

الأمن المعلوماتي للمنظمات: دراسة في المهددات وآليات التعزيز
Information Security in Organizations: a Study on Threats and Requirements

تاريخ الإرسال: 2021 / 06 / 16 تاريخ القبول: 2021 / 10 / 04 تاريخ النشر: 2021/12/30

سهيلة هادي

جامعة محمد خيضر، بسكرة، الجزائر، Email : hadisouheila@gmail.com

الملخص:

تهدف الدراسة إلى البحث في المهددات الطبيعية، البشرية والفنية للأمن المعلوماتي للمنظمات بغرض إبراز متطلبات تعزيزه الإدارية والتقنية، في ظل تنامي أهمية الحاجة إلى إرسائه نتيجة التطور المتسارع لتقنيات المعلومات والخسائر الناجمة عن تهديد أنظمة المعلومات حال ضياعها أو اختراقها. ويهدف دعم كفاءة أداء المنظمات من جهة، وكسب ثقة المتعاملين معها من جهة أخرى تتجلى أهمية دراسة الموضوع، الذي يهدف إلى تحقيق سرية، سلامة ووفرة المعلومات. هذه الثلاثية التي لن تستطيع جهود المنظمة بمفردها تحقيقها بل أيضا يستلزم دعم الدولة، والتعاون الدولي في هذا المجال عبر خلق الضمانات القانونية، الآليات المؤسسية والإجراءات العملية للتصدي للجرائم المعلوماتية التي تتسم بكونها جرائم عابرة للحدود.

الكلمات المفتاحية: الأمن المعلوماتي؛ المنظمات؛ تقنية المعلومات؛ أنظمة المعلومات؛ الجريمة المعلوماتية.

المؤلف المرسل: سهيلة هادي، Email : hadisouheila@gmail.com

Abstract:

This research paper aims to study the natural, human and technical threats to information security of organizations, in order to clarify its physical, administrative and technical requirements; as a result of the rapid development of information technology and the losses resulting from the threat of information systems if they are lost or compromised. And to support the efficiency of the performance of the organizations, and to gain confidence of their customers, it appears the importance of this study, which it seeks to achieve the confidentiality, integrity and availability of information, which the organization's efforts alone can not achieved it, but also it requires the support of the state and international cooperation in this field; through the creation of legal guarantees, institutional mechanisms and practical measures to face cybercrimes that are transboundary.

Keywords: Information Security; Organizations; Information Technology; Information Systems; Cybercrime

مقدمة:

تعتبر دراسة أمن المنظمات ضمن إطاره التقليدي فقط دراسة ناقصة، في ظل ما شهده العالم ولا يزال من سلسلة التطورات التكنولوجية التي أثرت على نمط عيش الإنسان، فالمنظمات باعتبارها آليات مؤسسية- تساهم في إشباع حاجات الجماهير على صعيد عدة مستويات - أصبح لزاماً عليها التكيف مع هذه المتغيرات بما يحقق أهدافها ويؤسس للثقة والجودة في مخرجاتها؛ لأن الحركية السريعة للنظام العالمي الجديد فرضت تحديات للمنظمات على المستوى الداخلي والخارجي، فهي مُطالبَة أكثر من أي وقت مضى التكيف مع المتغيرات الجديدة، في ظل الميزة التنافسية التي تتزايد بوتيرة جد متسارعة.



وانطلاقاً من فكرة من يمتلك المعلومة يمتلك القوة – دولة كانت أو منظمة أو فرداً – تبرز أهمية الأمن المعلوماتي والخطر الذي يشكله تهديد المنظومة المعلوماتية – المقصود أو غير المقصود – على المنظمة. وعلى هذا الأساس تعتبر المعرفة الدقيقة لهذه التهديدات من حيث طبيعتها أشكالها وأهدافها من العوامل المساعدة لإيجاد الآليات المناسبة لتعزيز أمن المنظمة المعلوماتي.

ونظراً للمكانة التي تحوزها المعلومات عموماً، وتقنيات المعلومات خصوصاً في المنظمة لأدائها الوظائف المنوطة بها، تبرز أهمية الموضوع لحاجة الكم الهائل من البيانات والمعلومات للحماية والتصدي لمختلف المخاطر التي تهدد النظام المعلوماتي للمنظمة عامة كانت أو خاصة، وعلى اختلاف طبيعة نشاطها اقتصادياً، إدارياً، وعسكرياً..إلخ.

ومن ناحية أخرى، يمكن اعتبار الأمن المعلوماتي من معايير فعالية المنظمات في ظل عصر المعلومات، حيث أصبحت المعلومات تمثل مورداً، وسيلةً وهدفاً للمنظمات في ظل التطور – المتسارع جداً – الذي تعرفه تقنية المعلومات ووسائل تهديد المنظومة المعلوماتية، الأمر الذي يدفع نحو البحث في متطلبات ضمان الأمن المعلوماتي عبر الآليات الاستباقية لدرء مخاطره، وتجنب المنظمة لخسائر مالية في حال اختراقه، ما يجعل نطاق الدراسة لا يقتصر فقط على حدود المنظمة، بل سيتجاوزه من خلال توضيح أهمية التعاون الدولي في هذا المجال، وتقييم لما تم طرحه من مبادرات.

لذلك تسعى هذه الدراسة إلى:

- توضيح مخاطر التعرّض المقصود للنظم المعلوماتية للمنظمات، والوسائل المستخدمة لتحقيق هذه الغاية.
- تقديم المتطلبات الداخلية لتعزيز الأمن المعلوماتي للمنظمات.
- إبراز أهمية التعاون الدولي في مجال الجريمة المعلوماتية لدرء مخاطرها.

توجد عدة دراسات بحثت في موضوع الدراسة عبر جوانب عديدة، منها:

- مؤلف الخثبر والقحطاني (2009): أين سلّطا من خلاله الباحثان الضوء على المهددات ذات الطبيعة التقنية لأمن المعلومات، ومن ثمة عرضا حلولاً تقنية لتعزيز الأمن المعلوماتي. بينما موضوع الدراسة أوسع من ذلك، إذ يهدف إلى دراسة مختلف المهددات بما تشمله من مهددات تقنية مستحدثة، وانطلاقاً من هذه التهديدات تم البحث في متطلبات تعزيز الأمن المعلوماتي للمنظمات.

- دراسة نوفيل وكريبط (2014): حيث تطرقا من خلالها الباحثان إلى التهديدات الداخلية والخارجية للأمن الإلكتروني للمنظمة، مع توضيح دوافعها والأشكال التي تتخذها. بالمقابل تسعى الدراسة إلى تقديم إستراتيجية أمن معلوماتي تتسم بالشمول من حيث الإعداد والتنفيذ، على المستوى الداخلي (المنظمة والدولة) وعلى المستوى الدولي، ومن حيث مواجهتها لمختلف المخاطر المهددة لأنظمة المعلومات للمنظمة.

- إن أغلب الدراسات التي تطرقت لهذا الموضوع ركزت على البعد التقني من جهة، وعلى المستوى الداخلي، أي: المنظمة من جهة أخرى، لتعزيز الأمن المعلوماتي للمنظمات، لذا تتميز هذه الدراسة بمحاولتها التطرق إلى أبعاد ومستويات أخرى لهذا الموضوع، بغرض معالجته بطريقة شاملة، بما يساهم في تعزيز الأمن المعلوماتي للمنظمات في ظل عصر المعلومات.

وانطلاقاً مما تقدم تتمثل إشكالية الدراسة في: كيف يمكن تعزيز الأمن المعلوماتي للمنظمات في ظل تنامي مهدداته ؟

للإجابة عن الإشكالية المطروحة، يمكن صياغة الفرضيات التالية:

1. يساهم تكوين وتوعية الموارد البشرية في مجال الأمن المعلوماتي، في تصدي المنظمة للجرائم المعلوماتية.

2. تجهيز المنظمة بتقنيات حماية المنظومة المعلوماتية، يُجَيِّب المنظمة الخسائر المالية.

3. يدعم التعاون القانوني الدولي في مجال مكافحة الجريمة المعلوماتية، تعزيز الأمن السبيري للمنظمات.



وستتم دراسة الموضوع بالاعتماد على أداة الإحصاء لتوضيح الخسائر التي يسببها تهديد المنظومة المعلوماتية للمنظمات ذات المصدر الداخلي أو الخارجي. وهذا بهدف إبراز أنواع، طرق وآثار تهديد الأمن المعلوماتي للمنظمات.

كما تمت الاستعانة بالمقترح القانوني، الذي سيركز على الضمانات القانونية المقدمة على المستوى الدولي لمواجهة الجريمة الالكترونية، وما ينبغي تعديله ضمن هذا المجال في ظل ما تتميز به تكنولوجيا المعلومات والاتصالات من تطور مستمر وسريع.

2. مفهوم الأمن المعلوماتي Information security

1.2 تعريف الأمن المعلوماتي:

قُدمت العديد من التعاريف للأمن المعلوماتي - الذي يندرج ضمن إطار الأمن غير التقليدي- منها من ركزت على وسائله، والأخرى على أهدافه، بينما هناك من عرفه انطلاقاً من مصادره. فالأمن المعلوماتي يدل على: "حماية أصول وموارد ومكتسبات نظام معلوماتي ما ... دون أن يؤثر على قدرة مستخدمي هذا النظام على الأداء أو يعوق عملهم من حيث الكفاءة أو التوقيت، وهذا الأمن المعلوماتي لا يمنع الجريمة المعلوماتية كلياً، لكنه كلما كان قوياً ودقيقاً وفعالاً، كان من الصعب ممارسة الاختراق ضد نظام المعلومات المستهدف" (عطية، 2009، ص 515). فالأمن المعلوماتي يهدف إلى حماية أنظمة المعلومات من الجرائم المعلوماتية. قد لا يمنع حدوث الجرائم المعلوماتية بشكل كلي، ولكنه يقلل منها، مما يدل على الخطر الحقيقي الذي تتسبب به مهددات الأمن المعلوماتي.

ومن ناحية أخرى، يُقصد بالأمن المعلوماتي ذلك الأمن الذي يشمل العديد من المحاور من أهمها: الأخطاء العفوية أثناء إدخال البيانات إلى الحواسيب، فقدان المعلومات بسبب تعطل الحواسيب وحوادث خلل للبرامج، سرقة المعلومات وفقدانها دون إذن لتتم إساءة استخدامها، أو بسبب حدوث الكوارث الطبيعية (صادق والفتال، 2008، ص 12). فالأمن المعلوماتي مصدران رئيسيان، الأول: بشري وقد يكون

فعل مقصود أو غير مقصود، أما الثاني: فمصدره طبيعي بسبب حدوث الكوارث الطبيعية.

بينما عرّفه (Williams, 2007, p. 3) استناداً للطبيعة الهادفة له، حيث: " يهدف الأمن المعلوماتي إلى :

- السرية: من خلال التأكد من أنه لا أحد يرى المعلومات الخاصة بك.
- السلامة: التأكد من أنه لم يتم تغيير المعلومات.
- الوفرة: التأكد من أن المعلومات متاحة للاستخدام عند الحاجة".

وعليه يتضح أن الأمن المعلوماتي، يعتبر الأمن الهادف إلى ضمان حماية النظام المعلوماتي من مصادر تهديد المعلومات التي قد تكون بشرية، طبيعية أو فنية بغرض تحقيق سرية، سلامة ووفرة المعلومات.

وينبغي الإشارة في هذا الإطار، أنه توجد بعض المفاهيم مرتبطة بشكل كبير بالأمن المعلوماتي، أبرزها مصطلح الأمن السيبراني Cybersecurity، الذي يدل على ذلك: "النشاط أو العملية أو القدرة أو الحالة التي تكون فيها نظم المعلومات والاتصالات والمعلومات الواردة محمية ومصانة ضد التلف أو الاستعمال غير المصرح أو التعديل أو الاستغلال" (Craingen, Diakun-Timbault and Purse, 2014, p.15). يبدو أن الأمن المعلوماتي أشمل وأعم من الأمن السيبراني، فالأول يهدف لحماية منظومة المعلومات من التهديدات الطبيعية والبشرية، مما يدفع لاتخاذ مجموعة من الإجراءات التي قد تكون إدارية، تقنية وفيزيائية، بينما الأمن السيبراني يهدف لضمان الحماية الالكترونية للمعلومة، أي: يركز على الجوانب التقنية لتحقيق أهدافه.

2.2 أهداف الأمن المعلوماتي: حيث يهدف إلى تحقيق:

- سرية المعلومات Confidentiality : أي حفظ المعلومات المخزنة أو المنقولة عبر الشبكة وعدم الاطلاع عليها أو استخدامها لأي أغراض دون إذن.
- سلامة المعلومات Integrity: بضمان عدم التغيير في المعلومات المخزنة أو المنقولة، ولها بُعدان، سلامة البيانات والمعلومات المرسل، وسلامة المصدر،

أي: مصدر إرسال البيانات والمعلومات. هذا و تجدر الإشارة إلى أن عملية الحفاظ على سلامة المعلومات أصعب بكثير من الحفاظ على سريتها، فضمان سرية المعلومات يتم بالحفاظ على سريتها، أما الحفاظ على سلامتها فيشمل ضمان السرية وعدم التغيير في البيانات.

➤ وفرة المعلومات Availability: وهي تعني ضمان بقاء المعلومات وعدم حذفها أو تدميرها، كأن تكون المواقع الالكترونية متاحة للاستخدام 24/24 ساعة وسبعة أيام في الأسبوع، وب حمايتها من أي هجوم قرصنة للموقع الالكتروني وخرق للإجراءات الأمنية الالكترونية (الطيبي، 2008، ص ص26-30).

لذلك يتوجب على المنظمات عند تصميمها لاستراتيجيات الأمن المعلوماتي مراعاة هذه الأهداف الثلاثة، لأنها تعتبر عوامل محددة لكسب ثقة المتعاملين في أداء المنظمة. وتُضاف إلى الثلاثية سابقة الذكر أهداف أخرى مهمة يسعى الأمن المعلوماتي للمنظمات توفيرها منها: التحديث، الدقة، الاكتمال، المرونة، الفائدة، الكفاءة، التكلفة، وقت الاستجابة، الاستقرار، التفصيل، القابلية للمعالجة، سهولة الاستخدام والوضوح (Slawomir, 2010, p.3). وهي أهداف إذا ما تحققت، جعلت مخرجات المنظمة تتسم بالجودة؛ لأنها تعمل على تحقيق رضا المتعاملين عن الخدمات المقدّمة.

ولقد برزت الحاجة إلى الأمن المعلوماتي كحاجة جدّ ملحة خصوصاً مع بداية القرن الحادي والعشرين، إذ بدأ يتم إجراء الدراسات الاستطلاعية حول القضايا المتعلقة بحالات الهجوم الالكتروني ومن أشهر المؤسسات التي تقوم بإعداد هذه الدراسات مؤسسة CERT، حيث سجلت عام 2003 حوالي 138000 حالة قرصنة، وفي سنة 2004م تمّت دراسة أكثر من 500 شركة، حيث بلغ مجموع الخسائر المالية الناجمة عن الهجمات الالكترونية لهذه الشركات حوالي 666 مليون دولار رغم أن هذه الشركات وظّفت تقنيات متعددة وحديثة للحماية كتقنية الجدران النارية بنسبة 98%، ما يعني أنه رغم استخدام التقنيات الالكترونية للحماية فهي غير كافية لضمان حمايتها وهذا راجع إلى:

- تعدد مصادر تهديد الأمن المعلوماتي الداخلية والخارجية، فجميع الفواعل أفراداً، منظماتٍ أو دولا هدفهم الاستحواذ على المعلومة، الأمر الذي تنجر عنه الجرائم الالكترونية.

- التطور المتزايد لتكنولوجيا المعلومات والاتصالات وتقنية المعلومات.
- وجود عقل بشري يهدف إلى امتلاك المعلومة سعياً للقوة، إرضاءً لفضوله، أو بدافع الانتقام والابتزاز (هادي، 2018، ص ص 229، 230).

الأمر الذي يجعل من ضمان الأمن المعلوماتي من التحديات الكبرى ليس فقط بالنسبة للمنظمات، بل للدولة في حد ذاتها، نتيجة تزايد التهديدات الأمنية الالكترونية من حيث عدد الهجمات والأضرار الناجمة عنها.

3. مهددات أمن معلومات المنظمات:

1.3 تصنيف مهددات الأمن المعلوماتي:

يمكن تصنيف مهددات الأمن المعلوماتي إلى ثلاث فئات رئيسية، كل فئة منها تضم العديد من التهديدات:

- التهديدات الفنية: وتشمل التهديدات الناجمة عن الأخطاء الفنية في أنظمة المعلومات، التي يغلب عليها الطابع الفني دون تدخل بشري، مثل: تهديدات عيوب التصميم والتشغيل، وتهديدات تشتت المعلومات التي تعود إلى تخزين البيانات في أماكن كثيرة ويتم التعامل معها من خلال شبكات متعددة، مما يحتم تطبيق أنظمة أمن معلومات متعددة، الأمر الذي يتسبب في ضعف منظومة أمن المعلومات وتشتتها.

- التهديدات البشرية: ويُقصد بها التهديدات الناجمة عن العنصر البشري - بشكل عمدي أو عن طريق الخطأ - وما يتسبب فيه من ضرر بوصوله إلى المعلومات والاطلاع عليها - دون أن يكون له صلاحية - أو إتلافها أو تسريبها. هذا الخطر الذي يتزايد عندما يكون لهذا العنصر صلاحية الدخول إلى أنظمة المعلومات أو أن يكون أحد الموظفين في المنظمة، وعن أهم مصادر التهديدات البشرية فيمكن توضيحها في: موظف المنظمة غير الواعي بالمخاطر الأمنية، المنظمات - بهدف التنافس -، التنظيمات الإرهابية، المهندسون وفنيو الصيانة خارج المنظمة (القحطاني، 2015، ص ص 61-63).

- تهديدات طبيعية: وتشمل الزلازل، الحرائق والفيضانات، فبالنسبة للأولى فهي تعمل على تدمير النظم المعلوماتية للمنظمة بالكامل، وغالبا ما يصاحب ذلك حريق ناتج عن التماس كهربائي. أما الفيضانات فتتسبب في عطل كلي أو جزئي للنظام المعلوماتي ويتوقف تأثير السيول على المنظمة حسب نوعية ودرجة مقاومتها لتلك السيول. كما للحرائق آثار تدميرية على الأجهزة المعلوماتية التي لا يمكن الاستفادة منها مرة أخرى (آل مواش، 2017، ص 58).

انطلاقا من هذه التهديدات، نستطيع القول أنه لا يمكن إهمال خطأ العنصر البشري الذي ينتج لنفس الجهة المستهدفة، لا سيما إذا كان بشكل عمدي مما يتسبب لها في خسائر باهضة. ففي تقرير لوزارة الدفاع الأمريكية عام 2000 ذكرت فيه أن 87 % من الهجمات المكتشفة التي تم شنّها على أنظمة المعلومات بالوزارة قام بها أشخاص من داخل الوزارة نفسها. وحسب تقديرات معهد أمن الحاسوب، فإن معدل تكاليف الهجوم الواحد من الداخل 2.7 مليون دولار، بينما لا يزيد معدل الهجوم الواحد من الخارج عن 57 ألف دولار (الخبث والقحطاني، 2009، ص ص 27، 28). لذلك لا ينبغي حصر اهتمام المنظمات على تحصين الأنظمة المعلوماتية للمنظمة ضد الهجمات ذات المصدر الخارجي فحسب، بل أيضا باتخاذ إجراءات استباقية لصد الأخطار من الداخل التي قد تكون دوافعها عدم الرضا الوظيفي .

وبما أن قطاع التجارة والخدمات يساهمان في تنمية الاقتصاد الوطني وتلبية حاجيات السكان بواسطة عدة مرافق، فإن تعرّض هذين القطاعين للهجوم الإلكتروني هو بمثابة شلل اقتصادي للدولة، ومنه تدمر المواطنين من الخدمات المقدمة، وهو الأمر الذي قد يؤدي إلى اللاتوازن الاقتصادي، لاسيما وأن الخسائر الاقتصادية الناجمة عن القرصنة الإلكترونية في المجال الاقتصادي ضخمة جدا، ففي دراسة أمريكية أشرفت عليها شركة Mac Ve لحماية برامج الإنترنت تتراوح الخسائر ما بين 375 و 575 مليار دولار سنويا، ومعظمها يتركز في قرصنة الحقوق الفكرية وسرقة المعلومات الخاصة بالشركات (هادي، 2017، ص ص 133، 134). الأمر الذي يجعل من أسباب الجريمة المعلوماتية الربح المالي وتحقيق الثراء، فوفق ما أشارت إليه إحدى المجالات المتخصصة

في الأمن المعلوماتي securite informatique تم التوصل إلى أن 43% من الجرائم المعلوماتية- المعلن عنها- كانت بدافع اختلاس الأموال؛ لسداد الديون المستحقة أو مشاكل عائلية سببها الأمور المالية أو إدمان ألعاب القمار أو المخدرات، لذا يتم بيع المعلومات المختلسة، ومثال ذلك: استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على 22 شريطاً ممغنطاً يحوي معلومات هامة بخصوص عملاء وإنتاج هذه الشركة، حيث هدد الذي قام بعملية الاختراق للنظام المعلوماتي للشركة ببيعها للشركات المنافسة إذا لم تُدفع له فدية مقدارها 200 ألف دولار. وبعد قيام الشركة بتقويم هذا الموقف، قدرت أن الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثير المطلب المطلوب، ما جعلها تدفع المبلغ من أجل استرداد الشرائط المسروقة (<http://bit.ly/2He9Bzo>).

وبالتالي فطبيعة نشاط المنظمة وحساسية معلوماتها تتحكم في كثرة أو قلة اختراقها، وفي الانصياع لمحاولات الابتزاز التي تتعرض لها. ورغم اختلاف أسباب الجرائم المعلوماتية إلا أنه توجد سمات مشتركة للمجرم المعلوماتي المتمثلة في: الذكاء، سرعة البديهة، التخصص في مجال تقنية المعلومات، الاحترافية، مما يساهم في تغلبه على عقبات الحماية المستخدمة من طرف الجهة المستهدفة.

وفي سياق ذو صلة، تتنامى أهمية توفير الأمن المعلوماتي للمنظمات نتيجة ما تعيشه الدول اليوم من حروب الجيل الرابع أو الحرب اللاتماثلية Asymmetric Warfare التي غيّرت مفهوم الحروب، أين تخسر الدولة احتكارها للحرب. ويعتبرها ماكس مانوارينغ Max G. Manwaring حرباً بالإكراه، فالخصم مرغم على خوض غمار الحرب رغم إرادته، دون الاعتماد على الجيوش فقط بل قد تكون عن طريق المواطنين أو الشركات متعددة الجنسيات، مستخدماً في ذلك القوة الذكية، بهدف خلق الدولة الفاشلة من أجل فرض واقع جديد. ففي حروب الجيل الرابع قد تتوفر أحدث أنواع الأسلحة إلا أنه قد يخسر القائد الحرب؛ لأنه يواجه خصماً أكثر ذكاءً وفطنة له قدرة أكبر على فهم وتحليل العلاقات بين الأشياء والاستنتاج، لأن مهمة الجندي لم تعد تقتصر على حمل السلاح وإنما تمتعه بالذكاء والمهارات الالكترونية للاستخدام الجيد

للسلاح، إضافةً إلى ذلك تمتعه بقوة الشخصية والقدرة العالية على التركيز وسرعة المناورة لتحقيق الهدف بدقة عالية (هادي ، 2017، ص 126). لذلك فإن سعي الدولة تعزيز الأمن المعلوماتي للمنظمات ضرورة حتمية، يندرج في إطار مساعيها حماية أمنها القومي؛ لاعتماد الحروب الالكترونية في تهديدها إضافةً إلى إستراتيجية عسكرية التكنولوجيا، اختراق المنظومة الاقتصادية وحتى الهيمنة الفكرية الثقافية.

2.3 طبيعة المعلومات المراد حمايتها: تتجلى المعلومات المطلوب حمايتها حسب (عبد الكريم والربيعي، 2013 ، ص 302) في:

- الأسرار الداخلية للشركات: والتي قد يؤثر إفشاؤها على مكانة الشركة في السوق، كالتأثير على حجم أعمالها وقائمة عملائها.
- المعلومات التقنية: أي المعلومات الفنية المستخدمة في الإنتاج، وهي الخطوات العديدة التي يتطلبها إنتاج وتوزيع منتجاتها أو خدماتها. حيث يحتفظ بعض الموظفين الأساسيين بهذه المعلومات، لذا يجب توثيقها واتباع إجراءات أمنية للحفاظ عليها.
- معلومات عن الموارد البشرية: والمتعلقة ببيانات الموظفين التي تتطلب اهتمام خاص لحماية الملفات التي تحتوي على معلوماتهم وبياناتهم الشخصية، منها: الرواتب، التأمين، الحالة الصحية وتقارير الأداء.
- معلومات العملاء: فالشركة بحاجة دائمة للاحتفاظ بمعلومات مفصلة عن عملائها وطبيعة عملهم وبعض المعلومات المهمة عنهم.
- سلعة المعلومات: مثل البرمجيات، الخرائط، الكتب، الإعلانات وغيرها من السلع التي تدخل المعلومات في تكوينها بنسبة كبيرة، وتكون حمايتها بواسطة قوانين الملكية الفكرية.
- المعلومات المؤقتة: هناك الكثير من المعلومات ذات الطبيعة المؤقتة كمسودات التقارير. هذه المعلومات قد تكون لها قيمة إستراتيجية للشركة.
- المعلومات الأمنية: وهي المعلومات التفصيلية حول كيفية حماية المعلومات الاستراتيجية في الشركة التي لها أهمية خاصة وحساسية عالية؛ لأنه من الممكن إساءة استخدامها بصورة أو بأخرى.

وبالتالي فكل ما يرتبط بالمنظمة من معلومات تخص سياسات وإجراءات العمل، وأيضا الموارد البشرية (عاملين ومتعاملين) يستلزم حمايتها لضمان تحقيق المنظمات أهدافها والتي ستعكس بشكل إيجابي على سمعتها. وضمن هذا الإطار يمكن التأكيد على أنه كلما كان هناك دافع قوي، وطريقة حديثة، وثغرة كبيرة، كلما نجح الهجوم الإلكتروني محققا أهدافه، ومسببا خسائر للجهة المستهدفة.

3.3 طرق الهجمات الإلكترونية: نظرا لما تمثله الهجمات الإلكترونية من خطر على الأجهزة، برامج وشبكات المؤسسة سيتم توضيحها لإبراز مدى خطورها. فهذه الهجمات الإلكترونية أخذت أشكالا مختلفة وأساليب متعددة، وهي في تطور مستمر مستغلة أي ثغرة موجودة في الأنظمة لاختراقها، ومن بين أشكالها نذكر:

- الفيروس Virus: يقصد بالفيروس المعلوماتي ذلك البرنامج الخبيث الذي يتضمن أهدافا تدميرية للحاسبات المصابة ولكل محتوياتها. يتميز بقدرته على نسخ نفسه في البرنامج الذي يصيبه، وبالتحكم به وتعديله، وقدرته على الانتقال من برنامج إلى آخر داخل نفس الحاسوب المصاب.

- الدودة Ver : تتميز الديدان الإلكترونية بآلية عمل خاصة بها فهي لا تعتمد على غيرها من البرامج لإصابة الحاسوب، كما أنه لكل دودة آلية عمل، فبعضها يقوم بالانتشار داخل الجهاز إلى أعداد هائلة، وبعضها الآخر يتخصص بالبريد الإلكتروني وإرسال رسائل غير مناسبة، مما يتسبب في حرج كبير للشخص أو الهيئة صاحبة البريد الإلكتروني (آل مواش، 2017، ص ص 50، 51).

- برنامج Macro: هو برنامج مصمم للعمل على تطبيق معين أو لعدة تطبيقات تشترك بلغة برمجة واحدة، مثل: excel و word فعند فتح الوثيقة المصابة فإن الفيروس ينتشر ليؤدي مهمته التخريبية، ومما يساعد انتشاره زيادة استخدام البرنامج (نوفيل وكريبط، 2014، ص 192).

- حصان طروادة Trojan Horse : في البداية تم تصميم هذا البرنامج لغرض مفيد لمعرفة ما يقوم به الأبناء في غياب الوالدين، أو ما يقوم به الموظفون في غياب المدير على جهاز الكمبيوتر. إلا أنه تم استغلال هذا البرنامج بشكل سيئ، وخطورته تكمن في

كونه يُتيح للمخترق الحصول على كلمة سرّ الدخول للجهاز بطريقة لا تثير الشك، فلا يستطيع صاحب الجهاز ملاحظة وجود دخلاء تمكنوا من الدخول إلى جهازه (ليتيم وليتيم، 2015، ص ص 243، 244).

– اعتراض البيانات Sniffing: تسمح هذه التقنية باستراق السمع للبيانات التي تنتقل في شبكة المؤسسة قبل استقبالها من طرف المستقبل، وكمثال على هذا النوع من البرمجيات Mpsnif و Sniffer ettercap .

– البريد غير المرغوب فيه Spamming : تدل رسائل البريد غير المرغوب فيه على إساءة استخدام نظام الرسائل الالكترونية بإرسال كم هائل من الرسائل العشوائية، غير المرغوبة من المستقبلين لهذه الرسائل، وفي الغالب يكون الغرض منها الاحتيال على صاحب البريد الالكتروني.

– انتحال نظام النطاقات DNS: يحدث بتوجيه مستخدمي الإنترنت أوتوماتيكياً إلى المواقع التي تحتوي على برامج الجوسسة أو المواقع التي تشبه المواقع التجارية والبنكية للإيقاع بالضحية، ويتم هذا من خلال الرسائل الالكترونية غير المرغوب فيها.

– الاضطهاد الالكتروني Phishing: ويعني سرقة البيانات الشخصية السرية والحساسة عن طريق رسائل البريد الالكتروني لغرض انتحال شخصية بنك أو مؤسسة أخرى، لإيهام الضحية بجدية الطلب وأهميته، والهدف من ذلك سرقة الأرقام السرية وغيرها من البيانات الشخصية (نوفيل وكريبط، 2014، ص ص 192، 193).

– التنصت Eavesdropping : ويدل على اعتراض الاتصالات من طرف غير المصرح بهم. ويكون محدود الفعالية عندما يتم الاستماع سرّاً فقط إلى الرسائل المتصلة بالشبكة. بينما يكون التنصت فاعلاً عندما يستمع الدخيل ويدخل شيئاً في تدفق الاتصالات، ما يؤدي إلى تشويه الرسائل، وسرقة المعلومات الحساسة (Alhassan and Adjei-Quaye, 2017,p.103).

– الهندسة الاجتماعية Social Engineering: ويقصد بها استخدام المهاجم حيلة نفسية لخداع مستخدمي الحاسوب للوصول إلى معلوماتهم. قد يتخذ الأسلوب الحسي كسرقة المعلومات الموجودة في النفايات، إنشاء مواقع لتحميل البرامج المجانية شرط

إدخال اسم المستخدم وكلمة المرور ومن ثمة سرقتها، أو الأسلوب النفسي بإيهام الضحية أنه شخص موثوق به (الخبر والفحطاني، 2009، ص ص 31-35).

إن تعدد هذه التقنيات يعكس رغبة المهاجم الإلكتروني في الاستحواذ على المعلومة عبر سعيه المستمر لاكتشافه الثغرات المعلوماتية في المنظمات، للتجسس عليها أو استغلالها، أو لتعطيل عمل الأجهزة والبرامج أو تقليل سرعتها، مما يؤدي إلى عرقلة أداء المنظمة لأنشطتها.

4. متطلبات الأمن المعلوماتي للمنظمات:

إن إستراتيجية الأمن المعلوماتي تقع على مسؤولية جميع الموارد البشرية في المنظمة، وأهم شروطها عدم تعارض أهدافها مع أهداف المنظمة. والتي تعتبر إجراءات استباقية ينبغي على المنظمات الحرص على تجسيدها لتوفير الحماية المعلوماتية لها، وهي تتمثل في الآتي:

1.4 متطلبات إدارية: ويبرز أهمها في الآتي:

1. التأكد من حسن عقود الصيانة، وذلك بعمل المراجعات القانونية والفنية الكافية لها.

2. تطبيق مبدأ التصنيف في مدى سرية المعلومات والبرامج، مثلاً: سري للغاية، سري لحد كبير، سرية وسط.

3. تصنيف ولاء العاملين والمتعاملين، مثلاً: موثوق كلياً، موثوق لحد كبير وموثوق لحد ما.

4. تصنيف مهارة وقدرة المتعاملين، مثلاً: ذوو المهارة العالية، ذوو المهارة المتوسطة وذوو المهارة الضعيفة.

5. ضرورة تولي إدارة وتشغيل شبكات المعلومات عناصر بشرية مدربة ومؤهلة للتعامل مع هذه التكنولوجيا، حيث لا مجال لعبث الهواة بهذه الأجهزة والتقنيات خاصة في المنظمات الحكومية والمنظمات الحيوية للدول.

6. وضع سجل خاص في استعلامات المركز لتدوين كافة أسماء الزائرين فيه، أسباب ووقت الدخول والخروج مع ضرورة متابعة هذا السجل.



7. عقد ندوات دورية بحضور المدراء لتذكير الموارد البشرية بضرورة أهمية الحفاظ على أمن وسرية البيانات والحواسيب (أبو حمام، 2014، ص ص 63- 67).

8. وضع العلامات الإرشادية والتحذيرية في الأماكن المناسبة.

9. تجهيز خرائط تفصيلية، عادية أو رقمية وإسقاط جميع نقاط المراقبة والكاميرات عليها لمعرفة مكان أي حادث وتسهيل عملية الوصول إليه.

1. التحكم في دخول الأجهزة وخروجها، وتوثيق ذلك، ويُفضّل استخدام الأرقام التسلسلية للأجهزة لضبط ذلك بشكل دقيق.

2. تثقيف العاملين وتدريبهم على الإجراءات والقواعد الأمنية الصحيحة دوريا.

3. رفع التقارير الدورية والاقتراحات عن الحماية المعلوماتية للقيادات العليا(القحطاني، 2015، ص 15).

فالمطلوبات الإدارية موجّهة بصفة رئيسية إلى الموارد البشرية العاملة بالمنظمة من خلال تكوينها، تأهيلها وتوعيتها كي يكون لها دورٌ فاعلٌ في حماية المنظومة المعلوماتية للمنظمات.

2.4 المتطلبات التقنية: من بين الآليات الفنية الضامنة للحماية أو الهادفة للتصدي للمهددات التي يمكن أن تتعرض لها أنظمة معلومات المنظمات يوجد:

➤ وسائل التحقق البيولوجي: لضمان استخدام النظام أو الشبكة من طرف الأشخاص المخوّلين بذلك الاستخدام، ينبغي الاعتماد على هذه الوسائل التي تضم البطاقات الذكية المستخدمة للتعريف البيولوجي التي تعتمد على سمات معينة للمستخدم، حيث تقوم بتسجيل معلومات عن بصمات الأصابع، الوجوه، الأصوات، شبكية العين والتوقيع الإلكتروني لتسمح المرور من بوابة معينة.

➤ التشفير Encryption : عبر ترميز البيانات العادية إلى نصوص مشفرة لتتغذر قراءتها من أي شخص لا يملك كلمة المرور لفك شفرة البيانات، فكل جهة أو فرد تمتلك مفتاحين لتشفير وفك البيانات، الأول: هو مفتاح خاص تحوزه فقط الجهة المخولة، في حين الثاني وهو المفتاح العام، الذي يتم نشره على

شبكة الحكومة الالكترونية، لاستخدامه من قبل الجهات الأخرى لتشفير الملفات والمعلومات المراد إيصالها للطرف الآخر (ليتيم ولتيم ، 2015، ص 248، 249).

➤ كلمات المرور Pass words: نظرا لأهميتها يجب الحرص عليها، فعند اختيارها يجب مراعاة اختيار كلمة مرور صعبة، عدم اطلاع الغير عليها، تغييرها دوريا، مع ضرورة أن تكون خليطا بين الحروف والأرقام.

➤ التحديث التلقائي Automatic update: حيث يعد التحديث الدائم للبرامج وأنظمة التشغيل من أهم عوامل حماية أمن شبكات المعلومات؛ لأن هذه النظم لا تخلو من الأخطاء التي تحدث في فترات البناء، لذا تعمل الشركات على إيجاد التحسينات المستمرة لسد نقاط الضعف في هذه البرامج والأنظمة.

➤ التخزين الاحتياطي Backup: وذلك بعمل نسخ احتياطية لمحتويات الحواسيب وشبكات المعلومات، وحفظها في مكان آمن وبعيد بشكل دوري، بهدف الرجوع إليها في حالة حدوث أعطال أو تدمير الشبكة (أبو حمام، 2014، ص 64، 65).

➤ جدران النار Firewalls: يعمل جدار النار كمنقح للبيانات الخارجة من شبكة المنظمة والداخلية إليها، ليسمح للأنظمة المُصرح بها فقط المرور. فهي تقنية جيدة لحماية شبكات الحاسوب حيث أن جدار ناري واحد يمكن أن يحمي عددا كبيرا من الأجهزة- إذا ما تمت تهيئة جدران النار ومراقبتها بالشكل الصحيح- مما يقلل من تكلفة الحماية. لكن بالمقابل لا بد من تهيئة وإدارة أشخاص مدبرين جيدا عليها؛ لأن التهيئة الخاطئة لجدار النار تخلق ثغرة أمنية كبيرة .

➤ أنظمة كشف ومنع التطفل: بالنسبة للأولى فهي برامج تُركب في أجهزة الحاسوب أو الخوادم Servers لمراقبة أي أنشطة مريبة عليها، كما تُستخدم هذه البرامج لمتابعة المستخدمين والتأكد من عدم قيامهم بحذف الملفات أو إعادة تهيئة الأجهزة والخوادم أو تغيير إعداداتها المهمة بما يُعرض هذه الأجهزة للخطر. أما عن الثانية فهي برامج لمنع التطفل تكشف البيانات والأنشطة غير

الطبيعية ثم تمنعها من الوصول إلى أهدافها مع قيامها بخطوات استباقية لمنع المتطفل الوصول إلى أهدافه (القحطاني، 2015، ص ص 253-274).

بناءً على ما تقدم، ينبغي تأكيد أن جملة المتطلبات - سאלفة الذكر - مترابطة مع بعضها البعض، فلا يمكن تعزيز الأمن المعلوماتي للمنظمة دون تجسيد هذه الثنائية، وإلا كان تخريب النظام المعلوماتي نتيجة اختراقه - من طرف القرصنة، الفضوليين، الشركات المنافسة أو حتى من العاملين في المنظمة نفسها- سهلاً. وبما أنه لتحقيق أهداف المنظمة لا بد من تضافر كل المستويات التنظيمية، الأمر الذي ينطبق كذلك على أهداف الأمن المعلوماتي لأن جميع العاملين في المنظمة بحوزتهم معلومات - متفاوتة الأهمية - يستوجب توفير الحماية لها.

كما لا يمكن تعزيز الأمن المعلوماتي للمنظمات إذا لم يبادر صناع القرار - لدرء خطر الجرائم المعلوماتية - بتجسيد الآتي :

- تشريع القوانين الرادعة للجريمة المعلوماتية.
- إنشاء المؤسسات التي تتولى مهمة مكافحة والوقاية من الجرائم الالكترونية وتطبيق القوانين، وأيضا المراكز التي تقوم بعملية تشفير المعلومات والبيانات وحفظها من الضياع.
- التوعية بمخاطر الجرائم المعلوماتية على مستوى المدارس، الجامعات، ووسائل الإعلام...
- دعم اقتناء المعدات والأجهزة، وكل الوسائل المتعلقة بتعزيز الأمن المعلوماتي بحوافز بنكية وجبائية.

ومن ناحية أخرى، يصعب تجسيد الأمن المعلوماتي في ظل غياب التعاون الدولي، ومن الجهود الدولية في هذا المجال نذكر:

- قيام المنظمة الدولية لتوحيد المقاييس بوضع مخطط لسلسلة من المعايير المتعلقة بأمن المعلومات وإدارة المخاطر، أطلق عليها اسم مجموعة المعايير المعنية بنظم إدارة المعلومات أو ISO27k التي يساهم تجسيدها في كسب المنظمات للميزة التنافسية

والمصادقية، ورضا المتعاملين عن مخرجاتها، ما يرفع من درجة الثقة فيها (<http://bit.ly/2UGRRVg>).

- تبني منظمة الأمم المتحدة دليلاً يتعلق باستخدام الحاسبات في تدفق البيانات الشخصية سنة 1989م، وفي سنة 1990 م تبنت الهيئة العامة دليل تنظيم استخدام المعالجة الآلية للبيانات الشخصية، وهي مبادئ غير ملزمة للدول الأعضاء مما يقوض فعاليته.

- إصدار القرار رقم 63/55 المتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، فقد أكدت فيه الأمم المتحدة على ضرورة أن تعمل الدول على تدريب العاملين في مجال القوانين وتزويدهم بما يحتاجون لمكافحة إساءة استعمال التكنولوجيا.

- إقليمياً، فقد تم إبرام اتفاقية بودابست سنة 2001 م بشأن الجريمة الالكترونية، وهي أول معاهدة دولية لملاءمة القوانين في مختلف الدول فيما يخص النشاط الإجرامي في عالم الإنترنت، بحيث تلزم الدول الموقعة على اتخاذ القوانين الجنائية ضد أنواع محددة من الأنشطة في الفضاء الالكتروني، وما يميز هذه الاتفاقية - وإن كانت بالأساس إقليمية - هو إمكانية مصادقة الدول غير الأوروبية عليها مثلما قامت به الولايات المتحدة الأمريكية، فهي تعتبر من أهم الاتفاقيات الداعمة للأمن المعلوماتي، عبر التصدي للولوج والاعتراض غير القانوني للمعلومات، الاعتداء على سلامة البيانات، إساءة استخدام أجهزة الحاسوب، التزوير والغش المعلوماتي، والاعتداءات على الملكية الفكرية. هذا وتستمد أهميتها هذه الاتفاقية من الطابع الإلزامي لها من خلال توحيد القوانين المتعلقة بالجرائم الالكترونية بين الدول الموقعة عليها. فاتفاقية بودابست لم تهمل المساعدة القضائية بين الدول الموقعة على الاتفاقية، هذا الذي يعتبر عاملاً مساعداً لتعزيز الأمن المعلوماتي خصوصاً وأنها اتفاقية تتسم بالزامية التضمين في الأنظمة القانونية الداخلية للدول الموقعة عليها، فمثلاً الفقرة الأولى من المادة 24 من الاتفاقية حددت تسليم المجرمين كنوع من التعاون لمكافحة الجرائم المعلوماتية، إضافةً إلى ضبطها لنوع الجرائم المتعلقة بالتعاون القضائي بين الدول الموقعة على الاتفاقية (هادي، 2018، ص ص 234 - 237).

يبدو جليا أن هناك إدراكاً على المستوى الدولي لمخاطر الجريمة الالكترونية لمصالح المنظمات والدول، ما يجعل الرهان قائما اليوم على توحيد الجهود لخلق ضمانات قانونية وآليات مؤسسية تنضم إليها العديد من الدول لدرء مخاطر الجريمة المعلوماتية. غير أن التعاون الدولي في مجال تعزيز الأمن المعلوماتي يواجه مجموعة من التحديات من بينها (دّار، 2017، ص ص 290-292):

- عدم وجود أنموذج موحد للنشاط الإجرامي: حيث يغيب الاتفاق العام المشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرّما في نظام آخر، وعوامل ذلك تعود للاختلاف في البيئات، العادات، التقاليد، والثقافات من مجتمع لآخر، مما ينعكس على اختلاف السياسة التشريعية من دولة لأخرى.

- تنوع واختلاف النظم القانونية والإجرائية: فمثلا المراقبة الالكترونية والتسليم المراقب وغيرها من الإجراءات الشبيهة التي تندرج في إطار جمع الأدلة أو التحقيق، فقد تكون قانونية في دولة وغير قانونية في دولة أخرى، بالتالي سيتعرق تنفيذ القانون.

- غياب قنوات الاتصال: إن أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة الالكترونية الحصول على البيانات والمعلومات عن المجرمين، ولتحقيق ذلك ينبغي وجود نظام اتصال يسمح للجهات القائمة بالتحقيق الاتصال بجهات أجنبية لجمع الأدلة أو معلومات مهمة، وعدم وجود هذا النظام ينعكس على عدم جمع الأدلة والمعلومات التي تكون مفيدة للتصدي للجرائم المعلوماتية.

- صعوبات المساعدات القضائية الدولية: فالأصل في الإنابة القضائية الدولية - والتي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي - أن تُسلّم بالطرق الدبلوماسية وهو ما يجعلها تتسم بالبطء والتعقيد، الذي يتعارض مع طبيعة تقيات المعلومات وما تتميز به من سرعة.

وبالتالي يمكن القول أنّ ثمة تحديات قانونية تعرقل مساعي التعاون والتنسيق بين الدول في مجال الأمن المعلوماتي، وللتغلب على هذه التحديات ينبغي:

- تحديث التشريعات الوطنية المتعلقة بالجرائم المعلوماتية.
- إبرام اتفاقيات تعاون يتم فيها توضيح مضامين وآليات هذا التعاون، وكذلك توحيد مفهوم الجريمة المعلوماتية.
- تحديث القوانين الجنائية الوطنية بما يتناسب والتطور الكبير الذي تشهده تكنولوجيا المعلومات والاتصالات.
- إنشاء آليات مؤسسية على المستوى الدولي تتولى مهمة تسريع إجراءات التحقيق وتطبيق القوانين.

5. الخاتمة:

بناءً على ما تقدم، فقد تم التوصل إلى النتائج التالية:

- يهدف الأمن المعلوماتي إلى حماية نظم المعلومات، البرمجيات والاتصالات من التهديدات الطبيعية، البشرية (المقصودة وغير المقصودة) والفنية، بغرض تعزيز سرية، سلامة ووفرة المعلومات. فالمنظمات مُطالبة أكثر من أي وقت مضى بتعزيز أمنها المعلوماتي لتحقيق أهدافها بالفعالية المطلوبة، لاسيما في ظل انتشار الخدمات الالكترونية عن بعد. وكذلك لتنامي انتشار الجرائم الالكترونية التي تعود دوافعها إلى: الربح المالي، عدم الرضا الوظيفي، الرغبة في الانتقام من الجهة المستهدفة، أو لإثبات القدرات الفنية على اختراق المنظومة المعلوماتية للمنظمة أو بدافع المنافسة، متخذةً طرقاً عديدة لذلك كالفيروسات، حصان طرداوة، البريد غير المرغوب فيه، انتحال نظام النطاقات، الاصطياد الالكتروني والهندسة الاجتماعية، وهو الذي يتسبب في إحداث أضراراً على المستوى العملي والمالي للمنظمة؛ لأن وتيرة تطور تقنيات المعلومات جد سريعة.

- إن تهديد المورد البشري الذي يعمل بالمنظمة لسرية، سلامة ووفرة المعلومة يُمثل تهديداً حقيقياً لها؛ لأن ذلك يتسبب في خسائر مادية أكثر من الخسائر التي يتسبب بها الهجوم الالكتروني من طرف أشخاص لا يعملون بالمنظمة.
- لإعداد إستراتيجية الأمن المعلوماتي للمنظمة وضمان فعاليتها، ينبغي مراعاة المراحل التالية:



- 1- التصنيف الدقيق للمعلومات في المنظمة حسب درجة المخاطر المترتبة على اختراقها.
- 2- تحديد المخاطر المحتملة على أمن المنظمة المعلوماتي.
- 3- تحديد طريقة مواجهة المخاطر: بإعداد خطة تتضمن آليات مواجهة تهديدات النظام المعلوماتي، يتم فيها إشراك جميع العاملين في المنظمة من حيث الإعداد والتنفيذ لضمان نجاحها.

- تُركز المتطلبات الإدارية للأمن المعلوماتي على العنصر البشري الذي يعمل بالمنظمة أو خارجها، عبر السماح فقط للمصرّح بهم الاطلاع أو امتلاك المعلومة، فكفاءة الموارد البشرية في المنظمة تمثل عاملاً محورياً لفعالية سياستها الأمنية. كما تُمثل وسائل التحقق البيولوجي- التشفير، التحديث التلقائي، التخزين الاحتياطي جدران النار، وأنظمة كشف ومنع التطفل - تقنيات هامة لدعم الأمن السبراني للمنظمة.

وفي الأخير، يمكن القول أنه إذا ما كانت مساعي آليات تعزيز الأمن المعلوماتي للمنظمات حصرًا على المنظمات، فستبقى محدودة الفعالية، ما لم تكن هناك إرادة سياسية لخلق ضمانات قانونية وأطر مؤسسية على مستوى الدولة لدرء مخاطر الجريمة الالكترونية التي هي في تزايد مستمر نتيجة التطور السريع الذي تعرفه تكنولوجيا المعلومات والاتصالات، وهو الأمر الذي يدفع نحو دعم مساعي التعاون القانوني الدولي في مجال مكافحة الجريمة المعلوماتية؛ لاعتبار أن هذا النوع من الجرائم عابر للحدود.

🚩 قائمة المراجع:

أ- المراجع العربية:

- 1- أبو حمام، محمد عبد الرحمان. (2014)، دور نظم المعلومات الإدارية في تحقيق الأمن المعلوماتي في جهاز الشرطة الفلسطينية، رسالة ماجستير، أكاديمية الإدارة والسياسة للدراسات العليا، جامعة الأقصى، غزة.
- 2- آل مواش، ضرغام جابر عطوش. (2017)، جريمة التجسس المعلوماتي: دراسة مقارنة. القاهرة: المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع.

- 3- الخثير، خالد بن سليمان. و القحطاني، محمد بن عبد الله. (2009)، أمن المعلومات بلغة ميسرة. الرياض: مركز التميز لأمن المعلومات.
- 4- درّار، نسيم. (2017)، الأمن المعلوماتي وسبل مواجهته في التعامل الالكتروني دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان.
- 5- الديبري، عبد العالي. (2013)، الجريمة المعلوماتية: تعريفها..أسبابها..خصائصها، متحصل عليه من: <http://bit.ly/2He9Bzo> تاريخ الاطلاع: 2019/03/15.
- 6- صادق، دلال. و الفتال، حميد ناصر. (2008)، أمن المعلومات. عمان: دار البازوري العلمية للنشر والتوزيع.
- 7- الطيطي، خضر مصباح إسماعيل. (2010)، أساسيات أمن المعلومات والحاسوب. عمان: دار حامد للنشر والتوزيع.
- 8- عبد الكريم، نهاد عبد اللطيف عبد الكريم. و الربيعي، خلدون هادي. (2013)، أمن وسرية المعلومات وأثرها على الأداء التنافسي، مجلة دراسات محاسبية ومالية، المجلد 08، العدد 23: 289-317.
- 9- عطية، طارق إبراهيم الدسوقي. (2009)، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية. الإسكندرية: دار الجامعة الجديدة.
- 10- القحطاني، ذيب بن عايض. (2015)، أمن المعلومات. الرياض: مدينة الملك عبد العزيز للعلوم والتقنية.
- 11- اللجنة الاقتصادية والاجتماعية لغربي آسيا. (2009)، بناء الثقة بالخدمات الالكترونية في منطقة الإسكوا، متحصل عليه من: <http://bit.ly/2UGRRVg> تاريخ الاطلاع: 2019/03/20.
- 12- ليتيم، فتيحة. وليتيم، نادية. (2015)، الأمن المعلوماتي للحكومة الالكترونية وإرهاب القرصنة، مجلة المفكر، العدد 12: 237-253.

13- نوفيل، حديد. و كربيط، حنان. (2014)، أمن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة، مجلة المؤسسة، العدد 03: 186-207.

14- هادي، سهيلة. (2017)، الحروب الالكترونية في ظل عصر المعلومات، مجلة رؤى إستراتيجية، المجلد 04، العدد 14 : 122-145.

15- هادي، سهيلة. (2018)، آليات تعزيز حق الإنسان في الأمن المعلوماتي، المجلة الجزائرية للعلوم القانونية الاقتصادية والسياسية، عدد خاص: 223-251.

ب- المراجع الأجنبية:

- 16- Alhassan, M.M. and Adjei-Quaye, A, (2017). **Information Security** in an Organization , *International Journal of Computer*, 24(1) : pp 100-116.
- 17- Craigen, D. Diakun-Tibault, N. and Purse ,R. (2014) , **Defining cyber security**, *Technology innovation management review* :13-21.
- 18- Slawomir,W (2010), **The Importance of Information Security** Management in Crisis Prevention in the Company , paper presented at the 6th international symposium on business administration global economic crisis and changes, [N.P].
- 19- Williams, R. H. (2007), Report Introduction to Information Security Concepts, [N.P].