمنظمات (<http://www.infosec.gov.hk/english/technical/files/overview.pdf>)

يمكننا القول إن اتساع قضية أمن المعلومات وتطور أهميتها على هذا النحو الخطير عالمياً وعربياً يعود إلى أمرين (غيطاس جمال محمد، [://studies.aljazeera.com](http://studies.aljazeera.com)):

الأول: أن أغلب دول العالم، بما فيها الدول العربية، ترفع حالياً شعار التحول إلى مجتمع المعلومات والمعرفة، وتنفذ خططا واسعة النطاق لتحويل هذا الشعار إلى واقع، وفي خضم هذه الخطط يتم إنشاء سلاسل من قواعد البيانات القومية الكبرى، كما يجري تطوير شبكات الاتصالات ونشر الإنترنت عبر خطوط الاتصالات العادية والسريعة، وتتجه الأمور لتعميم خدمات نقل

الصوت عبر بروتوكولات الإنترنت، وتنشط الدول في نشر مفاهيم وخدمات الحكومة الإلكترونية، وتصدر قوانين التوقيع الإلكتروني الذي يمهد الطريق صوب تفعيل أنشطة التجارة والأعمال الإلكترونية على نطاق واسع، وتتوسع في مبادرات توفير الحاسب لفئات المجتمع المختلفة بالمنزل والمدارس وللمهنيين، كما تتبنى عشرات من برامج التنمية المعلوماتية المتكاملة في مختلف الوزارات والهيئات والمؤسسات.

الثاني: أن تشييد بنية معلوماتية قومية واسعة المجال، وتبني التوجه نحو مجتمع المعلومات نقل المجتمع والدولة والمؤسسات إلى مرمى المخاطر، وحتم عليها مواجهة التحديات الشاملة والواسعة النطاق في أمن المعلومات. بمعنى أن تحديات أمن المعلومات في مجتمع يمتلك بنية معلوماتية واسعة يجعله يواجه تهديدات في أمن المعلومات تتسم بالشمول والاتساع وعمق التأثير وتنوع الأدوات وتعدد مصادر الهجوم وأدواته وغزارة الأهداف التي تشكل إغراء ومناطق جذب لمن يستهدفونه. هذا ويعتبر أمن المعلومات من المجالات الحيوية والمتجددة المطلوبة كثيرًا، إذ لا غنى عنه أبدًا، وقد غدا علما قائم بحد ذاته يدرس العديد من الجامعات، والمراكز التعليمية، وتمنح فيه شهادات متعددة.

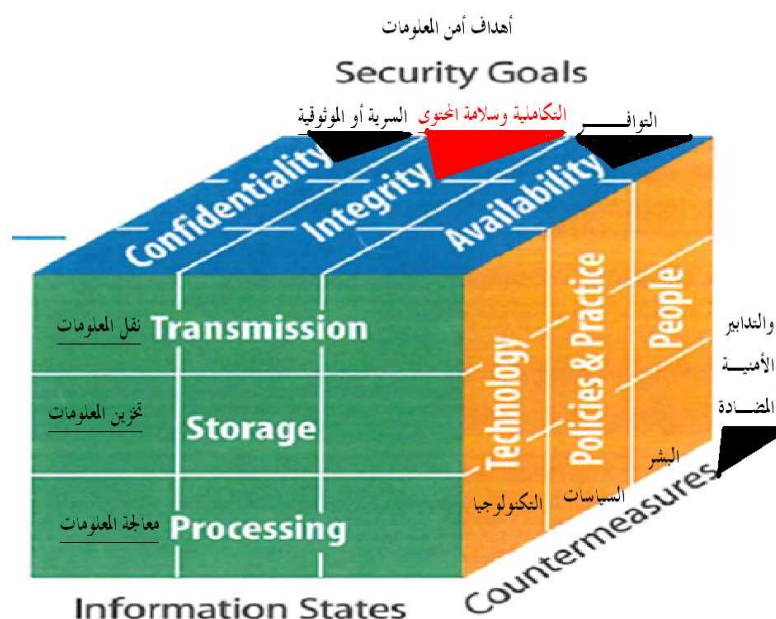
إن الأمن المعلوماتي ليس إلا مكونا من مكونات الأمن في المجتمع بشكل عام، وهو الركيزة الأساسية لتحقيق الثقة في نمو وازدهار مجتمع المعلومات. وفي إشارات واضحة إلى أهمية الأمن المعلوماتي في الفضاء الرقمي، برزت دعوات في الولايات المتحدة الأميركية إلى إسناد مهمة الدفاع عن الفضاء السيبراني الوطني إلى الوكالة الوطنية للأمن، وقد تعالت تحذيرات صدرت عن خبراء في مجال الانترنت من أن الهجوم الإرهابي القادم على الولايات المتحدة الأميركية ربما يكون من قبل قراصنة الانترنت، وجاءت هذه التحذيرات في أعقاب الهجوم الذي شنته روسيا على جميع المواقع الرسمية الجورجية على الانترنت قبل الدخول العسكري إلى أراضيها، وعليه لا يبدو الخطر على الانترنت أقل شأنًا وتأثيرًا عن الاعتداءات والهجمات التي يمكن أن تحصل في العالم المادي (<http://www.scis.gov.iq/upload/upfile/ar/security.doc>).

6- نموذج ماكمبر McCumber للأمن المعلوماتي

6-1- تعريف بنموذج ماكمبر McCumber للأمن المعلوماتي

النموذج هو نتاج جهود العالم جون ماكمبر McCumber قدمها في شكل ملخص بحث سنة 1991، وهو عبارة عن نموذج يقدم نهج منظم لتقييم وإدارة المخاطر الأمنية في أنظمة تكنولوجيا المعلومات، حيث يهدف إلى تبيان العوامل المتدخلة في تأمين المعلومات وإدارة المخاطر المرتبطة باستخدام، معالجة، تخزين ونقل المعلومات وحمايتها من الضياع أو التعديل، وضمان توافر المعلومات عند اللزوم فقط للأشخاص المخولين بالوصول لها، بالإضافة لتأمين الأنظمة والأجهزة المستخدمة والإجراءات اللازمة لحمايتها.

شكل رقم 1: نموذج ماكمبر McCumber للأمن المعلوماتي



من خلال نموذج ماكمبر McCumber للأمن المعلوماتي نلاحظ أن النموذج يركز على عدة نقاط أساسية من شأنها ضمان أمن وحماية المعلومات وأنظمتها وهي:

- ✓ الهدف من الأمن ويشمل سرية وموثوقية المعلومات، التوافر وتكاملية المحتوى؛
- ✓ التدابير الأمنية المضادة وتشمل البشر، السياسات والتكنولوجيا؛
- ✓ عناصر الأمن وتشمل أمن المعالجة أمن التخزين أمن تنقل البيانات والمعلومات.

2-6- أهداف نظام الأمن المعلومات حسب نموذج ماكمبر McCumber:

شكل رقم 2: عناصر المعلومات



إن أغراض أبحاث وإستراتيجيات ووسائل أمن المعلومات – سواء من الناحية التقنية أو الأدائية – وكذا هدف التدابير التشريعية في هذا الحقل، ضمان توفر العناصر التالية لأي معلومات يراد توفير الحماية الكافية لها.

(<http://rawabetcenter.com/archives/4545>)

السرية أو الموثوقية Confidentiality : وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

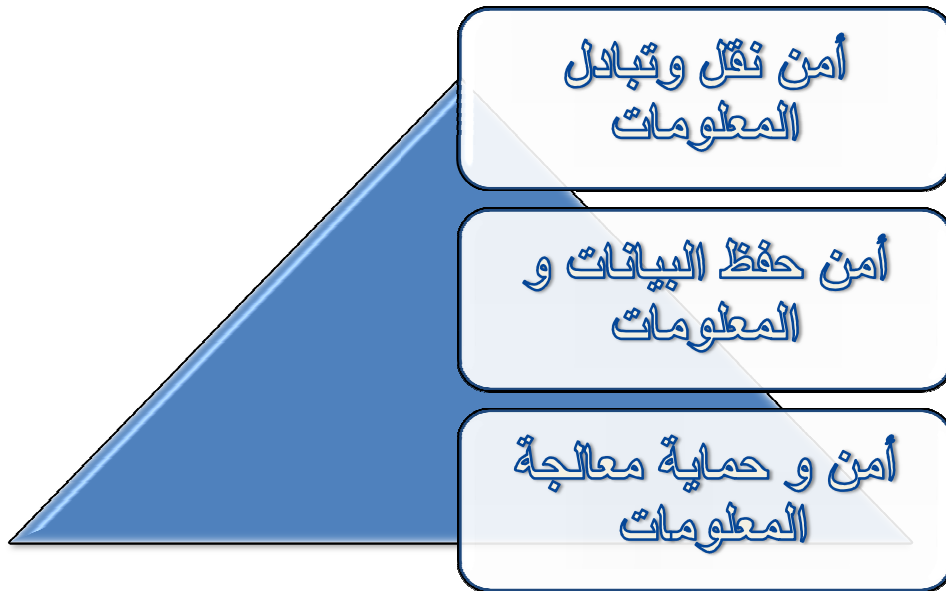
■ **التكاملية وسلامة المحتوى Integrity:** وهو التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

■ **استمرارية توفر المعلومات أو الخدمة Availability:** وهو التأكد من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها، مع عدم إنكار التصرف المرتبط بالمعلومات ممن قام به repadiatin وهو ضمان عدم إنكار الشخص الذي قام بتصريف ما متصل بالمعلومات أو مواقعها أنه الذي قام بهذا التصرف بحيث تتوفر قدرة.

6-3- مستويات الأمن المعلوماتي حسب نموذج ماكمبر McCumber:

يتم توفير الأمن للمعلومات والبيانات عبر عدة مستويات نوضحها في الشكل التالي:

شكل رقم 3: مستويات الأمن المعلوماتي



المصدر: مستويات من إعداد الباحث

* أمن حفظ البيانات والمعلومات: يهتم هذا المجال بالعديد من الآليات العلمية والعملية حول:

أمن مكان حفظ البيانات والبيئة المحيطة بها: ويتم ذلك من خلال وجودها في مواقع آمنة خاضعة لرقابة دقيقة من حيث الوصول الفيزيائي لهذه المواقع بحيث لا يصل إليه إلا من هو مصرح له من خلال البوابة الآمنة، والتي تعتمد أحياناً على التقنيات المتقدمة مثل قراءة بصمة اليد (Printfinger) (أو قزحية العين (Printeye) أو تردد الصوت أو من خلال الأرقام المتسلسلة أو البطاقات المغنطة وغيرها.

■ طريقة حفظ البيانات: ويتم ذلك من خلال التقنيات المتقدمة في أنظمة تشفير المعلومات المحفوظة (Encryptions) بمختلف أنواع التشفير التماثل أو غير التماثل سواء المعتمد دولياً أو التشفير المبتكر محلياً.

■ المواد التي تحفظ عليها البيانات: ويتم ذلك من خلال الحفظ على الأنسب من الأقراص الصلبة (HDD) الذاكرة (CASH) أو الأقراص المدمجة (CD) وغيرها من بيئات الحفظ المناسبة.

* أمن وحماية معالجة المعلومات:

تعتبر مصادر الخطر على أمن البيانات كثيرة جداً، ولعل من أهمها خطورة الوصول إلى البيانات من قبل أشخاص غير مسموح لهم بالوصول إليها، وبالتالي يتم تسريب المعلومات أو إتلافها أو تغييرها، ولهذا لا بد من الحرص على ضمان حمايتها ويتم ذلك بعدة آليات من خلال:

■ استخدام برامج الحماية الجدران النارية (Firewalls) للحماية من الاختراق للأجهزة المرتبطة فيزيائياً بشبكات، واستخدام المرشحات filters لضمان عدم نقل المعلومات غير المسموح بها، واستخدام برامج مكافحة الفيروسات (Anti-Virus) للحماية من الفيروسات المختلفة.

■ النسخ الاحتياطي (BACK UP)، وهذا يعالج مشكلة فقد البيانات الرقمية غير المكتوبة (Hard Copy) والتي تكون أكثر عرضة من غيرها للتلف أو العطب أو الفقد، ويمكننا أن نلاحظ عدة أنواع للأمن داخل النظام (سيد حسين فاروق، 1999، ص98):

✓ أمن الدخول: وهو النوع الأول من الأمن ويهتم بحماية مدخل النظام؛

✓ أمن نظام الملف: ويتمثل هذا الأمن في التحكم في الوصول إلى ملفات النظام؛

✓ أمن الحاسب الخادم: يتحكم في حماية الحاسوب الموزع.

* أمن نقل المعلومات والبيانات:

قديمًا كانت تستخدم آليات النقل الفيزيائي المباشر للبيانات، وكانت تحاط بسرية وحماية وتتم ببطء نسبي، والمتأمل حالياً يرى أن تلك الطريقة كانت أكثر أمناً من الطرق الحديثة من حيث التواصل الإلكتروني. وبعد التقدم التقني أصبحت آليات النقل الحديثة بما تميزت به من دقة وسرعة في نقل المعلومة هي الأنسب عند أخذ الاحتياطات اللازمة في عمليات نقل البيانات، ولذا نرى بأن هذا المجال يهتم بالبيانات الآمنة لنقل البيانات والمعلومات من خلال:

■ أمن نظم الاتصالات وبيئات النقل المستخدمة: ويتم عندما يكون الاتصال مباشر (direct connection) بواسطة خطوط الهاتف (Dialup) أو بالاتصال المباشر بالأقمار الصناعية (Satellite)، وذلك عندما يكون حجم البيانات متوسطاً نسبياً. وتكمن الخطورة هنا عند وجود متلصصين يقومون بعمليات التلصص (Sniffing) على خطوط الاتصال وتبرز هنا أهمية تشفير البيانات بقوة تشفير عالية والمحافظة على سلامة خط الاتصال من وجود المعترضين أو المتجسسين

■ **التطبيقات المستخدمة والبروتوكولات المناسبة:** وتتم عندما يكون الاتصال غير مباشر وفي وسيط مثل الإنترنت أو يكون نقل البيانات لموقع خدماتي عالي الأهمية الأمنية مثل البنوك أو الشراء المباشر ببطاقات الائتمان الإلكترونية، وهنا يكمن الخطر حيث يكون التجسس والاختراق من أبرز المشاكل الأمنية والتي لا يمكن القضاء عليها بشكل كامل بل يمكن الحد منها بشكل كبير عن طريق استخدام البروتوكولات الآمنة (Secure Sockets Layer) SSL أو ما يسمى بـ (HTTPS)، وتظهر أهمية التوقيعات الرقمية (PKI) والشهادات الإلكترونية للمواقع الآمنة وغيرها من وسائل الحماية.

4-6- التدابير الأمنية المضادة:

تتكون من التكنولوجيا والعمليات، والناس (Victor Maconachy).

(<http://www.ibm.com/developerworks/security/library/s-confnotes2/>)

- **العمليات:** تعتبر العمليات لا غنى عنها لأي نظام أمن، فهي جوهرية وذات طبيعة مستمرة. ويحكم أداة عمليات أمن المعلومات مجموعة من المعايير كتلك التي قررتها المنظمة الدولية للتوحيد القياسي ISO التي تعتبر ذات قيمة كبيرة لأي نظام أمن معلومات. وتطبق العمليات بطريقة منظمة كما تراجع باستمرار في إطار الخبرة المتراكمة بغية استبعاد الأخطاء والمخاطر.

- **البشر:** وهم الذين يمثلون العاملين، المستشارين، المتعاقدين، والفنيين وينجزون كل العمليات والخدمات، ويحتاج إلي تواجدهم بأعداد وتخصصات ملائمة وبمهارات وخبرات ودافعية مناسبة.

- **التكنولوجيا:** تعتبر متوافرة وجاهزة، ولمنتجاتها دورات حياة قصيرة نسبياً. وتعتبر سوق التكنولوجيا ذات طبيعة تنافسية، يتوافر لها عدد كبير من المنتجين والموردين والبائعين والموزعين الذين يأتون ويذهبون، وقد يندمجون في شركات أكبر أو قد يخسرون ويخرجون من سوق الأعمال. ويجعل ذلك من الصعب تقييم التكنولوجيا عما كانت عليه في الماضي (معراج وعبيدات، 2015).

- خاتمة

لقد كان لتطور بيئة المعلومات والاتصالات وانتشار الشبكات أثراً بالغاً في نمو التعامل الإلكتروني، وتتيح التطورات المتلاحقة والأجيال المتتالية للأجهزة والبرامج نطاقاً واسعاً ومعدلات بيانات عالية تزيد من تحسين خدمات جميع التعاملات الإلكترونية دون التقيد بالمكان والزمان، إلا أن هناك مشكلة الأمان في التعاملات الإلكترونية سواء على المستوى الشخصي أو المستوى المؤسسي وحتى على المستويات الوطنية، ومن هنا برز حتمية توفير الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات، إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال.

وعموماً يمكن القول أن الأمن المعلوماتي هو قضية جوهرية في الحياة المعاصرة تبدأ من خلال خلق وعي مجتمعي وسياسي لمهددات أمن المعلومات والاتصالات ومشاركة كل أعضاء المجتمع من الشركات التجارية ومنظمات مجتمع مدني ومؤسسات حكومية وأفراد، لبناء إستراتيجية في أمن المعلومات والاتصالات، وقد أورد الاتحاد مجموعة من التوصيات في أمن المعلومات نوردتها في ما يلي (عوض حاج علي www.profawad.info/123456)

➤ **سلامة التركيب والصيانة بطرق سليمة:** أن عدم التركيب والصيانة أن كان مقصوداً أو غير

مقصود يمثل مهدد أمني كبير، ويمكن أن يتم التواطؤ مع الجهة التي تقوم بالتركيب والصيانة لعمل اختراق أو بسبب خطأ أو ضعف في التركيب والصيانة يمكن العدو أو المنافس من عمل الاختراق الأمني الذي يريده (الاختراق الأمني هو منع جهات مأذون لها بالتعامل أو إتاحة التعامل مع جهات غير مأذون لها، إذن المطلوب أن تقوم بالصيانة أو التركيب جهات:

- مؤهلة علمياً ومهنيًا وذات خبرة
- موثوقة

كذلك المطلوب عمل العقود القوية في التركيب والصيانة ومتابعة وتنفيذ تلك العقود.

➤ استخدام الجدران النارية وكلمات السر: إن الحوائط النارية قابلة للاختراق، لذلك يجب تغييرها من وقت لآخر وفي فترات قصيرة، ومثل ذلك كلمات السر يجب تبديلها من وقت لآخر وعدم تعريفها لأي شخص آخر مهما بلغت ثقتك منه، كما يجب استخدام كلمات غير متوفرة في كلمات السر مثل (good morning,hello,sir). ويجب أن يستخدم في النظام الهوية الالكترونية أو الهوية البيولوجية إضافة لكلمة السر وهذا ما يعرف بالثنائية الأمنية.

➤ التشفير: يجب استخدام التشفير متى ما تم التعامل مع الانترنت، فعلى سبيل المثال التعامل مع الشبكات الافتراضية الخاصة (vpws) وبرنامج حماية بروتوكول الانترنت الافتراضية (IP see)، ويجب تغيير الشفرة بتكرارية عالية اعتماداً على سرية المعلومة (الشبكة الأمنية في تناقل المعلومة هي التي تستخدم شفرة جديدة مع كل رسالة (one pad key)).

إعطاء دور أوسع لمديري الشبكات: يجب أن يعلم مدير الشبكة بأنه هو المسؤول الأول والأساس من أمن الشبكة ومن ثم يتحمل هذه المسؤولية، ولا بد أن تعطى له الصلاحية والإمكانات التي يطلبها ويضع اللوائح والنظم والإجراءات الإدارية التي تمكنه من ذلك إضافة إلى المتطلبات التقنية.

استخدام استشاريين ومراجعين من الخارج: إن مراجعة إجراءات الحماية والأمنية بواسطة جهات خارجية متخصصة ضروري، ليكون ذلك رأياً آخر يؤكد على سلامة الإجراءات، كما يجب أن يكون المستشار أو المراجع مؤهلاً وموثوقاً (مراجعة خارجية).

المراجعة الدورية لإجراءات السلامة الأمنية: يجب أن تكون هنالك مراجعة دورية كل شهر أو شهرين أو ثلاثة عن مدى سلامة الإجراءات الأمنية وتحليل الاختراقات والتهديدات الأمنية. هذا بالطبع يتم بواسطة مسؤولي الأمن والحماية برئاسة مدير الشبكة داخل المؤسسة (مراجعة داخلية).

تحديد الأشخاص المخول لهم دخول غرفة المعلومات والشبكات: يجب إعطاء غرفة المعلومات والشبكات قدسيته باعتبارها المركز الرئيسي للاختراقات الأمنية، ولذا يجب تحديد أقل عدد ممكن من الأشخاص الذين يجوز لهم دخول الغرفة وكذلك المشرفين على أمنية النظام عموماً.

طلب معايير أعلى في برمجيات الأمن التجارية: يجب أن يتم اقتناء برمجيات أمنية من الشركات المؤهلة ذات الثقة العالية وذات الخبرة الطويلة في هذا المجال.

توعية وتثقيف المستخدمين (هندسة الأمن الاجتماعية): يجب أن تتم توعية وتعريف المستخدمين بالتهديدات الأمنية وعدم تضليلهم (يعني يُتوهموا بأن شكل هذه الشفرة لا يمكن كسرها وهذا النظام غير قابل للاختراق وأنه هنالك ضمان للأمن في شبكتنا كال ذلك كلام في غاية الخطورة لأنه من المعلوم في أمن المعلومات لا توجد أمنية مطلقة) إن توعية المستخدم بخطورة

ومهددت امن المعلومات والاتصالات تجعله علي بيته من أمره إذا قرر التعامل مع النظام أو غير الشبكة، فربما إذا علم ذلك ألا يتعامل مطلقاً مع الشبكة أو مع الانترنت في بعض أعماله.

تعميم الإجراءات الأمنية المذكورة على كل المؤسسات مهما صغرت: إن الإجراءات الأمنية التي تم ذكرها هي ليست للمؤسسات الكبرى الحساسة فقط، وإنما يجب أن تكون ثقافة والتزام عام في كل مؤسسة مهما صغرت ومهما قلت حساسيتها الأمنية.

قائمة المراجع

(1) طشقند، محمد البخاري، الانترنت ومبادئ الأمن المعلوماتي الدولي، 2016/01/12، (على الخط المباشر)، متاح على الرابط:

<http://www.larousse.fr/dictionnaires/francais>. <http://diae.net/4155>

(2) محمد عوض، العابدي، إعداد وكتابة البحوث والرسائل الجامعية: دراسة عن منهج البحث، القاهرة: شمس المعارف، 2005.

(3) الحسين، أحمد بن فارس بن زكريا ، معجم مقاييس اللغة، بيروت: دار الجيل، 1999.

(4) الزهراني، هاشم بن محمد ، المؤسسات المجتمعية والأمنية : رؤي مستقبلية، ورقة عمل مقدمة لندوة المجتمع والأمن المنعقدة بكلية الملك فهد الأمنية بالرياض ، 1425 هـ.

(5) قاموس المعاني، 2018/01/12، (على الخط المباشر)، متاح على الرابط <http://www.almaany.com/>:

(6) عراب، يونس، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها، 2018/05/12، [على الخط المباشر]. متوفر على الموقع: <http://www.arablow.com>.

(7) أليبرتو إسكوديرو، باسكال، تعريب أنس طويلة، أمن الشبكات اللاسلكية، كراسة المتدرب، 2018/02/11، (على الخط المباشر)، متوفر على الموقع: www.itrainonline.org/...Security/15_ar_mmtk_wireles.

(8) الشامي، أحمد ومحمد سيد حسيب الله، المعجم الموسوعي لمصطلحات المكتبات والمعلومات، الرياض: دار المريخ، 1988.

(9) أحمد أنور، بدر، مجتمع المعلومات الكوني، ومشكلات الخصوصية وأمن المعلومات، الإسكندرية، 1997.

(10) Review: mccumber cube methodology. The government of the hong kong special administrative region .An overview of information security standards, 21/05/2018..

<http://www.infosec.gov.hk/english/technical/files/overview.pdf>

(11) غيطاس، جمال محمد، الأمن المعلوماتي والجرائم الإلكترونية، أدوات جديدة للصراع، 2018/02/14. <http://studies.aljazeera.net/issues/>

(12) الشركة العامة لخدمات الشبكة الدولية، لجنة الفضاء الإلكتروني، للمعلومات، أمن الفضاء الإلكتروني، 2015، (على الخط المباشر)، متاح على الرابط <https://www.scis.gov.iq/upload/upfile/ar/security.doc>.

(13) سيد حسين، فاروق، الانترنت وأحدث ما كتب عنها، بيروت: دار الراتب الجامعية، 1999.

(14) W. Victor maconachy، corey d. Schou، Daniel ragsdale, the integrated ia model, 15/05/2018.

<Http://www.ibm.com/developerworks/security/library/s-confnotes2/>

(15) عوض، حاج علي، أمن المعلومات والمعايير الدولية، 2018/05/14، [على الخط المباشر]. متوفر على الموقع www.profawad.info/123456.

(16) معراج، هواري وعبيرات مقدم، إدارة مخاطر الأمن وشفافية المعلومات لنظم المعلومات في ظل البيئة الرقمية، 2018/12/11.

<https://ketabonline.com/books/100087/read?page=7>