Journal homepage:
http://ijimct.journals.ekb.eg/
Online ISSN: 2682-2881 Print ISSN: 2682-2105

Original Research Article

Information Security in the Arab World: Risks and Challenges

Jabreel AL-Arishee*.

Dean,Deanship of Development and Quality Chariman of Department and Professor of Information Sciences. King Saud University.Former member of SHoura Counsil of Kingdam of Saudi Arabia , Saudi Arabia.

ABSTRACT

This study aims at identifying the risks and challenges facing information technology in the Arab world, through measuring the magnitude of cybercrimes; cybersecurity capabilities in the Arab world; the impact of the gap in the research and development on cybersecurity; and the legal and organizational readiness to maintain cybersecurity and its security measures in the region. This study applied the descriptive analytical method as it is the most appropriate method to achieve its objectives. The study concluded to a number of results, such as: the Arab countries vary in their exposure to cybercrime risks and their capabilities to encounter those risks; the Gulf Countries are the least capable to combat cyber-attack risks due to the lack in technical skills compared to advanced countries; and the limited spread of communication networks in some Arab countries made them less exposed to cybercrime risks. It also showed that Arab countries, except of Oman, ranked last compared to other world countries regarding the legal and regulatory

ARTICLE INFO

Article history:

Received 15 Jun.2019

Accepted 20 May 2019

Online 29 November 2019

Keywords:

Information Security, Arab World, Information Security Risks, Information Security Challenges

* Corresponding author:Email: jeddah42@yahoo.com

readiness. Moreover, the Study highlights that there is no correlation between cybersecurity regulatory and administrative readiness for a country, and the capability to encounter cyber-attack risks. The study concluded to a number of recommendations, such as: the importance of enacting new regulations on cybercrimes; establishing a central government entity for cybersecurity-related issues; and developing a national cybersecurity strategy that clearly identifies the roles and responsibilities of entities.

ABSTRACT

Keywords:

أمن المعلومات، العالم العربي، مخاطر أمن المعلومات، تحديات أمن المعلومات

تهدف الدراسة إلى التعرف على المخاطر والتحديات التي تواجه أمن المعلومات في العالم العربي، وذلك من خلال التعرف على حجم مخاطر الجرائم السيبرانية في العالم العربي، وقدرة العالم العربي على مواجهة مخاطر الجرائم السيبرانية، وأثر الفجوة في قدرات العالم العربي في البحوث والتطوير على الأمن السيبراني، ومدى تأهب النواحي القانونية والتنظيمية للحفاظ على الأمن السيبراني وترتيبات السلامة السيبرانية في العالم العربي؛ واتبعت الدراسة المنهج الوصفي التحليلي باعتباره المنهج الأنسب لتحقيق أهداف الدراسة؛ وتوصلت الدراسة إلى مجموعة من النتائج أهمها: أن الدول العربية تتفاوت في درجة تعرضها لمخاطر الجرائم السيبرانية ومدى قدرتها على مواجهة هذه المخاطر، كما أن دول الخليج أقل قدرة على مواجهة مخاطر الهجمات بسبب انخفاض المهارات التقنية بها مقارنة بالدول المتقدمة؛ وأن قلة انتشار وسائل الاتصالات في بعض الدول العربية جعلها أقل عرضة لمخاطر الجرائم السيبرانية، و فيما يخص الجاهزية القانونية والتنظيمية فإن الدول العربية احتلت ترتيباً متأخراً مقارنةً بدول العالم باستثناء عمان، وبينت الدراسة أنه لا يوجد علاقة بين الجاهزية التنظيمية والإدارية للدولة في الأمن السيبراني، وبين القدرة على مجابهة مخاطر الهجمات السيبرانية؛ وخرجت الدراسة بمجموعة من التوصيات أهمها: ضرورة سن تشريعات جديدة تختص بالجرائم السيبرانية، وأهمية إنشاء هيئة حكومية مركزية تختص بكل ما يتعلق بالأمن السيبراني، ووضع استراتيجية وطنية للأمن السيبراني يتم فيها تحديد الأدوار والمسؤوليات بوضوح.

أولاً: مقدمة

يعتبر العصر الحالي هو عصر ثورة المعلومات والاتصالات، وتعد المعلومات هي السمة الأهم للعقود الأخيرة من القرن العشرين، ويرتبط أمن المعلومات ارتباطاً عضوياً بالأمن القومي في معظم دول العالم. فأمن المعلومات هو علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها. ومع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لاخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية . وفي هذا السياق؛ يعتبر الأمن في الفضاء السيبراني، كما هو في العالم المادي، أمراً يهم كل الدول في كل مكان، بغض النظر عن مدى تواجدهم في هذا الفضاء، ذلك أن الاعتداء على البنى التحتية الحساسة، ومنها تلك الخاصة بالاتصالات، يمكن أن يؤثر على كل الدول في منطقة جغرافية معينة، هذا فضلاً عن أثره المباشر على مصالح الدول المعنية بالفضاء السيبراني والتي تشكل بنيتها التحتية للاتصالات والمعلومات جزءاً من تركيبة البنية التحتية للفضاء السيبراني. فهذه العلاقة العضوية تفرض تعاون جميع الحكومات، ليس فقط لضمان أمن بنيتها التحتية، وإنما أيضاً للحاجة الماسة إلى نشر ثقافة الأمن لدى مواطنيها. لذا، فقد ارتقى الاهتمام بأمن المعلومات إلى المراتب الأولى في اهتمامات واضعي السياسات العامة في أغلب دول العالم، وعلى كل المستويات: الدولية والإقليمية والمحلية.

ومن الملاحظ أن لتطورات التكنولوجية في العصر الحديث صاحبتها تطورات كثيرة في سبل الإختراق، ووسائل الوصول غير المشروعة للأنظمة، وانتهاك الخصوصية، والذي بدوره يتطلب وجود قدر كافي من المعرفة والتدريب لجميع الأشخاص العاملين في مجال المعلوماتية.

ولذلك فإن نظام الأمن في الفضاء السيبراني في أي منشأة يجب أن يتضمن وسائل وضوابط رقابية على البيانات حتى يتم تقديم تقارير تحتوي على معلومات موثوق بها من قبل مستخدمي نظام المعلومات.

ومن الأمور التي يُعْنى بها مجال أمن المعلومات : حماية المعلومات من الاختراق، والوصول غير المخول، والاستعمال غير المصرّح به، والتجسس والاطلاع عليها من قبل المتطفلين، والإتلاف، والتدمير، والتعديل، والتفتيش، والنسخ، والتسجيل، والتوزيع، والنشر، ويبحث المختصون في أمن المعلومات في سبيل تحقيق الحماية اللازمة للمعلومات عن أفضل الطرق والسبل والوسائل التي يمكن من خلالها تأمين المعلومات من كلّ الأخطار.

ولا شكّ أن مجال أمن المعلومات له أهميّة كبيرة، فهو مجال يقوم بتأمين المعلومات وحمايتها من الأخطار التي تحيط بها، ويقوم هذا المجال بتوفير الحماية والأمان للحواسيب من البرمجيات الخبيثة التي سبق الكلام عنها، والتي تعد أكبر عدو للحواسيب .ومجال أمن المعلومات هو من المجالات الحيوية والمتجدّدة والمطلوبة كثيرًا، إذ لا غنى عنه أبدًا، وهذا المجال هو علم قائم بحد ذاته، ويدرّس هذا العلم في بعض الجامعات، والمراكز التعليمية، وتمنح فيه شهادات متعدّدة.

إن الغرض من أمن المعلومات هو حماية ما تملكه المؤسسات والهيئات والدول من موارد معلوماتية يتم تخزينها وتداولها من خلال البيئة الحاسوبية، والتي تشكل الأجهزة والشبكات الحاسوبية والبرمجيات والإنترنت أهم عناصرها. وعندما تقوم أي دولة باتخاذ التدابير اللازمة لأمن المعلومات والتي تستهدف تقليل الاحتمالات التي تشكل تهديدا لها، والحد من الأضرار الناجمة عن سوء الأداء، وضمان التعافي في أعقاب وقوع أي حوادث عارضة – سواء كانت مقصودة أو غير مقصودة – في خلال فترة زمنية مقبولة وبتكلفة مقبولة، فإنها بذلك تحافظ على مواردها المالية والمادية، وعلى سمعتها ووضعها القانوني ومواطنيها. فالدولة، أي دولة، هي المعنية الأولى بالأمن السيبراني، لأنها هي المنتج الأكبر للبيانات والمعلومات العامة والخاصة، كما أنها هي التي تضع النظم والقواعد التي تحدد الممنوع والمسموح. (جبريل العريشي، ومحمد الشلهوب، 1436هـ)

إن أجهزة ومكونات تكنولوجيا المعلومات والاتصالات مترابطة بشكل عام، وقد يؤدي تعطيل أحدها إلى التأثير على العديد من العناصر الأخرى .وعلى مدى

السنوات العديدة الماضية، أعرب الخبراء وصانعو السياسات عن مخاوف متزايدة بشأن حماية نظم تكنولوجيا المعلومات والاتصالات من الهجمات السيبرانية، التي يتوقع العديد من الخبراء أن يزداد تواترها وشدتها على مدى السنوات القليلة القادمة.

وقد أصبح قانون حماية أنظمة تكنولوجيا المعلومات والاتصالات ومحتوياتها يعرف بالأمن السيبراني .إن مفهوم الأمن السيبراني يمكن أن يكون مفهوما مفيدا، ولكنه يميل إلى تحدي تعريف دقيق .كما أنه يخلط أحيانا بشكل غير ملائم مع مفاهيم أخرى مثل الخصوصية، وتبادل المعلومات، وجمع المعلومات الاستخبارية، والمراقبة . غير أن الأمن السيبراني يمكن أن يكون أداة هامة في حماية الخصوصية ومنع المراقبة غير المأذون بها، ويمكن أن يكون تبادل المعلومات وجمع المعلومات الاستخبارية أدوات مفيدة لتحقيق الأمن السيبراني.

وتعتبر إدارة المخاطر على نظم المعلومات أساسية للأمن السيبراني الفعال . وتعتمد المخاطر المرتبطة بأي هجوم على ثلاثة عوامل: التهديدات (التي تهاجم)، وأوجه الضعف (نقاط الضعف التي يهاجمونها)، والآثار (ما يفعله الهجوم). ومعظم الهجمات السيبرانية لها آثار محدودة، ولكن الهجوم الناجح على بعض مكونات البنية التحتية الحيوية ، يمكن أن يكون له آثار كبيرة على الأمن القومي والاقتصاد وسبل العيش والسلامة للمواطنين الأفراد .والحد من هذه المخاطر عادة ما ينطوي على إزالة مصادر التهديد، ومعالجة نقاط الضعف، والحد من الآثار . (Eric A. , 2016 Fischer)

وفي ظل عالم رقمي مترابط يعج بالأخطار والكوارث الرقمية، يأتي أمن المعلومات بمفهومه وتطبيقاته وتقنياته ليحاول التغلب على هذه الأخطار والكوارس، ولكن التحديات التي تواجه أمن المعلومات كثيرة وبعضها معقد . فمن بعض تلك التحديات سرعة الهجوم، ففيروس (أو دودة رقمية) سلامر الذي انتشر في 2003 استطاع أن يصيب 75000 حاسوب في أول أحد عشر دقيقة من تفعيله الأولي، بل كان عدد الحواسيب التي تصاب تتضاعف كل ثمانية ثواني، حيث استطاع بعد اثنتي عشرة دقيقة من تفعيله أن يصيب أكثر من مليونين ونصف المليون حاسوب. إنها

سرعة هائلة لا تمّكن الشركات المختصة بكتابة خبر عن انتشارها في هذه السرعة الرهيبة.

ولقد حذر خبراء دوليون في أغسطس 2004 من تفاقم أزمة أمن المعلومات لدول منطقة الخليج العربي، وكانت الإحصاءات تشير إلى أن الاحتياطي المخصص لدول المنطقة العربية للإنفاق على أمن المعلومات حتى عام 2004 لا يتجاوز 200 مليون دولار، في حين أن المطلوب توفيره هو 5 مليارات دولار، وأشارت التقديرات إلى أنه يتعين على القطاع الخاص بمعاونة القطاع الحكومي التعاون في مجال المصارف بشكل خاص وضرورة أن تتبنى إستراتيجية مؤثرة لأمن المعلومات. وانتقد التقرير تساهل المؤسسات والمصارف في الحفاظ على سرية وأمن المعلومات وارجع التقرير، القصور إلى عدم وجود هيئة أو مؤسسة تقوم بتنظيم أمن المعلومات كما أشار التقرير الذي اعتمدته مؤسسة (AGT) الألمانية إلى خطورة هذا الوضع على الأمن القومي للدول العربية التي تمتلك أكثر من 50 ألف مؤسسة متخصصة، ورغم ذلك تعاني من مشاكل في نشاطها في ظل اقتصاد الأمن، وأشار التقرير إلى أنه سيعقد مؤتمرا بمبادرة ألمانية ومشاركة عربية في برلين تحت عنوان) كيفية الأمن للاقتصادات العربية ضد المخاطر الإلكترونية.

وعندما نقول إن أمن المعلومات أصبح من الأولويات في الشرق الأوسط، فإننا لا نوفي الأمر حقّه تمامًا. ففي منطقة تتمتع من جهة بالاستقرار الاقتصادي والسياسي في بلدان مجلس التعاون الخليجي، وتواجه من جهة أخرى تقلبات المشهد السياسي في دول مثل مصر ولبنان وسوريا وإيران، فإن أهمية الأمن المعلوماتي تزداد لتصبح تحديًا رئيسيًا، ليس للشركات الكبرى فحسب بل أيضًا على مستوى الدول. (المركز العربي للبحوث والدراسات) http://www.acrseg.org/36712

وفي الواقع، فإن الشرق الأوسط كان مسرحًا في السنوات الأخيرة لبعض التهديدات الرقمية المتطورة غير المسبوقة وحروبٍ إلكترونية لم يشهدها أي مكان آخر في العالم.

فضلاً عن ذلك فإن المستثمرين في أي دولة إذا لم يجدوا من الأنظمة والقوانين ما يواجه الجرائم السيبرانية التي تقوض الصناعات المعلوماتية، وإذا لم يجدوا دعما من الدولة، وحضورا لأجهزتها، لتنفيذ تلك الأنظمة والقوانين، فإنهم يعزفون عن الاستثمار في هذا المجال وتطويره، وهو ما يؤثر بالسلب على الاقتصاد.

ثانياً: مشكلة الدراسة:

وتتمثل مشكلة الدراسة الحالية في الاجابة على التساؤل الرئيس التالي:

ما هي المخاطر والتحديات التي تواجه أمن المعلومات في العالم العربي؟

ويتفرع من التساؤل الرئيس التساؤلات الفرعية التالية:

١. ما حجم مخاطر الجرائم السيبرانية في العالم العربي؟
٢. ما قدرة العالم العربي على مواجهة مخاطر الجرائم السيبرانية؟
٣. ما أثر الفجوة في قدرات العالم العربي في البحوث والتطوير على الأمن السيبراني؟
٤. ما مدى تأهب النواحي القانونية والتنظيمية للحفاظ على الأمن السيبراني وترتيبات السلامة السيبرانية في العالم العربي ؟

ثالثاً: أهداف الدراسة :

وقد تحددت أهداف الدراسة في التعرف على:

١) حجم مخاطر الجرائم السيبرانية في العالم العربي.
٢) قدرة العالم العربي على مواجهة مخاطر الجرائم السيبرانية.
٣) أثر الفجوة في قدرات العالم العربي في البحوث والتطوير على الأمن السيبراني.
٤) مدى تأهب النواحي القانونية والتنظيمية للحفاظ على الأمن السيبراني وترتيبات السلامة السيبرانية في العالم العربي .

رابعاً: منهج الدراسة

اتبعت الدراسة **المنهج الوصفي التحليلي**، وهو "الذي يهتم بتحديد الواقع وجمع الحقائق عنه وتحليل بعض جوانبه، بما يساهم في العمل على تطويره". (مدحت أبو النصر، 2004، 131 – 132)

وقد تم في هذا الإطار الاطلاع على آراء الباحثين ذات العلاقة بالأمن السيبراني، كما تم الرجوع إلى أحدث التقارير الدولية التي تختص بتقنية الاتصالات والمعلومات، وإخضاع كل ذلك للمقارنة والتفسير والتحليل العلمي، من أجل استنباط ما يتعلق بتحديد هدف الدراسة، واستخدام ذلك في طرح حلول لعلاج جوانب المشكلة. وفي إطار ذلك يتم – في العديد من القضايا– استخدام عمان والسعودية والأردن كنماذج للدول العربية وذلك بغرض إيضاح جوانب المشكلة.

خامساً: مصطلحات الدراسة

أمن المعلومات:

يعرف الباحث أمن المعلومات بإنه العلم الذي يُعنى بتوفير الحماية للمعلومات، وتشمل تلك الحماية القوانين والإجراءات والتشريعات التي تضمن منع المخاطر بجميع أنواعها ومصادرها، وتحقيق الحماية المستمرة للمعلومات.

سادساً– الإطار النظري

مفهوم أمن المعلومات:

تناول العديد من الباحثين والمختصين مفهوم أمن المعلومات من عدة زوايا سوف يتم سرد بعضاً منها كالتالي:

يعرف أمن المعلومات على أنه "العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها"، أما من زاوية تقنية فيعرف أمن المعلومات أنه عبارة عن "الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية"، ومن زاوية قانونية يعرف أمن المعلومات بأنه"محل دراسات وتدابير حماية سرية وسلامة محتوى

وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة".(†) ويعتبر هذا التعريف شامل لأمن المعلومات من شتى النواحي العلمية والعملية والقانونية.

تعريف ميلاد عبد المجيد (2015، 1)، لأمن المعلومات من الناحية الأكاديمية بأنه: "البحث في السياسات والاستراتيجيات التي ينبغي توخيها لحماية المعلومات من مختلف الاعتداءات التي قد تتعرض لها والمخاطر التي يمكن أن تهددها".

أما من الناحية التقنية فقد عرف أمن المعلومات بأنه: "مجموعة الوسائل والتدابير والإجراءات التي يجب توفيرها لتأمين حماية المعلومات من المخاطر المتأتية سواء من داخل بيئة المعلومات محل الحماية أو من خارجها".

ومن الملاحظ أن تعريف ميلاد عبد المجيد يتفق مع التعريف السابق في الناحية العلمية (الأكاديمية) باعتباره علم يبحث في سياسات واستراتيجيات أمن المعلومات ومن الناحية العملية (الفنية) باعتباره الجانب التطبيقي لإجراءات وسياسة حماية أمن المعلومات.

كما يعرف (سلطان ابراهيم، 2000، 396) أمن المعلومات بأنه: "السياسات والإجراءات والمقاييس الفنية والتي تستخدم لتحول دون الوصول غير المتعمد أو السرقة أو التدمير للسجلات".

كما عرفت (Linda, Robinson, 2004, 1) أمن المعلومات بأنه عبارة عن: "السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة لتداول حركات الأعمال إلكترونياً عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الإلكتروني وعلى شركات الأعمال والزبائن والمنظمين والمؤمنين وأي شخص آخر ممكن أن يكون معرضاً لمخاطر الاختراق".

(†) www.arablaw.org/information; p1

ونلاحظ أن تعريف سلطان ابراهيم، و Linda, Robinson يركزان على أمن المعلومات من الناحية التقنية والتي تركز على توفير السياسات والإجراءات اللازمة لحماية المعلومات.

تعريف أحمد جمعة وآخرون (2003، 342) فقد عرفوا أمن المعلومات بأنه: "حماية كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة ويتم ذلك عن طريق اتباع إجراءات ووسائل حماية عديدة تتضمن سلامة وأمن المعلومات.

ومن الواضح أن تعريف أحمد جمعة وآخرون قد ركز على الناحية القانونية (التشريعية) لأمن المعلومات من حيث التركيز على حماية أمن المعلومات وتوضيح الإجراءات والوسائل الواجب اتباعها لضمان سلامة وأمن المعلومات.

ويعد تطبيق أمن المعلومات من شتى النواحي العلمية والعملية والقانونية ذا أثر كبير على زيادة الثقة بنظام المعلومات بصفة عامة.

وقد شاع استخدام مصطلح الأمن السيبراني كمرادف لأمن المعلومات، وذلك بعد أن انتشر مفهوم الفضاء السيبراني(‡)، الذي يرتبط ارتباطاً وثيقاً بالإنترنت وبتكنولوجيا الاتصالات والمعلومات، عبر البنى التحتية المختلفة للاتصالات والأنظمة المعلوماتية، فضلاً عن العديد من الخدمات المعلوماتية التي لم نكن لنحصل عليها من دونه. لذا، تم استخدام مصطلحي "أمن المعلومات" و"الأمن السيبراني" كمترادفين في هذه الدراسة.

أهمية أمن المعلومات

أصبحت نظم الاتصالات والمعلومات تتحكم في مقاليد الدول، وتشكل عصب البنى التحتية في مؤسسات القطاع العام والخاص في كثير من مجالات الحياة: المياه والغذاء والصحة والدفاع والأمن والبنوك والنقل والاتصالات والطاقة وغيرها. وتعمل النظم المعلوماتية التي تتحكم في تلك المجالات في إطار شبكات تربطها معاً،

(‡) Word Net 3.0, Farlex clipart collection. © 2003-2012 Princeton University, Farlex Inc.

والمعلومات التي يجري خلقها ومعالجتها وبثها وتوزيعها واستخدامها معالجتها في هذه النظم، أصبحت هي جوهر الأنشطة الاقتصادية والاجتماعية في مجتمع المعلومات، وهو ما يجعلها عرضة للخطر، وربما لتقويض سيادة الدولة، حيث أصبحت تشكل الأهداف المحتملة لأي هجوم سيبراني. فالغنيمة التي يسعى لها المهاجمون ليست هي هذه النظم بحد ذاتها، ولكنها هي تلك المعلومات. فقد تنال الجرائم السيبرانية من القدرة على المعالجة والتخزين، كما قد تشوه الرصيد المعلوماتي أو تتلفه، بل ويمكن لها أن تنزل الضرر بالسلع غير الملموسة وبعمليات الإنتاج، وبعمليات صنع القرار. مما يحتم ضرورة بذل المزيد من الاهتمام لتأمين تلك النظم في مواجهة الهجوم أو الانتهاك أو المخاطر التي تنشأ بالمصادفة، أو بسبب الخطأ البشري، أو الجهل بطبيعة عملها، وذلك بغرض حماية المعلومات من الوصول غير المصرح به إليها، ومن الاستخدام غير القانوني لها، ومن الإفصاح عنها لمن ليس لهم حق معرفتها، ومن محاولات السيطرة عليها أو تعديلها أو إلغائها أو إتلافها.

إن التهديدات المتنامية بارتكاب الجرائم السيبرانية من قبل جهات تملك قدرات وموارد كبيرة، وتصاعد نجاح المهاجمين في سرقة أرقام بطاقات الاعتماد والبيانات المالية، يؤديان إلى فقدان الثقة بالتقنيات المستخدمة، وعدم الاطمئنان الى سلامة المعاملات في عمليات التجارة الالكترونية. ومن شأن توفير سبل الحماية أمام تلك التهديدات أن يتحقق الاستقرار الاقتصادي للفضاء السيبراني ويصبح بيئة موثوقا بها، وهو أمر أساسي تتطلع إليه المؤسسات عند أداء الأعمال، كما يتطلع إليه الأفراد لتحقيق التواصل الأمن فيما بينهم [§]. (الاتحاد الدولي للاتصالات، ومؤسسة ABI للأبحاث، 2015)

ولا يقتصر أمن الفضاء السيبراني على المؤسسات والأفراد، أو على الأموال التي تمثلها البنية التحتية والتجهيزات المستخدمة في صناعته، بل إنه يمتد ليصبح أيضا أمنا للدول والأنظمة السياسية والاجتماعية، ولجميع البنى التحتية الحساسة المرتبطة به. لذا، فلا يقف اهتمام الدول على تعزيز الأمن في الفضاء السيبراني عند

[§] http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-A.pdf

حدود الاهتمامات الاقتصادية والتنموية، بل إنه يتعداه إلى الاهتمام بحماية الأمن القومي. (جبريل العريشي، ومحمد الشلهوب، 1436هـ)

وتُظهر كثير من الاستبيانات التي تم إجراؤها أنَّ عدد ضحايا الجرائم السيبرانية يبلغ أضعاف عدد ضحايا الجرائم التقليدية. فتتراوح معدّلات المضارين من تزوير بطاقات الائتمان وانتحال الشخصية على الإنترنت والوقوع ضحية لمحاولات التصيُّد الاحتيالي ومحاولات الاطلاع بدون إذن على حسابات البريد الإلكتروني ما بين 1% و17% من نسبة السكان الذين يستخدمون الإنترنت في٢١ بلدًا في على مستوى العالم، بينما يبلغ معدل المضارين من السطو والسلب وسرقة السيارات التقليدية أقل من 5% من نسبة السكان في هذه البلدان نفسها. كما أن معدلات المضارين من الجرائم السيبرانية في البلدان التي تشهد مستويات نمو منخفضة أعلى من البلدان ذات النمو المرتفع مما يُبرز الحاجة إلى تعزيز جهود منع الجرائم في هذه البلدان. [(**)]

وساعد الاستخدام الواسع للأجهزة الإلكترونية من ازدياد وسائل وسبل الإختراق، والتي تهدف بمجملها إلى إيقاع الخطر بالنظم المعلوماتية.

لذا، فيمكننا القول بأن بناء مجتمع المعلومات يصحبه العديد من الممارسات عبر الإنترنت تستلزم متابعتها ومراقبتها بواسطة أخصائيين وباستخدام أدوات وتقنيات خاصة، وهو ما يعني أن كل الأنشطة الرقمية التي يتم ممارستها في مجتمع المعلومات تحتاج إلى أن يتم وضعها في سياق شامل للأمن السيبراني الذي يتقاطع مع جميع الصناعات وجميع القطاعات، من أجل أن تكون آمنة الاستخدام.

مخاطر المعلومات الإلكترونية

تعتبر المعلومات الإلكترونية من النظم التي تواجه العديد من المخاطر التي قد تؤثر على تحقيق أهداف تلك النظم وذلك نظراً لاعتمادها على الحاسوب، حيث تزامن التطور الكبير للحاسبات وأنظمة المعلومات مع التطور في تكنولوجيا المعلومات وسرعة انتشار هذه المعلومات واستخدامها إلكترونياً، ولقد صاحب هذا التطور في

(**) UNODC - دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتَّخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدِّي لها- فينا- 2013م.

استخدام المعلومات الإلكترونية العديد من المخاطر والمشاكل التي تؤثر على أمن المعلومات سواء كانت تلك المخاطر مقصودة أو غير مقصودة.

ولذلك تزايد الاهتمام الكبير بتوفير الوسائل والأساليب اللازمة لحماية المعلومات والرقابة على عملياتها وضمان استمرارية عمل تلك النظم بشكل صحيح وبالطريقة المطلوبة التي صممت من أجلها.

استراتيجية أمن المعلومات

تعرف استراتيجية أمن المعلومات أو سياسة أمن المعلومات بأنها: "مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها"[††].

ومن خلال ما سبق نصل إلى أن استراتيجية أمن المعلومات عبارة عن القواعد التي تحدد كيفية الوصول إلى المعلومات والتعامل معها.

وتعد استراتيجية أمن المعلومات مهمة جداً للحفاظ على المعلومات بحيث تمنع الأشخاص الذين لا يحق لهم الوصول إلى المعلومات أن يصلوا إلى تلك المعلومات أو التعامل معها أو التعرف عليها.

أهداف استراتيجية أمن المعلومات

ولكي تعتبر استراتيجية أمن المعلومات ناجحة وفعالة وقابلة للتطبيق فلا بد أن يشارك في إعدادها وتنفيذها جميع المستويات الوظيفية التي لها علاقة بتلك الاستراتيجية حيث تسعى تلك المستويات إلى انجاح تلك الاستراتيجية من خلال تحقيق أهداف استراتيجية أمن المعلومات والتي تتمثل في[‡‡]: تعريف مستخدمي المعلومات ومختلف الإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات والمعلومات بكافة أشكالها وفي مختلف مراحل جمعها وادخالها ومعالجتها ونقلها عبر الشبكات وإعادة استرجاعها عند الحاجة.

[††] www.arablaw.org/information, 24
[‡‡] www.arablaw.org/information; 28

تحديد وضبط الآليات التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة لكل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر.

بيان الإجراءات المتبعة لتفادي التهديدات والمخاطر وكيفية التعامل معها عند حصولها والجهات المكلفة بالقيام بذلك.

عناصر أمن المعلومات

من أجل حماية المعلومات من المخاطر التي تتعرض لها لا بد من توفر مجموعة من العناصر التي يجب أخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد تم تصنيف تلك العناصر إلى خمسة عناصر هي: (ميلاد، 2006، 18)

- **السرية أو الموثوقية Confidentiality**

وهي تعني التأكد من أن المعلومات لا يمكن الاطلاع عليها أو كشفها من قبل أشخاص غير مصرح لهم بذلك ولتجسيد هذا الأمر يجب على المؤسسة استخدام طرق الحماية المناسبة من خلال استخدام وسائل عديدة مثل عمليات تشفير الرسائل أو منع التعرف على حجم تلك المعلومات أو مسار إرسالها.

- **التعرف أو التحقق من هوية الشخصية Authentication**

وهذا يعني التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما إذا كان هو المستخدم الصحيح لتلك المعلومات أم لا، ويتم ذلك من خلال استخدام كلمات السر الخاصة بكل مستخدم، وتوضح مؤسسة (RSA) لأمن المعلومات(§§ ثلاث طرق للتحقق من الشخصية وهي: الأولى عن طريق شيء يعرفه الشخص مثل كلمة المرور، والثانية عن طريق شيء يملكه مثل رسالة الشيفرة (Token)وهي عبارة عن كود يقوم بإدخاله المستخدم للحاسوب للحيازة على صلاحيات التشغيل أو الشهادة الإلكترونية، والثالثة عن طريق شيء يتصف به الشخص من الصفات الفيزيائية مثل بصمة الإصبع أو المسح الشبكي أو نبرة

(§§) RSA Security Inc, www.rsasecurity.com

الصوت، وكل طريقة لها إيجابياتها وسلبياتها، وتنصح مؤسسة (RSA) باستخدام طريقتين مع بعضهما البعض من هذه الطرق الثلاثة.

- **سلامة المحتوى (Integrity)**

وهي تعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو تدميره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء كان التعامل داخليا في المشروع أو خارجيا من قبل أشخاص غير مصرح لهم بذلك ويتم ذلك غالبا بسبب الاختراقات الغير مشروعة مثل الفيروسات حيث لا يمكن لأحد أن يكسر قاعدة بيانات البنك ويقوم بتغيير رصيد حسابه لذلك يقع على عاتق المؤسسة تأمين سلامة المحتوى من خلال اتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات أو الفيروسات.

- **استمرارية توفر المعلومات أو الخدمة (Availability)**

وهي تعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمات لمواقع المعلومات وضمان عدم تعرض مستخدمي تلك المعلومات إلى منع استخدامها أو الوصول إليها بطرق غير مشروعة يقوم بها أشخاص لإيقاف الخدمة بواسطة كم هائل من الرسائل العبثية عبر الشبكة إلى الأجهزة الخاصة لدى المؤسسة.

- **عدم الإنكار (No repudiation)**

ويقصد به ضمان عدم إنكار الشخص الذي قام بإجراء معين متصل بالمعلومات لهذا الإجراء، ولذلك لا بد من توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص للشخص الذي قام به في وقت معين، ومثال ذلك للتأكد من وصول بضاعة تم شراؤها عبر شبكة الإنترنت إلى صاحبها، ولإثبات تحويل المبالغ إلكترونيا يتم استخدام عدة رسائل مثل التوقيع الإلكتروني والمصادقة الإلكترونية.

العوامل التي تساعد على اختراق المعلومات

تعتبر المعلومات الإلكترونية أقل أماناً من المعلومات اليدوية وذلك نظراً لاعتماد المعلومات الإلكترونية على حفظ بياناتها في ملفات إلكترونية يستطيع عدد

كبير من الأشخاص الوصول إليها والاطلاع عليها، ولذلك فإن المعلومات الإلكترونية قد تتعرض للعديد من المخاطر التي قد تهدد أمنها وذلك بسبب مجموعة من العوامل وهي كما يلي: (سلطان ابراهيم، 2000، 393- 394).

- ❖ المعلومات الإلكترونية تتضمن كم هائل من البيانات ولذلك فإنه يصعب عمل نسخ ورقية لها
- ❖ صعوبة اكتشاف الأخطاء الناتجة عن التغير في المعلومات الإلكترونية وذلك لأنه لا يمكن التعامل أو قراءة سجلاتها إلا بواسطة الحاسب والذي لا يكشف أي تغيير.
- ❖ صعوبة مراجعة الإجراءات التي تتم من خلال الحاسب وذلك لأنها غير مرئية وغير ظاهرة.
- ❖ صعوبة تغيير النظم الآلية مقارنة بالنظم اليدوية.
- ❖ احتمال تعرض النظم الآلية إلى إساءة استخدامها بواسطة الخبراء غير المنتمين للمنظمة في حال استدعائهم لتطوير النظم.
- ❖ قد تؤدي المخاطر التي تتعرض لها النظم الآلية إلى تدمير كافة سجلات المنظمة وبذلك فهي أشد خطورة على النظم الآلية من النظم اليدوية.
- ❖ انخفاض المستندات التي يمكن من خلالها مراجعة النظام تؤدي إلى انخفاض حالة الأمان اليدوية.
- ❖ احتمال تعرض النظم الآلية إلى حدوث أخطاء أو إساءة استخدام النظام في مرحلة تشغيل البيانات وذلك لتعدد عمليات التشغيل في النظام الآلي.
- ❖ ضعف الرقابة على النظام الآلي بسبب الاتصال المباشر للمستخدم بنظم المعلومات.
- ❖ التطور التكنولوجي في الاتصال عن بعد سهل عملية الاتصال بنظم المعلومات من أي مكان وبالتالي إمكانية الوصول غير المسموح به أو إساءة استخدام نظم المعلومات.

- ❖ استخدام العديد من التطبيقات في مواقع مختلفة لنفس قاعدة البيانات يؤدي إلى إمكانية اختراقها بفيروسات الحاسب وبالتالي امكانية تدمير أو تغيير قاعدة البيانات لنظام المعلومات.

ومن خلال ما سبق نجد أنه ينبغي على إدارة المؤسسة العمل على حماية بياناتها بكافة أشكالها، سواء كانت ورقية أو غير ورقية، كما أن نظام المعلومات الإلكتروني يكون عرضة للمخاطر أكثر من غيره من النظم ولذلك لابد للإدارة من وضع قيود على المستخدمين تحد من إمكانية التلاعب بالبيانات أو العبث بها سواء من أطراف داخل المؤسسة أو خارجها.

المخاطر التي يمكن أن تتعرض لها المعلومات الالكترونية

يعتبر موضوع حماية البيانات من الأمور الواجب الاهتمام بها في كافة مراحل إعداد نظم المعلومات حيث أن أمن البيانات والمعلومات أصبح من أهم عناصر الرقابة الواجب تطبيقها على المعلومات من خلال التخطيط المستمر خلال دورة حياة نظم المعلومات المستخدمة.

وتعتبر المخاطر المقصودة أشد خطراً على أداء فعالية النظم وتزداد تلك الخطورة في النظم الإلكترونية، وتكمن خطورة مشاكل أمن المعلومات في عدة جوانب منها تقليل أداء الأنظمة الحاسوبية، أو تخريبها بالكامل مما يؤدي إلى تعطيل الخدمات الحيوية للمنشأة، أما الجانب الآخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الاطلاع والتصنت على المعلومات السرية أو تغييرها إلى خسائر مادية أو معنوية كبيرة.(***)

ويصنف (Abu-Musa, 2004, 3: 9) مخاطر تهديدات أمن المعلومات الإلكترونية من وجهات نظر مختلفة إلى عدة أنواع:

(***) (www.ksu.edu.sa/security/ahdaf.html)

من حيث مصدرها: (The Source of Threats)

- ✓ **مخاطر داخلية (Internal):** حيث يعتبر موظفي المنشآت هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية وذلك لأن موظفي المنشآت على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق لدى المنشأة، ومعرفة نقاط القوة والضعف ونقاط القصور لهذا النظام ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم، ولذلك فإن موظفي الشركة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تغييرها. (bu–Musa, 2004, 2: 3)
- ✓ **مخاطر خارجية (External):** وتتمثل في أشخاص خارج المنشأة ليس لهم علاقة مباشرة بالمنشأة مثل قراصنة المعلومات والمنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات سرية عن المنشأة أو قد تتمثل في كوارث طبيعية مثل الزلزال والبراكين والفيضانات (والتي قد تحدث تدمير جزئي أو كلي للنظام في المنشاة. (Abu–Musa, 2004, 2: 4)

من حيث المتسبب بها: (The perpetrator)

- ✓ **مخاطر ناتجة عن العنصر البشري (Human Threats):** وتلك الأخطاء قد تحدث من قبل أشخاص بشكل مقصود وبهدف الغش والتلاعب أو بشكل غير مقصود نتيجة الجهل أو السهو أو الخطأ.
- ✓ **مخاطر ناتجة عن العنصر الغير بشري (Non–Human):** وهي تلك المخاطر التي قد تحدث بسبب كوارث طبيعية ليس للإنسان علاقة بها مثل حدوث الزلازل والبراكين والفيضانات والتي قد تؤدي إلى تلف النظام ككل أو جزء منه.

من حيث أساس العمدية (Intention)

- ✓ **مخاطر ناتجة عن تصرفات متعمدة (مقصودة) (Intentional):** وتتمثل في تصرفات يقوم بها الشخص متعمدا مثل ادخال بيانات خاطئة وهو يعلم ذلك، أو قيامه بتدمير بعض البيانات متعمدا ذلك بهدف الغش والتلاعب والسرقة، وتعتبر هذه المخاطر من المخاطر المؤثرة جدا على النظام.
- ✓ **مخاطر ناتجة عن تصرفات غير متعمدة (غير مقصودة) (Accidental):**وتتمثل في تصرفات يقوم بها الأشخاص نتيجة الجهل وعدم الخبرة الكافية كإدخالهم لبيانات بطريقة خاطئة بسبب عدم معرفتهم بطرق ادخالها أو السهو في عملية التسجيل وتعتبر هذه المخاطر أقل ضرراً من المخاطر المقصودة وذلك لإمكانية إصلاحها.

من حيث الآثار الناتجة عنها(Consequences)

- ✓ **مخاطر ينتج عنها أضرار مادية (Physical Damage):** وهي المخاطر التي تؤدي إلى حدوث أضرار للنظام وأجهزة الكمبيوتر أو تدمير لوسائل تخزين البيانات والتي قد يكون سببها كوارث طبيعية لا علاقة للإنسان بها أو قد تكون بسبب البشر بطريقة متعمدة أو عفوية.
- ✓ **مخاطر فنية ومنطقية (Technical or Logical):** وهي المخاطر الناتجة عن أحداث قد تؤثر على البيانات وإمكانية الحصول عليها للأشخاص المخول لهم بذلك عند الحاجة لها أو إفشاء بيانات سرية لأشخاص غير مصرح لهم بمعرفتها وذلك من خلال تعطيل في ذاكرة الكمبيوتر أو إدخال فيروسات للكمبيوتر قد تفسد البيانات أو جزء منها وتلك المخاطر قد تؤثر على الموقف التنافسي للمنشأة.
- ✓ وقد تحدث المخاطر السابقة من خلال قيام المهاجم بالبحث في مخلفات التقنية الخاصة بالمؤسسة من قمامة وأوراق متروكة بهدف الحصول على أية معلومات قد تساعد على اختراق النظام للحصول على كلمات السر المدونة على الأوراق الملقاة أو الأقراص الصلبة التي يتم استبدالها، أو أي معلومة

أخرى تساهم في اختراق النظام والتي تعرف بتقنية القمامة، ونستطيع أن ندرك درجة خطورة تقنية القمامة من خلال معرفة ما حصل مع وزارة العدل الأمريكية.

حيث قامت وزارة العدل الأمريكية ببيع مخلفات أجهزة تقنية بعد أن تقرر اتلافها وكان من ضمن تلك المخلفات جهاز كمبيوتر يحتوي قرصه الصلب على كافة العناوين الخاصة ببرنامج حماية الشهود وخوفا من نشر تلك المعلومات أو استثمارها ضد الوزارة فقد قامت وزارة العدل بنقل كافة الشهود وتغيير مكان اقاماتهم وهوياتهم وهذا تطلب تكلفة مالية ضخمة وذلك بسبب الاخفاق في اتلاف الأقراص بطريقة صحيحة. (†††)

المخاطر على أساس علاقتها بمراحل النظام

- **مخاطر المدخلات (Input):** وهي المخاطر الناتجة عن عدم تسجيل البيانات في الوقت المناسب وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال خطوط الاتصال، وتتمثل المخاطر المتعلقة بأمن المدخلات إلى أربعة أقسام أساسية هي: خلق بيانات غير سليمة، تعديل أو تحريف بينات المدخلات، حذف بعض المدخلات، ادخال البيانات أكثر من مرة.
- **مخاطر التشغيل (Processing):** ويقصد بها المخاطر المتعلقة بالبيانات المخزنة في ذاكرة الحاسب والبرامج التي تقوم بتشغيل تلك البيانات وتتمثل مخاطر تشغيل البيانات في الاستخدام غير المصرح به لنظام وبرامج التشغيل وتحريف وتعديل البرامج بطريقة غير قانونية أو عمل نسخ غير قانونية أو سرقة البيانات الموجودة على الحاسب الآلي، ومثال على ذلك قيام الموظف بإعطاء أوامر للبرنامج بأن لا يسجل أي قيود في السجلات المالية تتعلق بعمليات البيع الخاصة بعميل معين من أجل الاستفادة من مبلغ العملية لصالح المحرف نفسه.

(†††) www.arablaw.org/information ; p.11

- **مخاطر المخرجات (Output):** ويقصد بها المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عملية تشغيل ومعالجة البيانات، وقد تحدث تلك المخاطر من خلال طمس أو تدمير بنود معينة من المخرجات أو خلق مخرجات زائفة وغير صحيحة أو سرقة مخرجات الحاسب أو إساءة استخدامها أو عمل نسخ غير مصرح بها من المخرجات أو الكشف الغير مسموح به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق أو طبع وتوزيع المعلومات بواسطة أشخاص غير مسموح لهم بذلك، كذلك توجيه تلك المطبوعات والمعلومات خطأ إلى أشخاص ليس لهم الحق في الاطلاع على تلك المعلومات أو تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها مما يؤدي إلى استخدام تلك المعلومات في أمور تسيء إلى المؤسسة وتضر بمصالحها.
- **مخاطر بيئية:** وهي المخاطر التي تحدث بسبب عوامل بيئية، مثل الزلازل والعواصف والفيضانات والأعاصير المتعلقة بأعطال التيار الكهربائي والحرائق، وسواء كانت تلك الكوارث طبيعية أو غير طبيعية فإنها قد تؤثر على عمل النظام المحاسبي وقد تؤدي إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة مما يؤثر على أمن وسلامة نظم المعلومات المحاسبية الالكترونية.

أسباب حدوث المخاطر التي تواجه أمن المعلومات الإلكترونية

تتعرض المعلومات الإلكترونية للعديد من المخاطر التي تهدد أمنها وقد تم تقسيم تلك المخاطر إلى أربعة أقسام رئيسة تتعلق بمراحل النظام الأساسية من ادخال وتشغيل ومخرجات والقسم الرابع يتعلق بالمخاطر البيئية وقد ترجع أسباب حدوث تلك المخاطر إلى أسباب تتعلق بالمدخلات والمخرجات وأسباب تتعلق بالتشغيل أو قد نعتبرها أسباب إدارية رقابية وأسباب لها علاقة بالموظفين، وتتلخص تلك الأسباب في البنود التالية:

١. عدم كفاية وفعالية الأدوات الرقابية المطبقة لدى إدارة المنشأة.
٢. ضعف نظم الرقابة الداخلية لدى المنشأة وعدم فعاليتها.
٣. اشتراك بعض الموظفين في استخدام نفس كلمات السر من أجل الدخول إلى النظام والعبث بمحتوياته.
٤. عدم الفصل بين المهام والوظائف المتعلقة بالمعلومات الإلكترونية في المنشأة.
٥. عدم وجود سياسات واضحة وبرامج محددة ومكتوبة فيما يختص بالأمن السيبراني لدى المنشأة.
٦. عدم توفر الحماية الكافية ضد مخاطر الفيروسات الإلكترونية.
٧. ضعف وعدم كفاءة النظم الرقابية المطبقة على المخرجات الالكترونية.
٨. عدم وجود سياسات وبرامج محددة ومكتوبة لأمن المعلومات الإلكترونية بالمنشأة.
٩. عدم التوصيف الدقيق للهيكل الوظيفي والاداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي لدى المنشأة.
١٠. عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي المنشأة
١١. عدم الزام الموظفين بأخذ إجازاتهم الدورية.
١٢. عدم الاهتمام الكافي بفحص التاريخ الوظيفي المهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.
١٣. عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي المنشأة.
١٤. عدم وجود الوعي الكافي لدى الموظفين بضرورة فحص أي البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر.

متطلبات أمن المعلومات والحد من حجم مخاطر الجرائم السيبرانية

تعتبر مسألة حماية أمن المعلومات الإلكترونية من المسائل الهامة والضرورية والتي ينبغي على المؤسسة أخذها بعين الاعتبار ووضع خطة حماية شاملة في حدود إمكانياتها التنظيمية والمادية ويجب أن تكون تلك الحماية قوية وليست ضعيفة ولذلك فإنه توجد عدة متطلبات لحماية أمن المعلومات، وتقليل حجم مخاطر الجرائم السيبرانية تتمثل في: (Jessup, 2013, 145)

١ .وضع سياسة حماية عامة لأمن المعلومات الإلكترونية تتحدد حسب طبيعة عمل المنشأة.

٢ .يجب على الإدارة العليا في المنشأة دعم أمن المعلومات لديها.

٣ .يجب أن توكل مسؤولية أمن المعلومات في المؤسسة لأشخاص محددين.

٤ .تحديد الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة.

٥ .تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية.

٦ .الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل آمن.

٧ .تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط.

٨ .تأمين استمرارية عمل وجاهزية نظم المعلومات خاصة في حالة الأزمات ومواجهة مخاطر الجرائم السيبرانية.

أساليب الرقابة على المعلومات الإلكترونية

مع تطور تكنولوجيا المعلومات ومع الانتشار الواسع لتطبيق المعلومات بطرق إلكترونية أصبحت هناك حاجة ماسة لحماية تلك النظم من المخاطر التي تتعرض لها وتوفير أساليب الرقابة اللازمة لحماية المعلومات الإلكترونية وضمان إنجاز عملياتها بالشكل الصحيح وفي الوقت المناسب ولذلك فإن الرقابة على المعلومات الإلكترونية تقسم إلى ثلاث مجموعات رئيسية حسب مراحل النظام وهي:

-الرقابة على المدخلات

وهي تهدف إلى التأكد من أن البيانات التي تم إدخالها إلى النظام أدخلت في الوقت المناسب وبشكل صحيح، وضمان سير تلك البيانات خلال خطوط الاتصال

وعدم فقدها أو تغييرها واكتشاف أي أخطاء تتعلق بالبيانات قبل عملية تشغيلها وذلك لضمان خلو البيانات المدخلة من أي أخطاء وليتم الحصول على مخرجات سليمة بناء على مدخلات سليمة ولذلك فلابد من الحصول على مدخلات البيانات في مرحلة مبكرة من مراحل معالجتها في النظام، وذلك (للأسباب التالية): (عبد الرازق قاسم، 2003، 358)

١ .امكانية تصحيح الأخطاء التي تم اكتشافها في البيانات التي تم رفضها في بداية ادخالها والرجوع إلى المستندات الخاصة بها وفحص أسباب رفضها.

٢ .أن البيانات التي تم ادخالها بشكل صحيح ليس من الضرورة أن تكون بيانات جيدة ولذلك يجب اجراء اختبارات أخرى لفحصها خلال مراحل تداولها ومعالجتها.

٣ .خلو نظام المعلومات المحاسبي من بيانات غير دقيقة في المراحل الأخيرة لعمليات المعالجة يمكن من حماية ووقاية الملفات الرئيسية وعمليات المعالجة في خطواتها الأخيرة.

٤ .اعتماد نظام المعلومات المحاسبي على مدخلات جيدة يمكنه من الحصول على مخرجات جيدة.

-الرقابة على تشغيل البيانات

وهي تهدف إلى التحقق من أن البيانات تم تشغيلها بصورة دقيقة وبشكل صحيح وأنه تم معالجة كافة العمليات المتعلقة بالتشغيل وقد تم استخدام جميع البرامج المناسبة واللازمة لعملية التشغيل، ومن أهم الوسائل الرقابية على تشغيل العمليات ما يلي: (كمال الدين الدهراوي، 2003، 188)

١ .تطبيق الاختبارات التي تضمن صحة عمليات التشغيل بحيث يتم رفض التعامل مع المدخلات أو المخرجات غير الصحيحة.

٢ .استكمال مسار المراجعة الذي يمكن من تتبع سجل عملية من عمليات التشغيل والمساعدة في إعداد القوائم.

٣ .تزويد برامج التشغيل بوظائف ومهام تمكن من تسجيل أي عملية محاولة للتدخل في عمل البرنامج أثناء عملية التشغيل والمعالجة.

- الرقابة على المخرجات

وهي تهدف للتأكد من أن نتائج مخرجات عملية التشغيل كاملة وصحيحة وجيدة ودقيقة، وأنه تم تسليمها وتوزيعها للأشخاص المسموح لهم باستلامها والاطلاع عليها، وتستند الرقابة على المخرجات على البند السابق وهو عملية الرقابة على التشغيل، فإذا كانت الرقابة على المدخلات وعلى عملية التشغيل جيدة ودقيقة فهذا يؤدي إلى الحصول على مخرجات سليمة ودقيقة.

حماية أمن المعلومات الإلكترونية:

لتحقيق متطلبات أمن وحماية المعلومات الإلكترونية فلابد للمؤسسة من اتباع عدة اجراءات للحماية ومنها:(Jessup, 2013, 149)

١ .اجراءات الحماية الفيزيائية لنظم المعلومات بما فيها الحماية المادية للأجهزة التي تحتوي على نظم المعلومات.

٢ .انتقاء العاملين في النظم المعلوماتية بحيث يكونوا ذوي خبرة وثقة وأمانة ويعملون لمصلحة المنشأة وتوعيتهم أمنياً للمحافظة على أمن المعلومات.

٣ .إجراءات الحماية الخاصة بنظم تشغيل البيانات والبرامج التطبيقية اللازمة لذلك وضبط الصلاحيات الخاصة بنظم التشغيل.

٤ .إجراءات الحماية الخاصة بالشبكات المعلوماتية ومنع اختراقها.

٥ .العمل على تشفير المعلومات التي يتم تخزينها ونقلها حتى لا يتم معرفة ماهيتها في حالة الحصول عليها من أشخاص غير مصرح لهم بذلك.

٦ .إجراءات حفظ البيانات بصورة عامة وحفظ نسخ منها في مواقع آمنة يمكن الرجوع إليها عند الحاجة لذلك.

7. إجراءات ضمان استمرارية عمل وجاهزية نظم المعلومات في شتى الظروف التي قد تواجه النظم، مثل تعطل أو توقف النظم المعلوماتية عن العمل.

إجراءات الحماية المتبعة لمواجهة مخاطر الجرائم السيبرانية:

تعتبر قضية تطبيق حماية أمن المعلومات قضية مهمة جداً لدى المؤسسات والشركات التي تعتمد في عملها على تكنولوجيا المعلومات، حيث تسعى المؤسسات إلى حفظ أمن نظمها المعلوماتية من خلال تطبيق شتى وسائل الحماية مثل جدران النار "والذي يعتبر أحد وسائل أمن المعلومات والذي صمم لمنع الوصول الغير مصرح به من وإلى الشبكة الخاصة، ويتم بناؤه من خلال القطع المادية والبرمجيات".(Volonino, Robinson, 2004, p199)

إضافة إلى برامج مكافحة الفيروسات وطرق حماية تقنية أخرى، ولكن هذا الأمر يعتبر خطير جداً ولا يمكن أن نضمن نجاحه بدون إدارة ممتازة، وإجراءات تشغيلية جيدة، حيث يقع على عاتق المنشأة إصدار القرارات الإدارية المتعلقة بأمن نظم المعلومات لتجنب مخاطر الجرائم السيبرانية التي يمكن أن تتعرض لها.

ومع ذلك فإننا نجد أنه مع قيام الشركات بتطبيق وسائل الحماية المطلوبة إلا أن هناك بعض الاقتراحات الناجحة لنظم المعلومات، كما أن كل كتب أمن الشركات أوضحت أن الأمن السيبراني أساساً قضية إدارية وليست تكنولوجية، فبدون تغيير جوهري في ثقافة أمن السيبراني وممارساته، فإن شراء التكنولوجيا سوف لا يجلب إلا قليلاً من الأمن السيبراني، ولذلك فإن على المنشآت اتباع العديد من الإجراءات لمواجهة مخاطر الجرائم السيبرانية ومن تلك الإجراءات: (Panko, Raymond R, 2004, 22)

-تعهد التزام الإدارة العليا

حيث يقع على عاتق الإدارة العليا للشركة الالتزام بشكل قوي بتطبيق أمن المعلومات، كما أن الإدارة العليا لتكنولوجيا المعلومات تحتاج أيضا إلى التزام قوي بتطبيق أمن المعلومات، فأمن المعلومات يعتبر دائماً سبباً غير مرغوباً لأقسام تكنولوجيا المعلومات في الشركة. (Panko, Raymond R, 2004, 31)

فمثلاً في سنة (2002) أوضحت ردود استطلاع (Network World Survey) أن أعلى خمس اهتمامات في تكنولوجيا المعلومات كانت اهتمامات الأمن

السيبراني، وحماية الشبكة، وتحسين أنظمة الاسترجاع من الكوارث، وبناء شبكات افتراضية خاصة. (John cox, 2002, 18)، لذلك هذه الردود المتشابهة تقول أيضاً أنهم خططوا فقط لزيادة ميزانية أمن المعلومات بمعدل 5%.

- تنفيذ الإجراءات المطلوبة

وهي حرجة أيضاً لأفراد تكنولوجيا المعلومات، وموظفي الشركة الآخرين، لتنفيذ مهام أمن المعلومات بشكل مخلص وجيد، فمعظم الهجمات تستفيد من الاختراقات الناتجة من الإعدادات الغير صحيحة لأدوات الأمن السيبراني، وكذلك بسبب فشل الموظفين التشغيليين في تغطية نقطة ضعف أمن معروفة في البرمجيات. (Panko, Raymond R, 2004, 32)

ولذلك يجب على إدارة الشركة متابعة موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة من مخاطر الجرائم السيبرانية.

-وضع الإجراءات ومعاقبة الموظفين

ربما الشيء المقيت جداً، أنه من الحرج أن تنفذ إجراءات الأمن السيبراني من خلال إقرار موظفين يقومون بكسر هذه الإجراءات، فالمبدأ الأساسي للإدارة أن تحصل على ماذا تريد أن تنفذ، حيث أن كثيراً من موظفي المستوى التشغيلي، وحتى مدراء الإدارة العليا سوف يكسرون إجراءات الأمن السيبراني لكي يجعلوا حياتهم أفضل أو لأسباب أخرى، وما دام المنتهكين لا يعاقبون، فالأمن لا يمكن له أن يزدهر، وبالطبع فإن المعنيين بالأمن السيبراني يحتاجون للتدريب على وسائل حماية أمن معلوماتهم من مخاطر الجرائم السيبرانية، ويجب أن يكونوا واقعيين باقتراح العقوبات. وبشكل عام ينبغي على إدارة الشركة أن تضع قواعد خاصة لحماية الأمن السيبراني من مخاطر الجرائم السيبرانية ومعاقبة الموظفين المخلين بهذه القواعد. (Panko, Raymond R, 2004, 32)

- تطبيق خطة الأمن السيبراني الشاملة

من الدروس الحرجة الأخرى التي تدرس بواسطة حوادث الأمن السيبراني المؤلمة، هو أن الشركة يجب أن تملك خطة شاملة لأمن المعلومات، فيجب عليها أن تغلق جميع أبواب الاختراق وبينما تقوم المؤسسة بحماية نفسها من الاختراق يحاول المهاجم اكتشاف نقطة ضعف واحدة لكي يخترق من خلالها الأنظمة، ولذلك فإن إحدى الطرق لتحسين الحماية هو انشائها بشكل معمق، لأن المهاجم يحاول كسرها خلال اجراءات مضادة ومتعددة يقوم بها بشكل متكرر حتى ينجح، فمثلاً تقوم الشركة بوضع عدة جدران نارية (Firewalls) واحد منهم رئيسي والأخرى متفرعة، فيقوم المهاجم بمحاولة اختراقها كلها للوصول إلى النظام المستهدف، ومع أن اجراءات الحماية صعبة الإعداد، فإنه من السهل وجود اختراق، حتى ولو كانت المؤسسة تعتقد أنها تمتلك حماية شاملة إلا أنه من المهم أيضاً امتلاك تدقيق الحماية (Security Audit) ، حيث أن مجموعة الهجوم قد تُوظف لدى الشركة لكي تحاول اختراق النظام، ولكي تكون المؤسسة آمنة فلا بد لها من تحقيق الأهداف الجوهرية لحماية أمن المعلومات من مخاطر الجرائم السيبرانية.

دورة التخطيط-الحماية-الاستجابة (Plan-Protect-Respond PPR)

الشركات المهتمة جدا بالحماية الشاملة من مخاطر الجرائم السيبرانية يجب أن تمر إجراءات تطبيقها خلال عملية تدعى التخطيط-الحماية-الاستجابة (PPR) .

* **التخطيط:** يشمل تخطيط الحماية الشاملة، فالمهاجمين يحتاجون نقطة ضعف واحدة للاختراق

ويندرج تحت هذه المرحلة: (Panko, Raymond R, 2004, 37 – 39)

- **تحليل المخاطر:** فيجب على المؤسسة تحليل المخاطر المتعلقة بأمن المعلومات، كما يجب عليها تحديد حجم النفقات التي ستصرفها في سبيل وضع إجراءات الحماية.

- **سياسات الحماية:** حيث يتم تطبيق هذه السياسات على نطاق واسع داخل المؤسسة، فمثلاً تسمح المؤسسة بإجازة لموظفيها لمدة أسبوعين سنوياً على أن يكون منها أسبوعا بشكل متتالي، والغرض من ذلك كشف حالات الغش لدى الموظفين.
- **وضع سياسات إرشاد تشمل الإجراءات والفحص:** ويقصد بذلك وضع مجموعة محكمة وشاملة من السياسات التي يجب أن توضع لترشد الأفعال التي تحدث في المستوى الأدنى من المؤسسة، ويشمل ذلك وضع السياسات التي تتحكم بالتكنولوجيا مثل وضع سياسة لربط الشبكة الداخلية للمؤسسة مع الشبكة العالمية (الإنترنت)، تتضمن هذه السياسة احتياج المؤسسة من جدران النار (Firewalls) وأماكن تشغيلها وأن تتحكم السياسات بالإجراءات.

* **الحماية:** من الملاحظ دائماً أن أمن المعلومات لدى المؤسسة يكون مفتوحاً خلال مرحلة الحماية، وأحياناً يقوم المهاجم بكشف نقطة ضعف في هذه المرحلة وربما تكون ناجحة، وتشمل طرق الحماية تركيب الأجهزة الخاصة بالحماية مثل جدران النار(Firewalls) وتنزيل البرامج اللازمة لها، وإعدادها برمجياً بما يتناسب مع سياسات الحماية المطلوبة، وأن يتم تحديث طرق الحماية باستمرار، لأن أدوات الحماية تصبح غير مفيدة مع مرور الوقت، وتشمل أيضًا فحص طرق الحماية والإعدادات الخاصة بها باستمرار، وهو ما يسمى بتدقيق أمن المعلومات.

* **الاستجابة:** يقوم المهاجم باختراق الأنظمة أحياناً وينجح في ذلك حتى مع وجود حماية قوية، فإذا حصل مثل هذا الحادث ولم تكن هناك خطة موضوعة لتقليل مخاطر هذا الحادث، تكون عملية الرجوع للأنظمة بوضعها الطبيعي عملية صعبة ومستحيلة، لذلك يجب على المؤسسة أن تضع إجراءات صارمة تشمل إنتاج تقارير رسمية لتعريف وتحديد حادث الاختراق وتحديد المهاجمين وإيقافهم وإصلاح الدمار الناتج، وفي بعض الحالات معاقبة المهاجمين.

أمن المعلومات في العالم العربي من منظور المخاطر التقنية

تشير العديد من الدراسات إلى وجود دلائل على أن الدول التي توجد بها بنية تحتية متواضعة للإتصالات والمعلومات مع نظم قانونية مليئة بالثغرات، تشجع الهاكرز على استخدامها كمنصات – أو نقط انطلاق– لهجماتهم السيبرانية، كما أنها تصبح هي نفسها عرضة للهجمات السيبرانية طالما ظلت غير قادرة على بناء بنية تحتية قوية مدعومة بنظم قانونية محكمة تعالج قضايا أمن المعلومات. وهناك دلائل على أن الانتشار الجغرافي للفيروسات والديدان الرقمية يتعقب أماكن وجود الفجوات الرقمية، ويكون أكثر انتشارا من خلال الأجهزة النقالة في البلدان ذات مجتمعات المعلومات الناشئة. (ICSC In: Fathiya, 2014, 21)

وثمة من يرى أن الدول التي تضم مجتمعات المعلومات الناشئة، تواجه العديد من الثغرات الأمنية الناشئة عن الفجوة الرقمية الكبيرة، وهي الثغرات التي ينبغي معالجتها من خلال وضع قضايا الأمن السيبراني في الاعتبار منذ اللحظة الأولى التي تشرع فيها في تطوير بنيتها التحتية. (ICSC In: Fathiya, 2014, 23)

سابعاً– الدراسات السابقة:

يعتبر موضوع أهمية مخاطر المعلومات الإلكترونية من المواضيع الهامة والحديثة نسبياً، حيث أنه من خلال مراجعة الدراسات والأبحاث السابقة والمتعلقة بهذا الموضوع نجد أن هناك ندرة في العالم العربي حول هذا الموضوع مع توفر دراسات قليلة في العالم الغربي وهذا إن دل على شيء فإنما يدل على الحداثة النسبية لهذا الموضوع رغم أهميته الحيوية لكثير من المنشآت الهامة.

وتجدر الإشارة إلى أن الأبحاث القليلة التي تمت في هذا الموضوع قد استهدفت التعرف على المخاطر المحتملة التي قد تواجه أو تهدد أمن تلك النظم والتعرف على أسبابها ومحاولة تطوير قائمة تتضمن أهم المخاطر التي قد تواجه الأمن السيبراني، ومن ثم محاولة اختبار مدى جوهرية وأهمية تلك المخاطر في الواقع العملي من خلال مجموعة من الدراسات الميدانية التي تمت في هذا الشأن، وذلك من خلال التعرف على معدل تكرار حدوثها وحجم الخسائر الناجمة عنها. ومن هذه الدراسات :

- دراسة قام بها Abu-Musa, (2001) لاستكشاف واختبار المخاطر الهامة التي تهدد أمن المعلومات المحاسبية الإلكترونية في القطاع المصرفي بمصر، حيث قام Abu-Musa بعمل دراسة مسحية شملت جميع البنوك الرئيسية العاملة بجمهورية مصر العربية مستخدماً في ذلك استمارة استقصاء للتعرف على أراء كل من رؤساء أقسام الحاسب الألى ورؤساء أقسام المراجعة الداخلية فيما يختص بالمخاطر الهامة التي تهدد أمن المعلومات الإلكترونية في البنوك التي يعملون بها، ولقد تم الحصول على ردود تتمثل في ٧٩ استمارة استقصاء من بينها ستة وأربعون استمارة استقصاء تم استيفاء بياناتها من قبل رؤساء أقسام الحاسب الألى، وثلاثة وثلاثون تم ملئ بياناتها بواسطة رؤساء أقسام المراجعة الداخلية، ومن ثم كانت نسبة الردود هي 79% فيما يختص بأقسام الحاسب الألى و57% فيما يختص بأقسام المراجعة الداخلية. ومن خلال تلك الدراسة قام Abu-Musa بتطوير قائمة شملت تسعة عشر من المخاطر المحتملة لأمن المعلومات الإلكترونية لاختبار مدى تواجدها وأهميتها في البيئة المصرية، وتضمنت تلك القائمة بعض المخاطر المحتملة التي تم اختبارها لأول مرة في تلك الدراسة والتي تتعلق بصفة أساسية بمخاطر الأمن السيبراني، ولقد تضمنت القائمة المخاطر الأتية:
  - الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.
  - الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.
  - التدمير غير المتعمد(غير المقصود) للبيانات بواسطة الموظفين.
  - التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين.
  - المرور (الوصول) غير الشرعي (غير المرخص به) للبيانات/ النظام بواسطة الموظفين.
  - المرور غير الشرعي (غير المرخص به) للبيانات/ النظام بواسطة أشخاص من خارج المنشأة.
  - اشتراك الموظفين في كلمة السر.

- الكوارث الطبيعية مثل الحرائق، الفيضانات أو انقطاع مصدر الطاقة.
- الكوارث غير الطبيعية والتي هي من صنع الإنسان مثل الحرائق، أو الفيضانات.
- إدخال فيروس الكمبيوتر للنظام المحاسبي.
- طمس أو تدمير بنود معينة من المخرجات.
- خلق مخرجات زائفة /غير صحيحة.
- سرقة البيانات /المعلومات.
- عمل نسخ غير مصرح (مرخص) بها من المخرجات.
- الكشف (الإظهار) غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.
- طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.
- المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم/ ليس لهم الحق في استلام نسخة منها
- المستندات الحساسة يتم تسليمها إلى أشخاص لا تتوافر فيهم الناحية الأمنية وذلك بغرض تمزيقها.
- مقاطعة تحويل البيانات من أماكن بعيدة.

وتشير نتائج الدراسة إلى أن الإدخال غير المتعمد لبيانات غير صحيحة من قبل الموظفين، التدمير غير المتعمد للبيانات من قبل الموظفين، إدخال فيروس الكمبيوتر إلى النظام، الكوارث الطبيعية والكوارث التي هي من صنع الإنسان، اشتراك بعض الموظفين في استخدام نفس كلمة السر، وكذلك توجيه البيانات والمعلومات إلى أشخاص غير مخول لهم باستلامها تعد من أهم المخاطر التي تواجه أمن المعلومات الإلكترونية في المنشآت، وتجدر الإشارة إلى أنه في جميع الحالات فإن رؤساء أقسام المراجعة الداخلية قد أعطوا تقديرات أعلى لمعدلات حدوث تلك المخاطر في المنشآت التي يعملون بها مقارنة بتقديرات رؤساء أقسام الحاسب الألى، وتشير نتائج الدراسة

أنه لا توجد اختلافات جوهرية بين أنواع المنشآت المختلفة إلا فيما يختص بالمرور غير المرخص به للبيانات/ النظام من قبل أطراف خارجية (قراصنة المعلومات).

- دراسة (Loch, et al, 2002) من أوائل الدراسات في هذا المجال حيث استهدفت استكشاف مدى إدراك مديري المعلومات فيما يتعلق بالمخاطر الأمنية التي تواجه الأمن السيبراني في بيئة الحاسبات الشخصية والحاسبات الكبيرة وكذلك شبكة الحاسبات الإلكترونية، كما قام بتطوير قائمة تضمنت إثنى عشرة من المخاطر المحتملة التي تواجه أمن المعلومات الإلكترونية بناء على الأبحاث النظرية المتاحة وكذلك محاولة اختبار مدى وجود وأهمية تلك المخاطر عملياً من خلال البحث الميداني، ولقد تضمنت تلك القائمة المخاطر التالية:
  - الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة موظفي المنشأة.
  - الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة موظفي المنشأة.
  - التدمير غير المتعمد للبيانات بواسطة موظفي المنشأة.
  - التدمير المتعمد للبيانات بواسطة موظفي المنشأة.
  - المرور (الوصول) غير المرخص للبيانات/ النظام بواسطة موظفي المنشأة.
  - الرقابة غير الكفاية على الوسائل Media، مثل الأشرطة والأقراص الممغنطة.
  - الرقابة الضعيفة على المناولة اليدوية لمدخلات ومخرجات الحاسب الألى.
  - الوصول غير المرخص به للبيانات/ النظام بواسطة أطراف خارجية قراصنة المعلومات Hackers .
  - الوصول غير المرخص به للبيانات/ النظام من قبل المنافسون.
  - إدخال فيروسات الكمبيوتر إلى النظام أو البرامج.
  - الأدوات الرقابية المادية غير الكافية.
  - الكوارث الطبيعية مثل الحرائق والفيضانات أو انقطاع مصدر الطاقة وغيرها.

- ولقد قام الباحثون بعمل دراسة مسحية شملت ٦٥٧ من مديري المعلومات في الولايات المتحدة، وطُلب من المشاركين في الدراسة أن يقوموا بترتيب أهم ثلاث مخاطر فيما يتعلق بأمن المعلومات الإلكترونية من بين بنود القائمة المقترحة للمخاطر، وأوضحت النتائج أن الكوارث الطبيعية والأحداث غير المقصودة لموظفي المنشأة قد تم تصنيفها ضمن الثلاث مخاطر الهامة في جميع بيئات تكنولوجيا المعلومات، كما أعطى المشاركون في الدراسة أهمية أكبر للمخاطر الداخلية مقارنة بالمخاطر الخارجية لأمن المعلومات الإلكترونية، كما أظهرت الدراسة أن التدمير غير المتعمد للبيانات والإدخال غير المتعمد لبيانات غير سليمة بواسطة موظفي المنشأة وكذلك الرقابة غير الكافية على الوسائل مثل الأشرطة والأقراص الممغنطة تُعد أهم ثلاث مخاطر تواجه أمن المعلومات فيما يتعلق بأجهزة الحاسب الشخصية، بينما أوضحت الدراسة أن أهم ثلاث مخاطر تتعلق بأجهزة الحاسب الألى الكبيرة تتمثل في الإدخال غير المتعمد لبيانات غير سليمة من قبل موظفي المنشأة، الكوارث الطبيعية، والتدمير غير المتعمد للبيانات بواسطة موظفي المنشأة، بينما أظهرت الدراسة أن الكوارث الطبيعية والدخول غير المصرح به للبيانات/ النظام من قبل أطراف خارجية (قراصنة المعلومات) وضعف الأدوات الرقابية المادية تعد أهم ثلاث مخاطر تهدد أمن المعلومات الإلكترونية في بيئة شبكة الحاسب الآلي.
- دراسة (Abu-Musa, 2004) حيث قام بعمل دراسة تطبيقية للتعرف على المخاطر الهامة التي تهدد أمن المعلومات الإلكترونية في المنشآت السعودية، وأظهرت نتائج الدراسة أن نسبة عالية من المنشآت التي شاركت في الاستقصاء قد عانت من وجود خسائر مالية كبيرة نتيجة بعض التعديات على أمن المعلومات بها سواء من قبل أطراف داخلية (موظفي المنشأة) أو أطراف خارجية (قراصنة المعلومات)، وأن تلك الخسائر قد تراوحت ما بين 100,000 و200 مليون ريال سعودي، كما أوضحت الدراسة أن كثيراً من تلك التلاعبات والاختلاسات والتعديات على أمن المعلومات قد تم اكتشافها عن طريق الصدفة نتيجة لعدم

كفاية وفعالية الأدوات والضوابط الرقابية المطبقة في تلك المنشآت، وأن معظم الاختلاسات والتلاعبات التي تم اكتشافها قد تم تسويتها داخلياً ولم يتم الإفصاح أو التقرير عنها للجمهور حفاظاً على سمعة الشركة وتحسين صورتها في السوق، أما فيما يختص بمدى إدراك المنشآت السعودية للمخاطر الهامة التي تهدد المعلومات ومعدلات تكرار حدوث تلك المخاطر بها، حيث أشارت النتائج إلى أن أهم المخاطر التي تهدد الأمن السيبراني في المنشآت السعودية هي: الإدخال المتعمد وغير المتعمد لبيانات غير صحيحة بواسطة موظفي المنشآت، إدخال فيروسات الكمبيوتر إلى النظام المحاسبي، مشاركة الموظفين في استخدام نفس كلمات السر، طمس أو تدمير مخرجات الحاسب الآلي، الكشف (الإظهار) غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الأوراق، وكذلك توجيه المطبوعات والمعلومات إلى أشخاص غير مخول لهم باستلام تلك المعلومات أو الإطلاع عليها، ولم تظهر النتائج أي اختلافات جوهرية بين المنشآت المختلفة فيما يختص بتقديرها لأهمية المخاطر التي تهدد أمن المعلومات الإلكترونية في بيئة الأعمال السعودية.

- دراسة (Ryan and Bordoloi, 2007)وهي دراسة تطبيقية لتقييم مخاطر أمن المعلومات في النظم الإلكترونية في المنشآت التي تحولت من نظام أجهزة الكمبيوتر الكبيرة إلى نظام خدمة العملاء، ولقد قام الباحثان بتطوير قائمة شملت خمسة عشر من المخاطر المحتملة التي قد تهدد أمن المعلومات الإلكترونية بناء على الدارسات السابقة والأبحاث التي تمت في هذا الشأن، ولقد قام الباحثان بتوزيع قائمة استقصاء على مائة وعشرين شركة من الشركات الكبيرة والمتوسطة الحجم في الولايات المتحدة، وتم الحصول على ردود من ٥٢ شركة بما يعادل ٤٧% من عدد الاستبيانات التي تم توزيعها، ولقد طلب من المشاركين في الاستبيان أن يقوموا بترتيب مدى خطورة وأهمية المخاطر المحتملة لأمن المعلومات الإلكترونية في بيئة أجهزة الحاسب الألى الكبيرة وكذلك في نظام خدمة العملاء مستخدمين في ذلك 10-Point Scale، وتشير نتائج تلك الدراسة إلى

وجود فروق جوهرية (عند مستوى معنوية p = 0.05) بين المنشآت التي لديها نظام أجهزة الكمبيوتر الكبيرة وتلك التي تطبق نظام خدمة العملاء فيما يختص بمخاطر أمن المعلومات الإلكترونية التالية: التدمير غير المتعمد للبيانات بواسطة موظفي المنشأة، الإدخال غير المتعمد لبيانات خاطئة بواسطة موظفي المنشأة، التدمير المتعمد للبيانات بواسطة موظفي المنشأة، الإدخال المتعمد لبيانات خاطئة بواسطة موظفي المنشأة، الخسائر الناجمة عن عدم إعداد نسخ إضافية Backups أو الرقابة على ملفات الدخول للنظام Log Files أو فشل النظام وسقوط الشبكات، وقد أعترف الباحثان أن قائمة المخاطر، المقترحة من قبلهم قد تضمنت بعض العناصر التي لا يمكن اعتبارها ضمن مخاطر أمن المعلومات بالمعنى الدقيق.

- دراسة (Are Nakrem ,2007) والتي أكدت على أنه لا يوجد نظرية بعينها في مجال أمن المعلومات ولكن هناك العديد من المحددات والأطر والمعايير والبحوث، وأكدت الدراسة أيضاً على أن أمن المعلومات وبخاصة في خلال السنوات القليلة الماضية أصبح قضية في غاية الأهمية بالنسبة للشركات الكبري وعلى مستوى العالم، وأكدت أيضاً على أن فم أمن المعلومات يعتمد بدرجة كبيرة على سلوك الموظفين والعاملين حيث أن الدراسة أرجعت نسبة 20% تتأثر بالامكانات التكنولوجية المساندة و نسبة 80% يتأثر بالسلوك البشري ، وقد قدمت هذه الدراسة مفهوماً مختصراً لأمن المعلومات في العبارة التالية " حمياة المعلومات الالكترونية من الاستخدامات غير القانونية" ، وقد ألقت الدراسة الضوء على تعريف الوعي الأمني على أنه درجة أو مستوى إلمام كل فرد أو موظف وتطبيقة للنقاط التالية:
  - أهمية أمن المعلومات .
  - مستويات أمن المعلومات اللازمة للمؤسسة التي يعمل بها.
  - مسئوليات الحفاظ على أمن المعلومات لكل فرد داخل المؤسسة .

- دراسة قام بها (Dhillon, 2009) تتعلق بطبيعة اختراقات أمن المعلومات التي حدثت في أماكن مختلفة من العالم، حيث ناقش فيها العديد من خسائر أمن المعلومات التي تنتج من الاحتيال على أنظمة الحاسوب، حيث أنه يمكن تفادي هذه الخسائر إذا تبنت المنظمات نظرة أكثر واقعية في التعامل مع مثل هذه الحوادث بالإضافة إلى تبني نظرة تحكم أمنية تضع تأكيدا متساويا للتدخلات الشكلية والرسمية والتقنية لأنظمتها الإلكترونية، ومن خلال نتائج الدراسة اقترح بأن تطبيق السيطرة، كما هو معروف في سياسة أمن المعلومات، يردع حقيقية سوء استعمال الحاسوب، كما أن ارتكاب الاحتيال على أنظمة الحاسوب من قبل المستخدمين الداخليين، تعرف كمشاكل التخزين، واحتيال أنظمة الحاسوب عالية التقنية يصعب منعها خاصة إذا امتزجت بالمعاملات القانونية.
- دراسة أخرى (Siponen, 2009) قدمت تصوراً لبرنامج وعي أمن المعلومات في المؤسسات وذلك لتقليل أخطاء المستخدمين، ولتحسين فعالية سيطرة الأمن المطبقة توصلت إلى أن تقنيات أو إجراءات أمن المعلومات تفقد فائدتها الحقيقية إذا تم إساءة استخدامها، أو تم تفسيرها بطريقة خاطئة أو تم تطبيقها بشكل غير صحيح من قبل المستخدمين.
- دراسة (Michael E. Whitman, 2011) وقد ركزت على إجابة ثلاثة أسئلة، السؤال الأول يتعلق بحصر التهديدات التي تواجه أمن المعلومات، والثاني يتعلق بدرجة خطورة هذه التهديدات، والثالث يتعلق بعدد مرات حدوثها (شهرياً)، حيث قام الباحث بعمل تقييم لعدد من الأبحاث والمقالات في مجال أمن المعلومات، وحصر التهديدات التي تواجه أمن المعلومات لتشمل اثنتي عشرة وهي كالتالي: الخطأ أو الفشل البشري (حوادث، أخطاء المستخدمين)، سرقة الحقوق الذهنية والفكرية (قرصنة، انتهاك حقوق الطبع)، أفعال التجسس المتعمدة (وصول غير مخول)، أفعال متعمدة لابتزاز المعلومات (ابتزاز كشف المعلومات)، أفعال متعمدة للتخريب أو التدمير (دمار الأنظمة أو المعلومات)، أفعال متعمدة للسرقة (مصادرة غير شرعية من الأجهزة أو المعلومات)، هجوم متعمد للبرمجيات

(فيروسات، نكران الخدمة، حصان طروادة)، قوة الطبيعة (نار، فيضان، زلزال، برق)، نوعية انحرافات الخدمة من مجهزو الخدمة (قضايا متعلقة بالشبكة وقوتها)، حالات فشل أو أخطاء أجهزة تقنية (فشل أجهزة)، حالات فشل أو أخطاء البرامج التقنية (أخطاء برمجية، فجوات مجهولة)، تقادم تكنولوجي، ثم قام الباحث بعمل دراسة مسحية شملت ١٠٠٠موظف أغلبهم من مدراء المعلومات، والمدراء ومشرفين، وطلب من المشاركين أن يقوموا بترتيب أهم ثلاث مخاطر فيما يتعلق بأمن المعلومات من بين بنود القائمة المقترحة للمخاطر، وأوضحت النتائج أن الهجوم المتعمد للبرمجيات وحالات فشل أو أخطاء البرامج التقنية والخطأ أو الفشل البشري قد تم تصنيفها ضمن الثلاث مخاطر الهامة في جميع بيئات تكنولوجيا المعلومات، وفيما يتعلق بعدد التهديدات الشهرية لأمن المعلومات، أوضحت الدراسة أن بعض التهديدات لم يتم اكتشافها، مثل الأفعال المتعمدة لابتزاز المعلومات، والاستملاك الغير شرعي للمعلومات من المنظمة، نسب معظمهم ذلك إلى الطبيعة الشريرة للدخلاء، لكن بشكل عام معظم المستجيبين أشاروا إلى حدوث معظم التهديدات سواء داخلية أو خارجية، كما أوضحت النتائج أن التهديد حقيقي، وخطورته عالية، وأن الأنظمة المعرضة للتهديد يصعب حمايتها، وركزت الدراسة على أن الإدارة يجب أن تكون مطلعة أكثر على تهديدات أمن المعلومات، ويجب أن يزداد وعيها في كل المجالات، وأن مستوى فهمهم العام لأمن المعلومات متأصل من علاقتها مع البيئة التي تعمل بها.

- دراسة (Mattias Hanson, et al. 2015) التي حاولت التعرف على الاتجاهات المعاصرة في أمن المعلومات من منظور دولة السويد، وقد توصلت هذه الدراسة إلى بعض النتائج الهامة التي أمكن استخلاصها في النقاط التالية :

– صعوبة تتبع التطور المستمر في مجال أمن المعلومات لما يتصف به من كونه عملية معقدة ومتشابكة ، وتتصف قضية امن المعلومات باتساعها مما يجعل الأمر صعباً على المختصين للتنبؤ بمستقبل أمن المعلومات .

– كما انتهت الدراسة أيضاً بتحديد دواعي التطور التكنولوجي وهي:

1- السلوك البشري .

2- التطورات العالمية .

3- الخدمات المستحدثة.

4- الأحداث الفردية التي تؤثر على سلوكياتنا جميعاً.

وقد أكدت الدراسة أيضاً أن قصة أمن المعلومات في غاية التشابك والصعوبة وتتصف بالتغير المستمر والسريع، وأنه أصبح لزاماً أن يتم رفع مستوى وعي الأفراد بأمن المعلومات وعلى الدول أن تهتم بنشر ثقافة أمن المعلومات ، وتدريب متخذي القرار على قضية أمن المعلومات وأهميتها في كافة القطاعات.

- وأخيراً جاءت دراسة (Eric A. Fischer ,2016) التي هدفت إلى تحديد مخاطر الأمن السيبراني ، فقد ذكرت أن المخاطر المرتبطة بأي هجوم تعتمد على ثلاثة عوامل: التهديدات (التي تهاجم)، وأوجه الضعف (نقاط الضعف التي يهاجمونها)، والآثار (ما يفعله الهجوم). وتعتبر إدارة المخاطر التي تتعرض لها نظم المعلومات أساسية بالنسبة للأمن السيبراني الفعال هي 5 فئات.
  - **ما هي التهديدات من وجهة نظر دراسة Eric ؟** ويقال على نطاق واسع أن الأشخاص الذين يحتمل أن يؤديوا الهجمات الإلكترونية أو يحتمل أن يكونوا قد وقعوا في فئة واحدة أو أكثر من الفئات الخمس: المجرمون الراغبون في تحقيق مكسب نقدي من جرائم مثل السرقة أو الابتزاز؛ جواسيس نية على سرقة المعلومات السرية أو الملكية التي تستخدمها الجهات الحكومية أو الخاصة؛ المحاربين من الدولة القومية الذين يطورون القدرات ويتعرضون للهجمات الإلكترونية دعما للأهداف الاستراتيجية للبلد؛ " hacktivists " الذين يقومون بهجمات إلكترونية لأسباب غير نقدية؛ والإرهابيين الذين يشاركون في الهجمات الإلكترونية كشكل من أشكال الحرب غير الحكومية أو التي ترعاها الدولة.

- **ما هي نقاط الضعف؟** الأمن السيبراني هو من نواح كثيرة سباق التسلح بين المهاجمين والمدافعين .أنظمة تكنولوجيا المعلومات والاتصالات معقدة جدا، والمهاجمون يبحثون باستمرار عن نقاط الضعف، والتي يمكن أن تحدث في العديد من النقاط .يمكن للمدافعين حماية في كثير من الأحيان من نقاط الضعف، ولكن ثلاثة تحديا بشكل خاص: أعمال غير مقصودة أو متعمد من قبل المطلعين مع الوصول إلى نظام؛ نقاط الضعف في سلسلة التوريد، والتي يمكن أن تسمح بإدراج البرامج الضارة أو الأجهزة أثناء عملية الاستحواذ؛ و غير معروفة سابقا، أو صفر يوم، نقاط الضعف مع عدم وجود إصلاح ثابت .وحتى بالنسبة إلى مواطن الضعف التي تكون فيها سبل الانتصاف معروفة، فإنها قد لا تنفذ في كثير من الحالات بسبب قيود الميزانية أو العمليات.
- **ما هي الآثار؟** ويمكن أن يؤدي الهجوم الناجح إلى المساس بسرية ونزاهة وتوافر نظام تكنولوجيا المعلومات والاتصالات والمعلومات التي يعالجها . يمكن أن يؤدي الانتحار الإلكتروني أو التجسس الإلكتروني إلى تسلل المعلومات المالية أو الملكية أو الشخصية التي يمكن للمهاجم الاستفادة منها، وغالبا بدون معرفة الضحية .ويمكن أن تؤدي هجمات الحرمان من الخدمة إلى إبطاء أو منع المستخدمين الشرعيين من الوصول إلى النظام .بوتنيت البرمجيات الخبيثة يمكن أن تعطي أمر المهاجم من نظام لاستخدامها في الهجمات الإلكترونية على أنظمة أخرى .يمكن أن تؤدي الهجمات على أنظمة التحكم الصناعية إلى تدمير أو تعطيل المعدات التي تسيطر عليها، مثل المولدات والمضخات وأجهزة الطرد المركزي.

من خلال ما سبق نجد أن جميع الدراسات السابقة ركزت على أهمية المخاطر التي تواجه الأمن السيبراني وأنواع تلك المخاطر، ولكن لم يتم دراسة أسباب حدوث المخاطر أو التعرف على الاجراءات اللازمة من أجل مواجهة تلك المخاطر ومنع حدوثها، ولذلك فإن البحث الحالي قد ركز على التعرف على حجم تلك المخاطر

والجرائم السيبرانية التي يواجهها العالم العربي ومدى قدرته على مجابهتها، إضافة إلى معرفة أسباب حدوث تلك المخاطر وإجراءات الحماية المتبعة ضد المخاطر التي تواجه الأمن السيبراني.

ثامناً- نتائج الدراسة التحليلية

ويتم في هذه الجزئية الإجابة عن تساؤلات الدراسة التي تتعلق بتوضيح حجم مخاطر الجرائم السيبرانية في العالم العربي والناجمة عن الآثار المحتملة للفجوة الرقمية التي تعاني منها الدول العربية بصورة متفاوتة، كما تحاول الدراسة أيضاً تحليل لتقدير قدرة العالم العربي على مجابهة تلك المخاطر، والتعرف على أثر الفجوة في قدرات العالم العربي في البحوث والتطوير على الأمن السيبراني ، وأخيراً بيان مدى تأهب النواحي القانونية والتنظيمية للحفاظ على الأمن السيبرني وترتيبات السلامة السيبرانية في العالم العربي.

وفي النهاية تقدم الدراسة بعض التوصيات التي تختص بالأمن السيبراني والتي يمكن استنتاجها للحد من المخاطر التي تهدد الأمن في الفضاء السيبراني.

التساؤل الأول: ما حجم مخاطر الجرائم السيبرانية في العالم العربي؟

لكي نقيس حجم مخاطر الجرائم السيبرانية في العالم العربي فسنقوم باستخدام ما ورد من معلومات في الدراسة التفصيلية لتقييم تطور تقنية الاتصالات والمعلومات في العالم – والتي تم إجراؤها بواسطة الاتحاد الدولي للاتصالات، الذي قام بنشر نتائجها في تقريره عام 2014 (ITU, 2014).

وقد تم في هذا التقرير استخدام مؤشر رئيس كمعيار لمقارنة مدى تطور تقنية الاتصالات والمعلومات بين دول العالم المختلفة، وتم تحديد ثلاثة مؤشرات فرعية تمثل في مجموعها قيمة هذا المؤشر الرئيس:

الأول: مؤشر النفاذ، للدلالة على درجة "نفاذ " تقنية الاتصالات والمعلومات في الدولة، ويتم حسابها بناء على عدد المشتركين في خدمات الهاتف الثابت والنقال، ومتوسط سرعة الاتصال بالإنترنت bandwidth، وعدد الأسر التي تقتني أجهزة

حاسوبية، وعدد المنازل التي يتاح لها خدمة الاتصال بالإنترنت. ويشكل هذا المؤشر الفرعي40% من قيمة المؤشر العام لتطور التقنية

الثاني: مؤشر الاستخدام للدلالة على درجة "استخدام" التقنية، ويتم حسابه بناء على عدد مستخدمي الإنترنت، وعدد المشتركين في خدمة النطاق العريض السلكية واللاسلكية. ويشكل هذا المؤشر الفرعي 40% من قيمة المؤشر العام لتطور التقنية.

الثالث: مؤشر المهارات للدلالة على درجة " المهارة الفنية" في استخدام التقنية، ويتم حسابه على أساس درجة تعلم المهارات التقنية. ونظرا لصعوبة قياس هذا المؤشر الثالث، فقد تم استخدام عدد الملتحقين بالتعليم في المراحل المختلفة باعتباره مؤشرا بديلا لدرجة تعلم مهارات التقنية، باعتبار أن من يتقدمون للتعليم والتدريب التقني هم من المتعلمين بصفة عامة ومن الحاصلين على مؤهل عال على وجه الخصوص. لذلك فإن هذا المؤشر الفرعي يشكل 20% فقط من قيمة المؤشر العام لتطور التقنية.

وسنقوم فيما يلي بإطلاق مصطلح "انتشار التقنية" للدلالة على درجة نفاذ التقنية ودرجة استخدامها، كلاهما معاً. كما سنقوم باعتبار أن المؤشر العام لتطور التقنية الذي أوجده الاتحاد الدولي للاتصالات هو – في نفس الوقت– مؤشر على درجة انتشار التقنية، حيث أن مؤشري النفاذ والاستخدام – اللذين يمثلان معا درجة انتشار التقنية– يشكلان 80% من قيمة المؤشر العام لتطور التقنية.

يشير تقرير الاتحاد الدولي للاتصالات – السالف ذكره– إلى أن المتوسط العام لتطور تقنية الاتصالات والمعلومات للدول العربية مجتمعة في عام 2013 يبلغ 4,55 وهو يقل– قليلا– عن المتوسط العالمي العام للمؤشر والذي يبلغ 4,77.

ويبين الشكل التالي وضع الدول العربية بالنسبة لمناطق العالم الأخرى فيما يخص تطور تقنية الاتصالات والمعلومات:

ويشير التقرير إلى أن دول الخليج بالإضافة إلى لبنان تحظي بترتيب مرتفع يزيد عن المتوسط العام لدول العالم وذلك في قيمة المؤشر العام لتطور التقنية، وهو ما يتضح من الشكل السابق، وتزداد قيمة هذا المؤشر في هذه الدول عاما بعد عام وهو ما يعني أن هناك تطورا مستمرا بها، فضلا عن أن هذه الدول تحظى بترتيب مرتفع بين دول العالم بالنسبة للمؤشرات الفرعية الدالة على درجة نفاذ التقنية ودرجة استخدامها.

ومن منظور أمن المعلومات، فإن زيادة درجة نفاذ تقنيات الاتصالات والمعلومات وزيادة عدد مستخدميها – أي زيادة انتشار تقنية الاتصالات والمعلومات– في هذه المجموعة من الدول العربية يؤديان إلى زيادة المخاطر الناجمة عن أعمال التجسس السيبراني، وسرقة المعلومات، واختراق الأنظمة، ومن ثم تزداد الحاجة في تلك الدول إلى وضع ترتيبات لأمن المعلومات والتدريب على المهارات اللازمة لإدارتها. (Pimienta: Pimienta In: Fathiya, 2014)

أي أن بناء مجتمع المعلومات من خلال التركيز على تطوير البنى التحتية لتقنية المعلومات لا يعد وحده أمرا كافيا، بل يجب في نفس الوقت أخذ احتياجات الأمن السيبراني في الاعتبار منذ اللحظة الأولى، بحيث تندمج مع البنى التحتية ولا تكون منفصلة عنها، وبهذا فقط يمكن لتلك الدول (دول الخليج ولبنان)، أن تحصل

على المميزات الخالصة لمجتمع المعلومات، مثل الدول المتقدمة، وتنجو من أن يتم اعتبارها إحدى الحلقات الضعيفة في سلسلة الأمن السيبراني الدولي والتي يستقر فيها الهاكرز أو يستخدمونها كمنصة ينطلقون منها لارتكاب جرائمهم . (Ghernaouti in: Fathiya & George, 2014)

ويشير التقرير إلى أنه فيما يخص باقي الدول العربية فإن قيمة المؤشر العام لتطور التقنية فيها تقل عن المتوسط العام لدول العالم، كما يلاحظ فيها تأخرا عن الأعوام السابقة بالنسبة للترتيب العام.

ومن منظور التعرض لمخاطر الهجمات السيبرانية فيمكننا القول بأن سكان هذه الدول أقل عرضة للهجمات السيبرانية من سكان المجموعة الأولى (دول الخليج ولبنان)، حيث أن العامل الرئيسي الذي يمنع ملايين البشر في هذه الدول من أن يسقطوا كضحايا للجرائم السيبرانية هو ضعف انتشار التقنية الذي يجعلهم محرومين من استخدام الإنترنت، حيث كلما ازدادت إتاحة الإنترنت – وزاد عدد المستخدمين لها – يزداد بالتالي عدد ضحايا الجرائم السيبرانية. (Fathiya & George, 2014) [‡‡‡]. وبطبيعة الحال فإن هذا لا يعني أن تظل هذه الدول على هامش مجتمعات المعلومات لكي تكون آمنة من الهجمات السيبرنية، وإلا أصبحت كمن يسعى لأن يظل فقيرا خشية أن يقع ضحية للصوص.

وتتوافق النتائج السابقة مع ما جاء بتقرير المنتدى الاقتصادي العالمي (2014)، والذي جاء فيه أنه – كما هو الحال في السنوات السابقة– فإن منطقة الشرق الأوسط وشمال إفريقيا تظهر بصورة متفاوتة إلى حد كبير ما بين دولة وأخرى، وذلك من حيث قدرة البلدان على الاستفادة من تقنية الاتصالات والمعلومات لتعزيز القدرة التنافسية وتحقيق الرفاهية. فإسرائيل والعديد من دول مجلس التعاون الخليجي تواصل جهودها في زيادة استيعاب تكنولوجيا الاتصالات والمعلومات في شتى المجالات، بينما لا تزال العديد من البلدان في شمال إفريقيا تعاني من قصور وضعف يمنعها من الاستفادة الكاملة من معطيات تقنية الاتصالات والمعلومات.[§§§]

[‡‡‡] https://pure.strath.ac.uk/portal/files/35636573/2_alizki_weir.pdf
[§§§] http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf

التساؤل الثاني: ما قدرة العالم العربي على مواجهة مخاطر الجرائم السيبرانية؟

الأمن السيبراني له واجهتان لا تنفصلان: واجهة يتعامل معها مسؤولوا الأمن السيبراني، يقومون من خلالها بتحديد إجراءات الأمن، وواجهة أخرى يقوم من خلالها ذوو الميول الإجرامية بتحديد أساليب عملهم على ضوء تلك الإجراءات، وعلى أساس مواطن الضعف التي لم يستطع مسؤولوا الأمن حمايتها. فالمهارة والمعرفة التي يرصدها ويبحث عنها المجرمون السيبرانيون هي نفس المهارة والمعرفة التي يمتلكها– أو التي ينبغي أن يمتلكها– المسؤولون عن أمن النظام وعن حمايته. وحينما يمتلك المجرمون السيبرانيون مهارات ومعارف أكثر تقدما، فإن ذلك يجعل اختراق الأنظمة أكثر سهولة من الدفاع عنها. (جبريل العريشي، ومحمد الشلهوب، 1436هـ)

ويتوافق ذلك القول مع من يرى أن النموذج الحالي للفضاء السيبراني، والذي يعتمد اعتمادا كليا على الإنترنت، وعلى برمجيات الشركات الكبرى كميكروسوفت، يعتبر هو نفسه مصدراً من المصادر التي تخلق أنواعا من الفجوات الرقمية، وذلك بما يتسبب فيه من عدم المساواة في الحصول على الخدمات عبر الإنترنت، وفي القدرة على مواجهة الفيروسات وبرامج التجسس، وكذا عدم المساواة الناشيء عن عدم التوافق بين الأنظمة، أو الناشيء عن اختلاف درجة صعوبة البرمجيات التي يستخدمها البعض عن تلك التي يستخدمها البعض الآخر، وغير ذلك من سلسلة الاختلافات الطويلة المصاحبة لاستخدام هذا النموذج. فهذه الاختلافات والتعقيدات تحتاج إلى مستويات معينة من المهارات لمعالجتها . (Rallet In: Fathiya & George, 2014). لذا، فعندما تقل تلك المهارات، ويقل عدد من يمتلكونها، تصبح الدولة أكثر عرضة لمخاطر الجرائم السيبرانية.

ويشير تقرير الاتحاد الدولي للاتصالات (2013)، إلى أن المؤشر الفرعي الدال على مهارة استخدام التقنية، والذي يستخدم عدد الملتحقين بالتعليم في المراحل المختلفة باعتباره معيارا لذلك، منخفض في كل الدول العربية بدون استثناء، كما أنه لم يشهد تطورا خلال العامين السابقين على إصدار التقرير، وهو ما يشير إلى وجود

فجوة في المهارة التكنولوجية بين الدول العربية بصفة عامة وبين دول العالم المتقدم. (الاتحاد الدولي للاتصالات، ومؤسسة ABI للأبحاث، 2013)

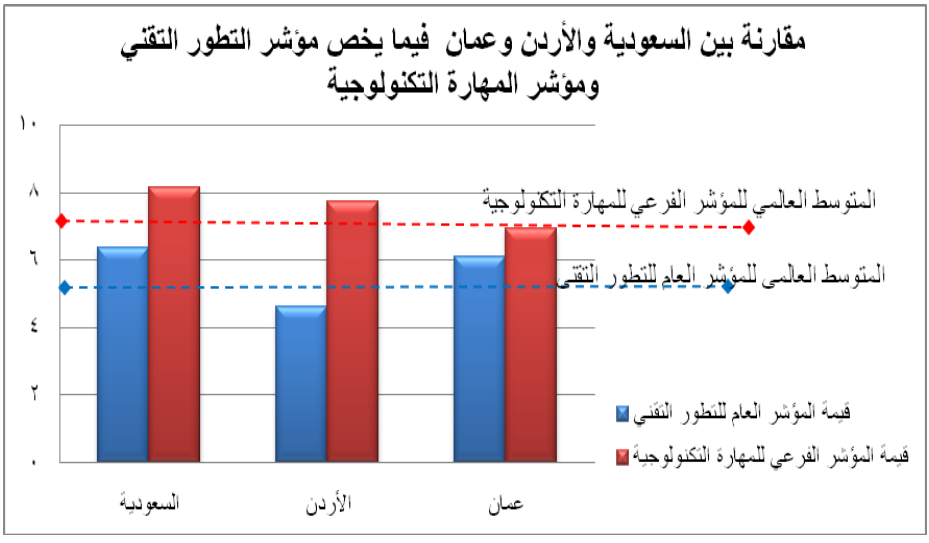
ويظهر من التقرير أن دول الخليج، بالرغم من انها ذات ترتيب متقدم نسبيا بين دول العالم فيما يخص المؤشر العام لتطور التقنية، إلا أن ترتيبها فيما يخص المؤشر الفرعي للمهارات التقنية كان متأخرا. كما يظهر منه أن الدول العربية الأخرى ذات الترتيب المتأخر نسبياً فيما يخص المؤشر العام لتطور التقنية، كانت أيضا ذات ترتيب متأخر أو أكثر تأخراً بالنسبة للمؤشر الفرعي للمهارات التقنية، فيما عدا الأردن وفلسطين والجزائر. فقد كان ترتيب تلك الدول الثلاث بالنسبة للمؤشر الفرعي للمهارات التقنية يتقدم كثيرا عن ترتيبها بالنسبة للمؤشر العام للتطور التقني.

ولو أخذنا السعودية كنموذج لدول الخليج التي يزيد مؤشر تطور التقنية فيها عن المتوسط العالمي العام، والأردن كنموذج للدول العربية التي يقل مؤشر التقنية فيها عن المتوسط العالمي العام، فإن الجدول والشكل التاليين يعرضان ترتيب الدولتين بالنسبة لدول العالم ومعهما عمان، كما يعرضان وضع كل من الدول الثلاث فيما يخص المؤشر العام للتطور التقني وكذلك المؤشر الفرعي الدال على المهارات التكنولوجية.

وقد أضفنا عمان لما لها من شأن متميز بين دول العالم العربي فيما يخص الترتيبات التنظيمية والقانونية ذات العلاقة بالأمن السيبراني كما سيتضح في الجزئية التالية.

الدولة	الترتيب بين دول العالم فيما يخص المؤشر العام للتطور التقني	قيمة مؤشر تطور التقنية	الترتيب بين دول العالم فيما يخص المؤشر الفرعي للمهارة التقنية	قيمة المؤشر الفرعي للمهارة التقنية
المتوسط العالمي	-	4.77	-	6.66
السعودية	47	6.36	51	8.17
الأردن	87	4.62	62	7.74
عمان	52	6.10	90	6.95

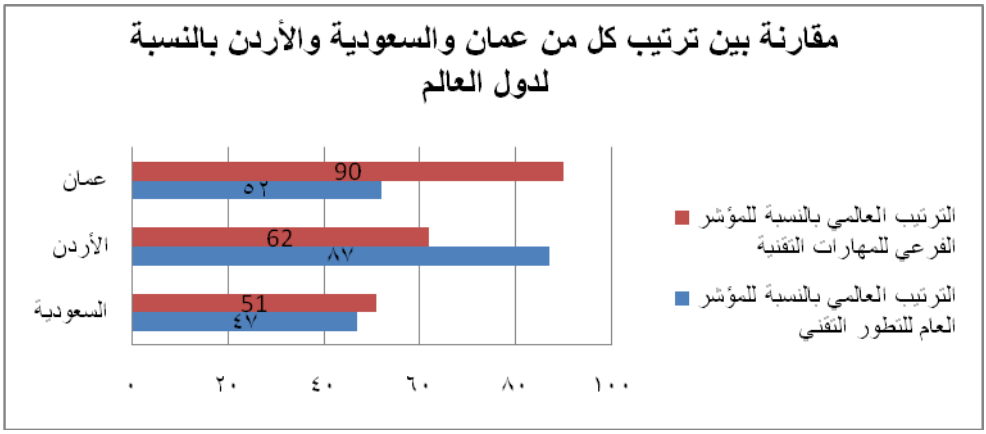
ويبين الشكل التالي قيمة المؤشرات بالنسبة للدول الثلاث:



ويبين الشكل السابق أن قيمة مؤشر المهارة التكنولوجية هي الأعلى في السعودية تليها الأردن ثم عمان، وأنها تزيد في الدول الثلاث عن المتوسط العالمي. أما بالنسبة لمؤشر التطور التقني فإنه يزيد بالنسة للسعودية وعمان عن المتوسط العالمي، بينما يقل بالنسبة للأردن عن المتوسط العالمي بقدر بسيط، مع ملاحظة أنه

في التقرير السابق للاتحاد الدولي للاتصالات (عام 2013) كان مؤشر التطور التقني في الأردن يزيد عن المتوسط العالمي.

ويبين الشكل التالي الترتيب بين دول العالم للسعودية والأردن– ومعهما عمان– فيما يخص مؤشري التطور التقني والمهارة التكنولوجية.



ومعلوم– كما سلف وذكرنا – أنه كلما ازدادت إتاحة تقنيات الاتصالات والمعلومات وزيادة عدد المستخدمين لها يزداد بالتالي عدد ضحايا الجرائم السيبرانية. لذا فإذا اعتبرنا أن الترتيب العام على مستوى العالم بالنسبة لمؤشر التطور التقني هو معيار نسبي بين دول العالم لزيادة النفاذ إلى تلك التقنيات وزيادة عدد مستخدميها (أي زيادة انتشارها)، فإنه في نفس الوقت يعتبر معيارا نسبيا لحجم مخاطر التعرض للهجمات السيبرانية. فكلما تقدم الترتيب زادت المخاطر والعكس صحيح.

وعلى الجانب الآخر فإن الترتيب العام على مستوى العالم بالنسبة للمؤشر الفرعي للمهارة التكنولوجية هو معيار للقدرة النسبية على مواجهة مخاطر الجرائم السيبرانية، فكلما تقدم الترتيب كلما زادت تلك القدرة النسبية.

فإذا تساوى الترتيبان، فإن ذلك يشير إلى أن المهارة التكنولوجية في الدولة تتناسب – إلى حد ما – مع درجة انتشار التقنية في هذه الدولة، وإذا تقدم الترتيب بالنسبة للمهارة التكنولوجية عن الترتيب بالنسبة لانتشار التقنية فإن هذا يعني أن الدولة في أمان نسبي بالنسبة لمخاطر الجرائم السيبرانية وأنها تسير بصورة متوازنة لبناء مجتمع المعلومات.

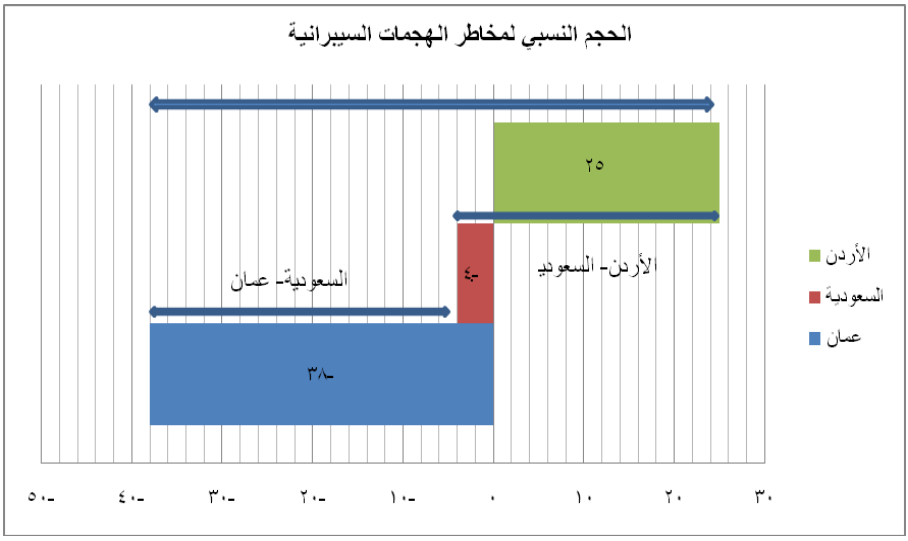
وعلى الجانب الخر، إذا تقدم الترتيب بالنسبة لانتشار التقنية عن الترتيب بالنسبة للمهارة التكنولوجية فهذا يعني أن الدولة أكثر عرضة لمخاطر الجرائم السيبرانية وذلك مقارنة بالحالة السابقة.

لذا، فإن الفارق بين الترتيبين بالنسبة لكل دولة يمثل الحجم النسبي لمخاطر الجرائم السيبرانية وذلك عند مقارنتها مع دولة أخرى(****)

والجدول التالي يوضح الحجم النسبي لمخاطر الجرائم السيبرانية في كل من السعودية والأردن وعمان.

الدولة	أ- الترتيب العالمي بالنسبة لمؤشر التطور التقني	ب- الترتيب العالمي بالنسبة لمؤشر المهارة التكنولوجية	الحجم النسبي للمخاطر الناشئة عن الجرائم السيبرانية (أ – ب)
عمان	52	90	38-
السعودية	47	51	4-
الأردن	87	62	25

كما يبين الشكل التالي التالي التمثيل الرسومي للحجم النسبي لمخاطر الجرائم السيبرانية في الدول الثلاث:



الأردن– عمان

(****) Fathiya Al Izki & George R S Weir,… Previous reference

ونستنتج من الشكل السابق أن حجم المخاطر النسبي يزيد في السعودية عن الأردن بمقدار 29 نقطة، وأن حجم المخاطر النسبي يزيد في عمان عن الأردن بمقدار 63 نقطة، وحجم المخاطر النسبي يزيد في عمان عن السعودية بمقدار 34 نقطة. أي أن السعودية أكثر عرضة لمخاطر الجرائم السيبرانية من الأردن، وعمان أكثر عرضة من كليهما.

ويلاحظ أننا نصل إلى نفس النتيجة لو استخدمنا الفارق بين المؤشرات– بدلا من الفارق بين الترتيب العالمي– كمعيار للحجم النسبي للمخاطر السيبرانية.

نخلص مما سبق إلى أن زيادة انتشار تقنية الاتصالات والمعلومات في دول الخليج ولبنان جعلها أكثر عرضة لمخاطر الجرائم السيبرانية، وهذه نتيجة طبيعية تواجهها كل دول العالم المتقدم التي تبني مجتمعات المعلومات، إلا أن دول الخليج أقل قدرة من هذه الدول على مواجهة مخاطر تلك الهجمات بسبب انخفاض المهارات التقنية بها.

كما أن نقص انتشار تقنيات الاتصالات والمعلومات في باقي الدول العربية جعلها أقل عرضة لمخاطر الجرائم السيبرانية، وهذا ليس شيئا محمودا، إذا أنها بهذا النقص تفقد المميزات التي يتيحها مجتمع المعلومات. وفي نفس الوقت فإن هذه الدول– مثلها مثل دول الخليج– أقل قدرة على مواجهة مخاطر هذه الهجمات بسبب انخفاض المهارات التقنية بها، أي أنها جمعت بين أمرين غير محمودين: بطء التحول إلى مجتمع المعلومات، وزيادة التعرض لمخاطر المعلوماتية.

ونستثني من ذلك الدول التي يتقدم ترتيبها بالنسبة لمؤشر المهارة التكنولوجية عن ترتيبها بالنسبة لمؤشر التطور التقني بصورة كبيرة، وهي الدول الثلاث السالف ذكرها: الأردن وفلسطين والجزائر، فإن المهارة التكنولوجية بها تسبق تقدمها في بناء مجتمع المعلومات.

التساؤل الثالث: ما أثر الفجوة في قدرات العالم العربي في البحوث والتطوير على الأمن السيبراني؟

أشارت العديد من الدراسات إلى أن التقدم التكنولوجي يزداد كلما ازداد الإنفاق على البحث والتطوير. (A. Steven, 2014), (Nabaz T, 2014) [‡‡‡‡،†††††].

وثمة من يرى أن ما تسببه الفجوة الرقمية من عدم إتاحة الإنترنت وعدم الوصول إليها (وهو ما ينطبق على مجموعة الدول العربية ذات القيمة المنخفضة بالنسبة لمؤشر التطور التقني)، يكون سببا في ضعف القدرة البحثية للأفراد والمؤسسات أو الدول التي تعاني منها، وبالتالي في قلة عدد الباحثين وعدد براءات الاختراع، ذلك لأنها تقلل من فرصة الحصول على المعرفة لمن يحتاجون إليها، وفي نفس تقلل من القدرة على نشر المعرفة بواسطة من يمتلكونها، كما أنها تتسبب في ضياع فرص التعاون البحثي بين الدول وبعضها، إما بسبب عدم القدرة على التواصل فيما بينهم، أو بسبب عدم وجود تناسق بين المعرفة التي يملكها كل طرف منهم. (Dutta, 2012)

فالحوارات واللقاءات العلمية والمؤتمرات والاقتباسات داخل السياق العلمي، هي كلها أنشطة أكاديمية تساهم في تشكيل وإعداد العلماء الصغار وجعلهم أعضاء فاعلين ومساهمين في إنتاج وتأسيس مجتمع المعرفة، وتتقلص هذه الأنشطة مع وجود الفجوة الرقمية، ومن ثم تصبح القدرات البحثية ضعيفة، مما يؤدي إلى ضعف المهارات التكنولوجية اللازمة لمواجهة مخاطر الجرائم السيبرانية [§§§§]. (عبد الوهاب الحايس ، 2011)

فضلاً عن ذلك، فثمة من يرى أن وجود الفجوة الرقمية كمظهر من مظاهر الفجوة الاقتصادية والاجتماعية، (وهو ما ينطبق على نفس مجموعة الدول العربية السالف ذكرها)، يؤدي إلى وجود فجوة موازية في البحوث العلمية والابتكار، بما يعني أن عدد ما تنتجه دول الجنوب من الأبحاث العلمية وبراءات الاختراع يكون أقل

[†††††] http://www.oecd.org/eco/growth/35257726.pdf
[‡‡‡‡] http://ftp.iza.org/dp8080.pdf
[§§§§] http://repository.nauss.edu.sa/bitstream/handle/123456789/56535.pdf?sequence=1

من نظيره في الدول الغنية أو دول الشمال، وذلك بسبب اختلاف القدرة على توفير الميزانية التي تسمح بإجراء البحوث العلمية التي تلتزم بمعايير الجودة العلمية. (Gorman, 2003)

يشير تقرير التنمية البشرية للبرنامج الإنمائي للأمم المتحدة عام 2013 إلى أن القيم المسجلة لنسبة ميزانية البحث والتطوير في الدول العربية تقل كثيرا عن المستويات العالمية، ولا تتجاوز 0.6 % من الناتج القومي في دولة عربية واحدة، وهي المغرب، تليها الأردن بنسبة 0,4%، ثم باقي الدول العربية والتي تتراوح فيها ما بين 0,1% ، 0,3%. بينما تتراوح في البلدان المتقدمة بين 2.5%، 5 %، وتبلغ في إسرائيل– على سبيل المثال– 4.4% [(*****)]. (UNDP, 2013)

كما يشير التقرير إلى أن كل دول الخليج – ما عدا السعودية– لا يوجد لها قيمة مسجلة لحجم الإنفاق على البحث والتطوير، وذلك بالرغم من معدل التنمية البشرية المرتفع في هذه الدول.

فإذا استخدمنا ميزانية البحث والتطوير كمؤشر دال على مدى تقدم البحث العلمي في الدول العربية، فإننا نخلص من ذلك إلى نتيجة مفادها أن العالم العربي كله يعاني من ضعف – متفاوت– في قدرات البحث والتطوير، مما يتسبب بصورة أو بأخرى في حدوث ضعف مواز في المهارات التكنولوجية اللازمة لمواجهة مخاطر الجرائم السيبرانية. وهي نتيجة تعزز ما ورد في نهاية الفصل السابق من إشارة إلى وجود فجوة في المهارة التكنولوجية بين الدول العربية بصفة عامة وبين دول العالم المتقدم تجعلها أكثر عرضة لمخاطر الجرائم السيبرانية.

وتتفق تلك النتيجة مع ما ورد في تقرير المنتدى الاقتصادي العالمي، والذي خص فيه بعض الدول العربية بالتعليق على مستوى الابتكار فيها. وجاء فيه بشأن السعودية ما يلي:

"أن الضعف في نظام الابتكار في السعودية هو الذي جعلها تحتل المركز 31، وأن تعزيز نظام الابتكار – من خلال الاستثمار المتزايد للقدرة العلمية والتكنولوجية

[(*****)] http://hdr.undp.org/en/content/human-development-report-2013

للدولة– سيكون عاملا مهما في زيادة مشاركة السكان في الوظائف المعرفية، كما سيساعد في الانتقال من الاقتصاد القائم على الموارد إلى الاقتصاد الذي يقوم على الابتكار".

وينبغي ملاحظة أن ما تعرضه التقارير الدولية، ليس خطوطا حمراء لا يتم تجاوزها، وإنما هي مؤشرات تقريبية يتم تقديرها بناء على ما توصلت إليه الجهات الدولية من معلومات عن دول العالم. كما أن ما نستخلصه من نتائج من هذه التقارير لا يعد بدوره خطوطا حمراء، ولكنه يمثل رؤى تقترب من الواقع ولكنها قد لا تتطابق معه.

فعلى سبيل المثال، نجد أن القيمة المسجلة لميزانية البحث العلمي في السعودية– ذات الترتيب 58 بين دول العالم فيما يخص مؤشر المهارات التكنولوجية– تبلغ 0,1% من الناتج القومي، بينما القيمة المسجلة لميزانية البحث العلمي في الأردن – ذات الترتيب 64 بين دول العالم فيما يخص مؤشر المهارات التكنولوجية– تبلغ 0,4% من الناتج القومي. أي أن الأردن يتفوق على السعودية في المهارة التكنولوجية من منظور البحث العلمي، بينما السعودية تتفوق على الأردن في المهارة التكنولوجية من منظور مؤشر المهارة التكنولوجية الخاص بالاتحاد الدولي للاتصالات، والذي يعتمد على عدد الملتحقين بالتعليم في المراحل المختلفة.

ونفسر ذلك بأن ميزانية البحث العلمي في كل من الأردن والسعودية هي – في كل الأحوال – أقل كثيرا من دول العالم الأول التي تحظى بترتيب متقدم بالنسبة لمؤشر المهارة التكنولوجية. لذا، فإن هذه الميزانية بقيمتها الحالية– سواء في السعودية والأردن– لا تكفي لكي تحدث أثرا فعليا محسوسا على المهارة التكنولوجية، ومن هنا كان الترتيب السالف ذكره بالنسبة للأردن فيما يخص مؤشر المهارة التكنولوجية.

التساؤل الرابع: ما مدى تأهب النواحي القانونية والتنظيمية للحفاظ على الأمن السيبرني وترتيبات السلامة السيبرانية في العالم العربي ؟(الاتحاد الدولي للاتصالات، ومؤسسة ABI للأبحاث، 2015):

هناك وجهان لمجتمع المعلومات: الأول تقني، والآخر قانوني تنظيمي، والارتباط بين الاثنين حتمي وضروري. فإذا كان لا يمكن للقانون أن يعمل بعيدا عن التقنيات وخصائصها، وعن طبيعة النشاط التقني، سواء لتقرير الحقوق أو لوضع قواعد المسئوليات، فإنه في نفس الوقت يكون الاعتماد على الهندسة المعلوماتية، وتدابير الحماية الفنية للبيانات الشخصية قاصرا عن تقديم الحل للمسائل القانونية. فالحلول التقنية موجودة، ولكنها لا تكون حاسمة ونهائية أبداً، ولا تمثل – بصورة عامة – أكثر من الاستجابة لمشكلة معينة داخل سياق محدد[†††††]. (منى جبور، 2015)

ولقد قام الاتحاد الدولي للاتصالات ITU، بالتعاون مع مؤسسة ABI للأبحاث، بتطوير مؤشر قياسي عالمي CGI للأمن السيبراني وسمات السلامة السيبرانية بغرض تقييم مستوى تطور الأمن السيبراني على مستوى العالم، يتم من خلاله قياس القدرة التنظيمية والقانونية لكل دولة في هذا الشأن. ويرمي هذا المؤشر إلى تحفيز البلدان لتكثيف جهودها في مجال الأمن السيبراني، والمساعدة على تطوير ثقافة عالمية بالنسبة للأمن السيبراني ودمجها ضمن صميم تكنولوجيات المعلومات والاتصالات.

ويتكون مؤشر GCA من خمسة مؤشرات فرعية تقيس القدرات التنظيمية والقانونية للأمن السيبراني في الدول، وهذه المؤشرات الفرعية هي:

التدابير القانونية، والتي تشمل مدى وجود تشريعات تواجه النفاذ غير المخوَّل (دون حق) إلى أجهزة وأنظمة وبيانات الحاسوب، والتدخل فيها، أو اعتراضها

التدابير التقنية، وتشمل وجود فرق للاستجابة للطوارئ والحوادث الحاسوبية، سواء الأمنية أو غير الأمنية وذلك لتحديد التهديدات السيبرانية ومكافحتها والاستجابة لها وإدارتها، كما تشمل تلك التدابير وجود آليات معتمدة لتنفيذ معايير الأمن السيبراني

[†††††] http://xa.yimg.com/kq/groups/16186325/1096065403/name.doc.

المعترف بها دوليا والتي تضعها وكالات مثل المنظمة الدولية للتوحيد القياسي ISO، أو الاتحاد الدولي للاتصالات ITU أو غير ذلك، وكذا وجود إطار (أو أطر) معتمدة من الحكومة (أو تحظى بتأييدها) من أجل منح الشهادات واعتماد وكالات (حكومية) وطنية ومهنيي القطاع العام بموجب معايير الأمن السيبراني المعترف بها دولياً.

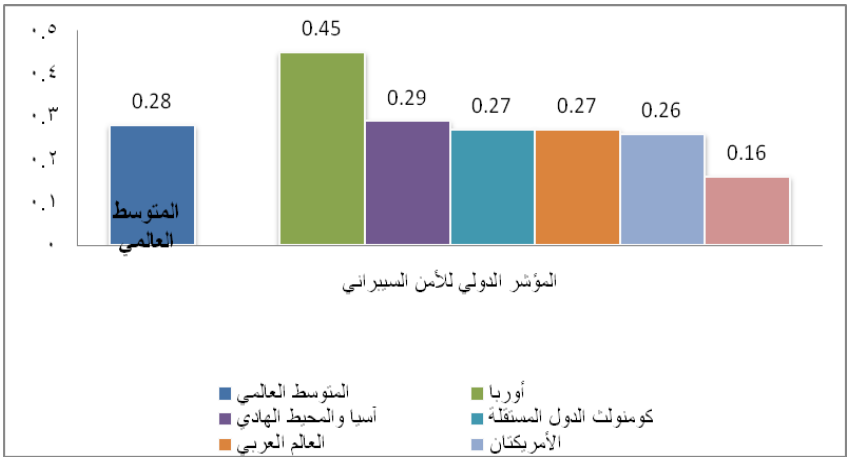
التدابير التنظيمية، والتي تشمل وجود السياسات والمؤسسات والاستراتيجيات التي تنظم تطور الأمن السيبراني على الصعيد الوطني

بناء القدرات، وتشمل وجود برامج البحث والتطوير وعددها، وبرامج التعليم والتدريب، والاختصاصيين المعتمدين ووكالات القطاع الخاص المعتمدة، ومنح الشهادات المهنية المعترف بها دوليا للأشخاص والمؤسسات.

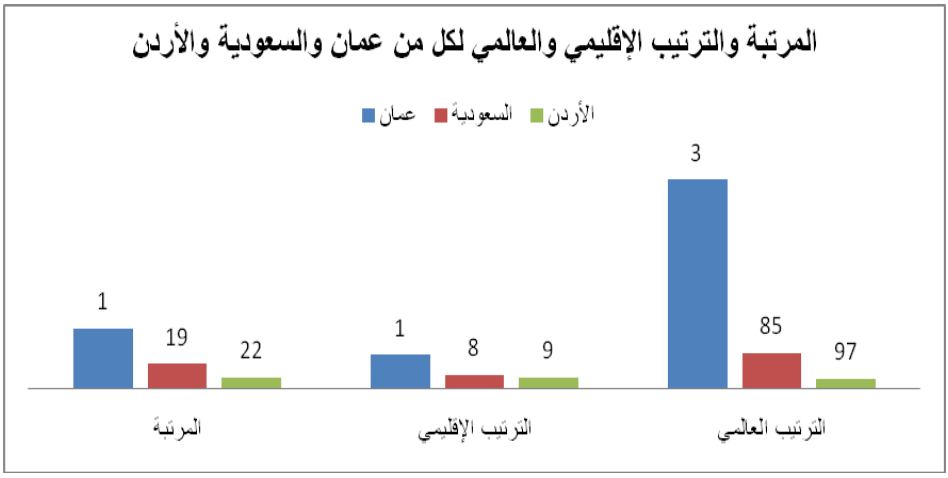
التعاون، ويشمل التعاون الذي يستند إلى وجود الشراكات والأطر التعاونية وشبكات تبادل المعلومات سواء على الصعيد الوطني أو الدولي.

وتقدم هذه البيانات الوصفية عروضاً واقعية لمستوى تطور التدابير التنظيمية والقانونية للأمن السيبراني في كل دولة، وهي تهدف إلى توفير منظور واضح لساحة الأمن السيبراني الحالي القائم على الدعائم الخمس لبرنامج الأمن السيبراني العالمي والسالف ذكرها.

وقد سجل العالم العربي مرتبة أقل من المتوسط العالمي، حيث كانت قيمة المؤشر الدولي للأمن السيبراني 0,27 بينما بلغ المتوسط العالمي 0,28 ، ويتضح ذلك من الشكل التالي:

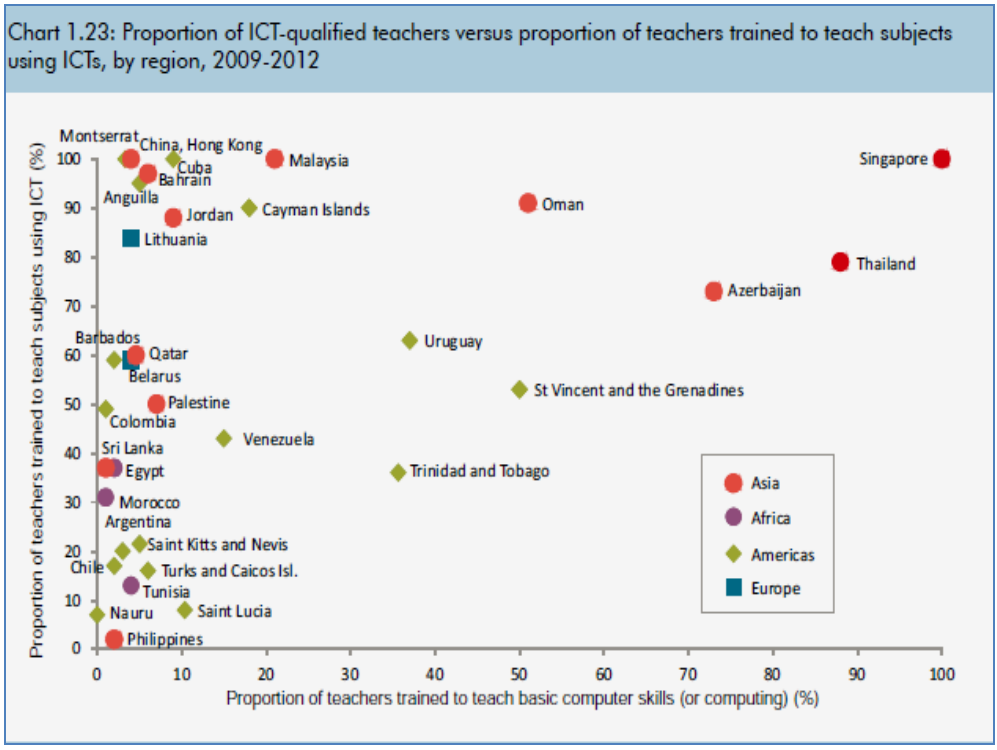


وقد تم ترتيب دول العالم (195 دولة) في تسع وعشرين مرتبة، وكانت عمان هي أعلى الدول العربية بالنسبة للترتيب العالمي حيث احتلت المرتبة الثالثة (وكان ترتيبها الخامس على مستوى العالم)، تليها قطر في المرتبة الثامنة (الترتيب 25 على مستوى العالم). بينما احتلت المملكة العربية السعودية المرتبة التاسعة عشرة (الترتيب 85 على مستوى العالم) واحتلت الأردن المرتبة الثانية والعشرين (الترتيب 97 على مستوى العالم)، كما يوضح الشكل التالي:



ويتضح من الشكل السابق التقدم المذهل لعمان بشأن الرقم القياسي العالمي للأمن السيبراني. وهو ما يعني أن عمان تتقدم بصورة كبيرة عن كل الدول العربية، وعن أغلب دول العالم، في مجال الإعداد التنظيمي والقانوني لمواجهة مخاطر الجرائم السيبرانية، وذلك حسب معيار CGI للأمن السيبراني وسمات السلامة السيبرانية.

ويتفق ذلك مع ما جاء في الشكل التالي – الذي ورد في التقرير السنوي للاتحاد الدولي للاتصالات ITU,(2014) والذي يبين نسبة عدد المعلمين الذين تم تدريبهم على تدريس المهارات الحاسوبية الاساسية إلى العدد الكلي للمعلمين في الدولة. فكما يبين الشكل، تبلغ تلك النسبة في عمان حوالي 50%، بينما تبلغ في الأردن – وكل الدول العربية المبينة في الشكل– حوالي 10% أو أقل. وهو ما يعني أن عمان تتقدم بالفعل بصورة كبيرة في مجال الإعداد التنظيمي والقانوني لمواجهة مخاطر الجرائم السيبرانية.



لقد ورد في وثيقة الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية أن منهجية تحديد مؤشرات الأداء فيما يخص الأمن السيبراني تقوم على أن تبادل المعلومات والتعاون هما مفتاح التصدي للتهديدات العابرة للحدود، وتتطلب هذه العناصر قدراً معيناً من التنظيم في العديد من التخصصات :القانونية والتقنية والتعليمية، وعلى أن المقارنة بين قدرات الأمن السيبراني للدول وترتيبها بناء على ذلك من شأنه أن يكشف أوجه القصور ويحفز الدول على تكثيف جهودها في مجال الأمن السيبراني، لأن القيمة الحقيقية لقدرات الأمن السيبراني لدولة ما لا يمكن أن تقاس على الوجه الصحيح إلا من خلال المقارنة. (الاتحاد الدولي للاتصالات، ومؤسسة ABI للأبحاث ، 20015)

لذا، فسيتم عقد مقارنة بين عمان من جانب ونماذج من الدول العربية (السعودية والأردن) من جانب آخر، وذلك للتعرف على الحيثيات التي جعلت عمان، وهي من دول العالم العربي التي تنتمي إلى شريحة الدول النامية، تحتل هذا الترتيب

المتقدم فيما يخص مؤشر الأمن السيبراني وترتيبات السلامة السيبرانية، وبفارق شاسع عن الدول العربية الأخرى.

ويبين الجدول في الملحق مقارنة بين المعطيات التي اعتمد عليها الاتحاد الدولي للاتصالات ومؤسسة ABI للأبحاث في تقديرهما للرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية وذلك فيما يخص كلا من عمان والسعودية والأردن.

وينبغي ملاحظة أن ما ورد في هذا الجدول بخصوص الدول الثلاث هو ما قامت تلك الدول بنفسها بالتصريح به في الاستبيان الذي تم إعداده لهذا الشأن بواسطة مؤسسة ABI للأبحاث. أي أن ما يعرضه الجدول من قدرات قانونية وتنظيمية لكل دولة إنما يمثل رؤية كل دولة لنفسها فيما يخص تلك القدرات.

ويبين الجدول والشكل التاليين وضع كل من الأردن والسعودية وعمان فيما يخص الرقم القياسي العالمي للأمن السيبراني ومؤشراته الفرعية، والتي تعكس ما ورد في جدول المقارنة (بالملحق):

الدولة	قانونية	تقنية	تنظيمية	بناء القدرات	التعاون	الرقم القياسي	المرتبة	الترتيب الإقليمي	الترتيب العالمي
عمان	0,75 00	0,66 67	1,00 00	0,75 00	0,62 50	0,74 67	3	1	5
السعودية	0,75 00	0,33 33	0,12 50	0,37 50	0,12 50	0,29 41	19	8	85
الأردن	0,50 00	0,00 00	0,50 00	0,00 00	0,12 50	0,20 59	22	9	97

ويتضح من الشكل السابق أن عمان تتفوق على كل من السعودية والأردن في كل المؤشرات الفرعية ما عدا الترتيبات القانونية التي تتساوى فيها مع السعودية.

كما أن السعودية تتفوق على الأردن في كل المؤشرات الفرعية ما عدا " التعاون" الذي يتساويان فيه معا، والترتيبات التنظيمية التي يتفوق فيها الأردن على السعودية.

والأمر اللافت للنظر هو أنه بالرغم من أن عمان كان ترتيبها 90 على مستوى العالم في مؤشر المهارة التكنولوجية، والذي يدل على مدى القدرة على مجابهة مخاطر الجرائم السيبرانية، وذلك حسب ما جاء في تقرير الاتحاد الدولي للاتصالات عام 2014، بينما كان ترتيب السعودية والأردن هو 51 و62 على التوالي، إلا أنها فيما يخص التأهب فيما يتعلق بالأمن السيبراني وترتيبات السلامة السيبرانية كان ترتيب عمان هو الخامس على مستوى العالم، بينما كان ترتيب كل من السعودية والأردن هو 85، 97 على التوالي، وهو ما يتضح من الجدول التالي:

الدولة	الترتيب العالمي بالنسبة لمؤشر المهارة التكنولوجية	الترتيب العالمي بالنسبة للرقم القياسي العالمي للأمن السيبراني
عمان	90	3
السعودية	51	85
الأردن	62	97

ويتضح من الجدول السابق أن عمان قد قطعت شوطا كبيرا في مجال الجاهزية القانونية والتنظيمية للدولة والتي تختص الأمن السيبراني، إلا أن قدراتها التقنية في مجابهة الجرائم السيبرانية– والتي يعكسها ترتيب مؤشر المهارة التكنولوجية – والذي يعتمد على عدد الملتحقين فيها بمراحل التعليم المختلفة فضلا عن الميزانية المخصصة للبحث والتطوير– تعد منخفضة بصورة كبيرة.

كما يتضح من الجدول السابق أن السعودية والأردن هما على العكس من ذلك، فكلاهما كان ترتيبه متأخراً بالنسبة للرقم القياسي العالمي للأمن السيبراني، مما يعكس عدم الجاهزية القانونية والتنظيمية للدولة بشأن الأمن السيبراني، بينما كان ترتيبهما متقدماً بصورة كبيرة عن عمان فيما يخص القدرة على مجابهة الجرائم السيبرانية كما يظهر من ترتيب كل منهما فيما يخص مؤشر المهارة الكنولوجية.

خلاصة نتائج الدراسة

لقد توصلت هذه الدراسة إلى مجموعة من النتائج والتي تعتبر في مجملها خلاصة التحليلات والمناقشات فقد أظهرت الدراسة أن الدول العربية تتفاوت في درجة تعرضها لمخاطر الجرائم السيبرانية ومدى قدرتها على مواجهة هذه المخاطر، فزيادة انتشار تقنية الاتصالات والمعلومات في دول الخليج جعلها أكثر عرضة لمخاطر الجرائم السيبرانية، وهذه نتيجة طبيعية تواجهها كل دول العالم المتقدم التي تبني مجتمعات المعلومات، إلا أن دول الخليج أقل قدرة من دول العالم المتقدم على مواجهة مخاطر تلك الهجمات بسبب انخفاض المهارات التقنية بها.

كما أن نقص انتشار تقنيات الاتصالات والمعلومات في باقي الدول العربية جعلها أقل عرضة لمخاطر الجرائم السيبرانية، وهذا ليس شيئاً محموداً، إذا أنها بهذا النقص تفقد المميزات التي يتيحها مجتمع المعلومات، وفي نفس الوقت فإن هذه الدول– مثلها مثل دول الخليج– أقل قدرة على مواجهة مخاطر هذه الهجمات بسبب انخفاض المهارات التقنية بها، أي أنها جمعت بين أمرين غير محمودين: بطء التحول إلى مجتمع المعلومات، وزيادة التعرض لمخاطر المعلوماتية.

ونستثني من ذلك الدول التي يتقدم ترتيبها بالنسبة لمؤشر المهارة التكنولوجية عن ترتيبها بالنسبة لمؤشر التطور التقني بصورة كبيرة، وهي: الأردن وفلسطين والجزائر، فإن المهارة التكنولوجية بها تسبق تقدمها في بناء مجتمع المعلومات.

كما أبرزت الدراسة أنه فيما يخص الجاهزية القانونية والتنظيمية للدولة فإن أغلب الدول العربية باستثناء عمان، وقطر بصورة أقل، قد احتلت ترتيبا متأخرا بالنسبة لدول العالم.

أما فيما يخص عمان، والتي كان ترتيبها الخامس على مستوى العالم، فقد قطعت شوطا كبيرا في مجال الجاهزية القانونية والتنظيمية للدولة والتي تخص الأمن السيبراني.

كما أوضحت الدراسة أنه لا يوجد علاقة بين الجاهزية التنظيمية والإدارية للدولة بشأن الأمن السيبراني، وبين القدرة على مجابهة مخاطر الهجمات السبرانية والتي تعتمد على انتشار المهارة التكنولوجية بين أبناء الدولة.

فعمان، بالرغم من أنها قطعت شوطاً كبيراً في مجال الجاهزية القانونية والتنظيمية للدولة والتي تخص الأمن السيبراني، إلا أن قدراتها في مجابهة الجرائم السيبرانية– والتي يعكسها ترتيب مؤشر المهارة التكنولوجية والذي يعتمد على عدد الملتحقين فيها بمراحل التعليم المختلفة فضلاً عن الميزانية المخصصة للبحث والتطوير – تعد منخفضة بصورة كبيرة.

وفي نفس الوقت فإن السعودية والأردن هما على العكس من ذلك. فكلاهما كان ترتيبه متأخراً بالنسبة للرقم القياسي العالمي للأمن السيبراني، مما يعكس عدم الجاهزية القانونية والتنظيمية للدولة بشأن الأمن السيبراني، بينما كان ترتيبهما متقدما بصورة كبيرة عن عمان فيما يخص القدرة على مجابهة الجرائم السيبرانية والذي يظهر من ترتيب كل منهما فيما يخص مؤشر المهارة الكنولوجية.

تاسعاً: التوصيات

تختلف الدول العربية – من دولة إلى أخرى – في قدرتها على مجابهة مخاطر الجرائم السيبرانية، وذلك حسب درجة انتشار تقنية الاتصالات والمعلومات في الدولة وحسب درجة المهارة في استخدامها، كما تختلف في درجة تأهبها فيما يخص التدابير القانونية والتنظيمية التي تختص بالأمن السيبراني.

ونرى أن ما أورده الاتحاد الدولي للاتصالات– بالتعاون مع مؤسسة ABI للأبحاث– في تقريره بشأن الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية– يمثل إطاراً شاملاً لما ينبغي وضعه من توصيات بخصوص الأمن السيبراني، فهو يشمل كل الجوانب التي تختص بالأمن السيبراني والتي تشكل اللبنات الأساسية لقياس القدرات الوطنية في هذا الشأن. كما أن ما ورد فيه – بالنسبة للدول ذات الترتيب المتقدم– يمثل أفضل الممارسات التي ينبغي على الدول ذات الترتيب المتأخر أن تلجأ إليها، فضلاً عن ذلك، فإن مجال تطبيقه – حسب ما جاء بالتقرير– يتقاطع مع جميع الصناعات وجميع القطاعات، رأسياً وأفقياً. وبالتالي فإن تمكين القدرات الوطنية وتطويرها يتطلب المساهمة من جانب كل القوى السياسية والاقتصادية والاجتماعية في الدولة، ويمكن القيام بذلك من جانب دوائر إنفاذ القانون والعدل والمؤسسات التعليمية والوزارات وشركات القطاع الخاص ومطوري التكنولوجيا، وبالشراكات بين القطاعين العام والخاص والتعاون ضمن الدولة نفسها. (الاتحاد الدولي للاتصالات، ومؤسسة ABI للأبحاث، 2015)

وبعد استعراض نتائج الدراسة فإنه يمكننا الخروج بمجموعة من التوصيات التي تختص بالأمن السيبراني والتي نستنتجها مما تم طرحه في هذه الدراسة:

١. سَن تشريعات جديدة تختص بالجرائم السيبرانية تحاكي ما صدر من تشريعات في الدول الأخرى، بحيث تغطي كافة الجوانب التي تختص بالأمن السيبراني
٢. إنشاء هيئة حكومية مركزية تختص بكل ما يتعلق بالأمن السيبراني، سواء التعامل مع الحوادث السيبرانية على المستوى الوطني، أو المراقبة والإنذار والاستجابة للحوادث السيبرانية، أو تطوير الهياكل التنظيمية اللازمة لتنسيق

التصدي للهجمات السيبرانية أو تحديد المعايير المرجعية التي تستخدم في قياس تطور الأمن السيبراني على المستوى الوطني أو على مستوى القطاعات.

٣. إيجاد إطار (أو أطر) معتمدة من الحكومة (أو تحظى بتأييدها) من أجل منح الشهادات للاختصاصيين العاملين في القطاع الحكومي واعتماد وكالات (حكومية) وطنية بموجب معايير الأمن السيبراني المعترف بها دولياً

٤. وضع استراتيجية وطنية للأمن السيبراني يتم فيها تحديد الأدوار والمسؤوليات بوضوح، كما يتم فيها تشجيع إشراك القطاع الخاص في المبادرات التي تطرحها الحكومة والتي تختص بالأمن السيبراني.

٥. وضع خارطة طريق وطنية عامة في مجال الأمن السيبراني، من خلال الاسترتيجية الوطنية السالف ذكرها، يتم فيها تحديد أصحاب المصلحة الرئيسيين، ويراعى فيها الاحتياجات التي تتطلبها حماية البنى التحتية للمعلومات على الصعيد الوطني، بالإضافة إلى تعزيز تبادل المعلومات داخل القطاع العام، وبين القطاعين العام والخاص.

٦. وضع برامج للتدريب وتشجيع تنظيم الدورات ومنح الشهادات للاختصاصيين في الأمن السيبراني– سواء على المستوى الوطني أو على مستوى قطاعات الدولة– والاستفادة في ذلك من المنظمات غير الحكومية والمؤسسات والمنظمات، ومقدمي خدمة الإنترنت، والمكتبات، ومنظمات التجارة المحلية، والمراكز المجتمعية، ومخازن الحواسيب، وكليات المجتمعات المحلية، وبرامج تعليم الكبار والمدارس، ومنظمات المجتمع المدني.

٧. تنفيذ برامج ومشروعات تستهدف بناء شراكات رسمية من أجل التعاون أو تبادل المعلومات أو التكنولوجيا أو الموارد الخاصة بالأمن السيبراني وذلك بين الهيئات والإدارات الحكومية وبعضها البعض، أو بين القطاعين العام والخاص.

٨. المشاركة الرسمية في مؤتمرات ومحافل الأمن السيبراني الدولية أو الإقليمية والتي يتم فيها تبادل المعلومات المتعلقة بالتهديدات وسيناريوهات الهجمات وأفضل الممارسات في مجالي التصدي والدفاع، أو إطلاق المبادرات التعاونية

التي تسهم في صد الهجمات السيبرانية المتكررة والدائمة والمساعدة في توقيف الفاعلين ذوي النوايا الخبيثة والتحقيق معهم ومحاكمتهم.

٩. تنفيذ استراتيجية تطويع العلوم والتقنية والابتكار التي اعتمدها المؤتمر الرابع عشر لوزراء التعليم العالي في الدول العربية– والذي عقد في الرياض في مارس 2014 – وذلك لخدمة عمليات التنمية في الدول العربية، وذلك من خلال تحسين جودة تعليم العلوم ، وإصلاح الجامعات ورفع مستواها العلمي، وبناء القدرات البحثية، وتشجيع التعاون الدولي. وتحث الاستراتيجية الدول العربية لزيادة الميزانية المخصصة لأنشطة البحث والتطوير بحيث تصبح 3%، من الناتج المحلي الإجمالي [‡‡‡‡‡]. (الاستراتيجية العربية للبحث العلمي والتقني والابتكار، 2013)

[‡‡‡‡‡] http://www.projects-alecso.org/wp-content/uploads/2014/02/1.pdf

المراجع

المراجع العربية

- مدحت أبو النصر (2004م). **قواعد ومراحل البحث العلمي، القاهرة** ، مجموعة النيل العربية، 131- 132.
- الاتحاد الدولي للاتصالات، ومؤسسة ABI للأبحاث، الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية- أبريل 2015 http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-A.pdf
- كمال الدين الدهراوي (2003م). "**مدخل معاصر في نظم المعلومات**"، الدار الجامعية للنشر والتوزيع، مصر.
- **الاستراتيجية العربية للبحث العلمي والتقني والابتكار** – الأمانة العامة- جامعة الدول العربية- ديسمبر 2013م. -http://www.projects-alecso.org/wp-content/uploads/2014/02/1.pdf
- منى الاشقر جبور – **الأمن في الفضاء السيبيري: الأمن المعلوماتي والأمن القانوني** http://xa.yimg.com/kq/groups/16186325/1096065403/name.doc.
- أحمد جمعة ،عصام العربيد ،زياد الزعبي (2003م). "**نظم المعلومات المحاسبية مدخل تطبيقي معاصر**"، دار المناهج للنشر والتوزيع.
- عبد الوهاب الحايس (2011م). التوجهات المنهجية لأطروحات الماجستير في قسم الاجتماع والعمل الاجتماعي بجامعة السلطان قابوس- **الملتقى العلمي "تجويد الرسائل والأطروحات العلمية وتفعيل دورها الأمني"** http://repository.nauss.edu.sa/bitstream/handle/123456789/56535.pdf?sequence=1.
- سلطان ابراهيم (2011م). "**نظم المعلومات الادارية (مدخل النظم)**"، الدار الجامعية للطبع والنشر والتوزيع، الاسكندرية.
- حرية شعبان محمد الشريف (2004م). **مخاطر نظم المعلومات المحاسبية الإلكترونية**، "دراسة تطبيقية على المصارف العاملة في قطاع غزة"، الجامعة الإسلامية، غزة.
- جبريل حسن العريشي، ومحمد الشلهوب (1436هـ). **أمن المعلومات**، الأردن، الدار المنهجية.
- عبد الرزاق قاسم (2003م). "**نظم المعلومات الحاسوبية**"، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن.

- ميلاد عبد المجيد (2015): "**نشر الطمأنينة وبناء الثقة في العصر الرقمي**"، تم دخول الموقع (www.abdelmajid-miled.com) /articles2015/8/23
- UNODC – **دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتَّخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدِّي لها**– فينا– 2013.

المراجع الأجنبية:

– Abu-Musa, Ahmad A. (2001), "Evaluating The Security of Computerized Accounting Information Systems: An Empirical Study on Egyptian Banking Industry", PhD. Thesis, Aberdeen University, UK.

– Abu-Musa, Ahmad A. (2004), "Important Threats to Computerized Accounting Information Systems: An empirical Study on Saudi Organizations" Pubic Administration, A Professional Quarterly Journal Published by The Institute of D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf

– Are Nakrem (2007): Managing information security in organizations A CASE study . Master thesis in information systems, Faculty of Economics and Social Sciences, Agder University College .

– Dhillon, G. (2009), "Managing and controlling computer misuse", Information Management & Computer Security, (Vol. 7, Number 4), PP. 171-175.

– Dutta, S. and Bilbao-Osorio, B. (2012). *The Global Information Technology Report 2012: Living in a Hyper- connected World*. SRO-Kundig, Geneva.

– .Eric A. Fischer (2016):Cybersecurity Issues and Challenges: In Brief Avilable at : Congressional Research Service. https://fas.org/sgp/crs/misc/R43831.pdf

– Europe 2020 indicators - Eurostat, Statistics Explained web site, research and development http://ec.europa.eu/eurostat/statistics-

explained/index.php/Europe_2020_indicators_-_research_and_development

- Fathiya Al Izki & George R S Weir, Information Security and Digital Divide in the Arab World, Cyberforensics - International conference of cybercrime, Security & Digital Forensics, Glasgow, 2014.
- Ghernaouti-Helie, Solange, From risk management to information security policies and practices: a multi perspective framework for ICT security effectiveness, ITU-T, 2008, Geneva (In: Fathiya Al Izki and George R S Weir, 2014).
- Gorman, M. (2003). The enduring library: Technology, tradition, and the quest for *balance*. Chicago, IL: American Library Association.https://pure.strath.ac.uk/portal/files/35636573/2_alizki_weir.pdf.
- ICSC (International Centre For Scientific Culture), information Security in the Context of the Digital Divide, Recommendations submitted to the World Summit on the Information Society, Tunis, (16 to 18 November 2005) (In: Fathiya Al Izki and George R S Weir, 2014)
- ITU, Measuring the information society (report) , International Telecommunication Union, 2014 https://www.itu.int/en/ITU
- ITU,(2014). Measuring the information society (report)...Previous reference.
- Jessup Leonard and Valacich, Joseph (2003), "Information Systems Today", Isted., Prentice hall.
- John Cox, "Survey: Security Remains Job, "Network World, May20, 2002, www.nwfusion.com /news/2002/0520nw500.htm"
- Loch, Karen D., Houston H. Carr and Merrill E. Warkentin (2002), "Threats to Information Systems: Today's Reality, Yesterday's Understanding", MIS Quarterly, (June), pp. 173 -186.

- Mattias Hanson, Tuve Johansson, Charlotte Lindgren, & Richard Oehme (2015): Information Security – trends A Swedish perspective. Available at: https://www.msb.se/RibData/Filer/pdf/27584.pdf.
- Nabaz T. Khayyat Jongsu Lee Almas Heshmati, How ICT Investment and Energy Use Influence the Productivity of Korean Industries, 2014.
- Panko, Raymond R (2004), Corporate Computer and Network Security, Prentice Hall, Upper Saddle, New Jersey.
- Pimienta D., La fracture numérique : un concept boiteux ?, République Dominicaine, Funredes, 2002. (qtd. In Muriel, 2009) (In: Fathiya Al Izki and George R S Weir, 2014)
- Public Administration Riyadh, Saudi Arabia, (Vol. 44, No. 3), pp. 1-65.
- Rallet, Alain, Lequeux, Fabrice, Unequal access and new multimedia services online or the current model of the Internet as the basis the "digital divide", International Conference: "ICTs & Inequalities: the digital Divides", Paris, Carré des Sciences, 18-19 November 2004 (Rallet In: Fathiya Al Izki and George R S Weir, 2014)
- Ryan, S. D. and B. Bordoloi (2007), "Evaluating Security Threats in Mainframe and Client / Server Environments", Information & Management, (Vol. 32, Iss. 3), pp. 137 - 142.
- Siponen, M. T. (2009), "A conceptual Foundation for Organizational Information Security Awareness", Information Management and Computer Security, Bradford, (Vol. 8, Iss. 8), PP. 31- 44.
- Steven Englander, Robert Evenson and Masaharu Hanazaki /R&D, INNOVATION AND THE TOTAL FACTOR PRODUCTIVITY SLOWDOWN.
- UNDP, Human Development Report (2013). The Rise of the South: Human Progress in a Diverse World. http://hdr.undp.org/en/content/human-development-report-2013.

- Volonino, Linda and Stephen R. Robinson (2004). "Principles and Practices of Information Security". Upper Saddle River, N.J.: Prentice Hall.
- Whitman Michael E. (2011), "Enemy at the Gate: Threats to Information Security", Communication of the ACM, (Vol. 46, Iss. 8), pp. 91-95.
- Word Net 3.0, Farlex clipart collection. © 2003-2012 Princeton University, Farlex Inc.
- World Economic Forum, The Global Information Technology Report, 2014 http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf.

الملحق

مقارنة بين عمان والسعودية والأردن بشأن المؤشرات التي تم الاعتماد عليها في تحديد الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية (§§§§§)

مؤشرات الأداء	عمان	السعودية	الأردن
1- التدابير القانونية			
1-1 التشريعات الجنائية المتعلقة بالأنشطة السيبرانية	تم سن تشريعات محددة تختص بالأنشطة السيبرانية وهي: - قانون جرائم المعلوماتية - قانون المعاملات الإلكترونية - قانون تنظيم الاتصالات	تم إصدار تشريع محدد يختص بالأمن السيبراني وهو: قانون مكافحة الجرائم المعلوماتية	تم إصدار تشريع محدد يختص بالأمن السيبراني وهو: قانون نظم المعلومات والجرائم السيبرانية
1-2 لوائح الأمن السيبراني ومتطلبات الامتثال لها	تم وضع سياسات وإصدار لوائح تتعلق بالجرائم السيبرانية وهي: سياسة الأمن العام- سياسة استخدام الإنترنت والبريد الإلكتروني- سياسة الويب والخدمات الإلكترونية- إطار عمل الحكومة الإلكترونية	تم إصدار تشريع تنظيمي يختص بالأمن السيبراني وهو: قانون المعاملات الإلكترونية	تم إصدار تشريع تنظيمي يختص بالأمن السيبراني وهو: قانون المعاملات الإلكترونية
2- التدابير التقنية			
2-1 فريق الاستجابة للطوارئ الحاسوبية (CERT)، فريق الاستجابة للحوادث الحاسوبية (CIRT): أسماء وأرقام الأفرقة الوطنية أو القطاعية المعتمدة رسمياً لمواجهة الطوارئ الحاسوبية وللاستجابة للحوادث	لدى عمان فريق وطني معتمد للاستجابة للطوارئ الحاسوبية (OCERT). ويستضيف هذا الفريق الوطني أول مركز للأمن السيبراني(RCC) تابع للاتحاد الدولي للاتصالات ITU ، وقد أنشئ في عام 2013	لدى السعودية فريق رسمي معتمد يعرف بـ الفريق السعودي للاستجابة للطوارئ الحاسوبية CERT SA	**لا يوجد** لدى الأردن فريق رسمي للاستجابة للطوارئ الحاسوبية إلا أنها تعمل في الوقت الراهن لإنشاء هذا الفريق. وقد تم تقييم الجاهزية لإنشاء هذا الفريق في الأردن بواسطة الاتحاد

(§§§§§) http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF

مؤشرات الأداء	عمان	السعودية	الأردن
الحاسوبية وللاستجابة للحوادث الأمنية الحاسوبية، وما إذا كانت مفوضة قانوناً أم لا			الدولي للاتصالات في عام 2014
2-2 المعايير Standards أطر الأمن السيبراني الوطنية (والقطاعية) المعتمدة رسمياً لتنفيذ معايير الأمن السيبراني المعترف بها دوليا	لدى الهيئة العمانية لتقنية المعلومات إطار عمل وطني للأمن السيبراني(وقسم مختص بذلك) معترف به على المستوى الرسمي، بغرض تطبيق المعايير العالمية المعترف بها لأمن المعلومات. ويعتمد إطار العمل على معيار ISO 27001	**لا يوجد** لدى السعودية إطار عمل رسمي يختص بتطبيق المعايير العالمية المتعارف عليها للأمن السيبراني، سواء على المستوى الوطني أو مستوى القطاعات.	**لا يوجد** لدى الأردن إطار عمل رسمي يختص بتطبيق المعايير العالمية المتعارف عليها للأمن السيبراني، سواء على المستوى الوطني أو مستوى القطاعات. إلا أن المركز الوطني لتقنية المعلومات NITC يقوم ببعض أعمال المراجعة على المؤسسات الحكومية مستخدما في ذلك معيار ISO 27001.
2-3 الشهادات أطر الأمن السيبراني الوطنية (والقطاعية) المعتمدة رسمياً لمنح الشهادات واعتماد الوكالات الوطنية والاختصاصيين في القطاع العام	في إطار تقديم خدمة التطوير الاحترافي في مجال أمن المعلومات يقوم فريق الاستجابة للطوارئ الحاسوبية (CERT) بتوفير تدريب احترافي على الأمن السيبراني في مختلف المجالات الأمنية، وذلك من خلال تقديم مناهج تدريبية- وشهادات – لرفع القدرة والمهارة في مجال أمن المعلومات. يتم تنفيذ البرنامج من	**لا يوجد** لدى السعودية إطار عمل رسمي لمنح الشهادات والاعتماد في مجال الأمن السيبراني، سواء للوكالات الوطنية أو	**لا يوجد** لدى الأردن إطار عمل رسمي لمنح الشهادات والاعتماد في مجال الأمن السيبراني، سواء للوكالات الوطنية أو للعاملين في القطاع العام.

مؤشرات الأداء	عمان	السعودية	الأردن
	خلال تعاون استراتيجي مع مؤسسات مرموقة في عمان ومع مؤسسات دولية للاعتماد مثل (ISC) ، SANS، EC- council	للعاملين في القطاع العام.	
3- التدابير التنظيمية			
3-1 السياسات استراتيجية و/أو سياسة وطنية أو قطاعية معترف بها رسمياً للأمن السيبراني	لدى عمان استراتيجية رسمية عامة معتمدة رفيعة المستوى، وكذلك خطة رئيسية، للأمن السيبراني	**لا يوجد** بالسعودية سياسة للأمن السيبراني، سواء على المستوى الوطني أو على مستوى القطاعات	لدى الأردن استراتيجية وطنية – رسمية ومعتمدة– للأمن السيبراني تحت عنوان: "الاستراتيجية الوطنية للأمن السيبراني وتدقيق المعلومات"
3-2 خارطة طريق لحوكمة الأمن السيبراني	لدى عمان خارطة طريق وطنية للأمن السيبراني تقع ضمن الاستراتيجية الرفيعة المستوى والخطة الرئيسية التي تختص بذلك	**لا يوجد** خارطة طريق لحوكمة الأمن السيبراني على المستوى الوطني في المملكة العربية السعودية	**لا يوجد** خارطة طريق لحوكمة الأمن السيبراني على المستوى الوطني في الأردن
3-3 الوكالة المسؤولة وكالة وطنية أو قطاعية معترف بها رسمياً مسؤولة عن تنفيذ استراتيجية/سياسة/خريطة طريق وطنية للأمن السيبراني	الفريق العماني للاستجابة للطوارئ الحاسوبية OCERT هو الجهة الرسمية المتعارف عليها والمسؤولة على تنفيذ الاستراتيجية الوطنية للأمن السيبراني، والإلتزام بالسياسات وخارطة الطريق	الفريق السعودي للاستجابة للطوارئ الحاسوبية CERT SA هو الجهة المسؤولة عن الأمن	المركز الوطني لتقنية المعلومات هو الجهة الرسمية المعتمدة والمسؤولة عن تنفيذ الاستراتيجية الوطنية للأمن السيبراني وكذا تنفيذ السياسات وخارطة الطرق

مؤشرات الأداء	عمان	السعودية	الأردن
		السيبراني في المملكة العربية السعودية.	
3-4 المعيار المرجعي: الممارسات الوطنية أو القطاعية المعترف بها رسمياً لتحديد المعايير المرجعية المستخدمة في قياس تطور الأمن السيبراني	يقوم الفريق العماني للاستجابة للطوارئ الحاسوبية OCERT – في إطار جهوده المستمرة لقياس تطور الأمن السيبراني في عمان- بمسح ميداني للأمن السيبراني على مختلف المستويات كما يقوم بالتدقيق ومراقبة الامتثال للسياسات وأطر العمل الصادرة. كما أن لدى عمان اتفاقا مع مؤسسة إيرنست آند يونج لتنفيذ تمارين على الالتزام بالمعيارية ضمن المسح العالمي لأمن المعلومات. ويتيح هذا المسح الفرصة للمنظمات لمقارنة نفسها مع غيرها فيما يخص القضايا الهامة لأمن المعلومات واكتساب رؤى تساعدها على اتخاذ القرارات المحورية من خلال الأسئلة التي تتعلق بميزانية الأمن والاستثمارات وحوكمة الأمن وفاعليته والتوجهات التقنية.	**لا يوجد** بالسعودية معيار مرجعي على المستوى الوطني الرسمي لقياس التطور في الأمن السيبراني	**لا يوجد** بالأردن معيار مرجعي على المستوى الوطني الرسمي لقياس التطور في الأمن السيبراني
4- بناء القدرات			
1-4 تطوير المعايير برامج/مشاريع البحث والتطوير الوطنية أو القطاعية المعترف بها رسمياً المتعلقة بمعايير الأمن السيبراني وأفضل الممارسات والمبادئ التوجيهية التي تستخدم في القطاع	قام الفريق العماني للاستجابة للطوارئ الحاسوبية OCERT- من خلال فريق البحث والتحليل- بقيادة تنفيذ مشروعات وطنية مثل: المشروع الوطني للإنذار المبكر Intelligence gathering Project برنامج النظافة السيبرانية بالإضافة إلى ذلك فإن مجلس البحث العلمي هو الجهة المسؤولة حصريا	**لا يوجد** في السعودية برنامج أو مشروع رسمي- سواء على المستوى الوطني أو على مستوى القطاعات،	**لا يوجد** في الأردن برنامج أو مشروع رسمي- سواء على المستوى الوطني أو على مستوى القطاعات، وسواء في القطاع العام أو الخاص- للبحث والتطوير في مجال

مؤشرات الأداء	عمان	السعودية	الأردن
الخاص أو العام	عن تمويل البحوث وتطويرها في الدولة. والعمل كنقطة محورية تدعم البحوث العلمية والابتكار في سلطنة عمان. ويعد البحث والتطوير في مجال الأمن السيبراني أحد المجالات الرئيسية التي يركز عليها المجلس	وسواء في القطاع العام أو الخاص– للبحث والتطوير في مجال معايير الأمن السيبراني، وأفضل الممارسات والإرشادات التي ينبغي تطبيقها	معايير الأمن السيبراني، وأفضل الممارسات والإرشادات التي ينبغي تطبيقها
4-2 تطوير القوى العاملة برامج التعليم أو التدريب المهني الوطنية أو القطاعية المعترف بها رسمياً لإذكاء الوعي بين عامة الجمهور، وتشجيع دورات الأمن السيبراني في مرحلة التعليم العالي وتعزيز منح الشهادات للاختصاصيين في القطاع العام أو الخاص	قام الفريق العماني للاستجابة للطوارئ الحاسوبية OCERT بإطلاق عدة مبادرات للتدريب على الأمن السيبراني والتوعية به وهي: - حملة للتوعية الوطنية - الحملة الحكومية الموحدة لأمن المعلومات - حملة حماية الأطفال عبر الإنترنت - برنامج سفير للفريق العماني للاستجابة للطوارئ الحاسوبية كما يعمل الفريق العماني للاستجابة للطوارئ الحاسوبية OCERT بشكل وثيق مع وزارة التعليم لتدريس مناهج أمن المعلومات في المدارس. بالإضافة إلى ذلك فإن الفريق العماني للاستجابة للطوارئ الحاسوبية OCERT هو جهة استشارية للجنة	الفريق السعودي للاستجابة للطوارئ الحاسوبية CERT SA، والمختص بإدارة الجودة في مجال الأمن ، مسؤول عن التوعية والتدريب والتعليم	**لا يوجد** لدى الأردن أي برامج رسمية معتمدة– سواء على المستوى الوطني أو على مستوى القطاعات– لإذكاء الوعي بين عامة الجمهور، وتشجيع دورات الأمن السيبراني في مرحلة التعليم العالي وتعزيز منح الشهادات للاختصاصيين في القطاع العام أو الخاص

مؤشرات الأداء	عمان	السعودية	الأردن
	تكنولوجيا المعلومات بوزارة القوى العاملة ويقوم بمراجعة مناهج تكنولوجيا المعلومات وأمن المعلومات الخاصة بكليات التعليم العالي الفنية. كما أنه جهة استشارية لكليات التعليم الخاص.		
4-3 الشهادات الاحترافية: عدد الاختصاصيين المعتمدين في القطاع العام بموجب برامج منح الشهادات المعترف بها دولياً في مجال الأمن السيبراني	يوجد لدى عمان (350) اختصاصي معتمد يعملون بالقطاع العام. وقد تم اعتمادهم بموجب برامج منح الشهادات المعترف بها دولياً في مجال الأمن السيبراني.	يوجد قاعدة بيانات إحصائية يتم فيها تخزين المعلومات التي تختص بمن يحصلون على شهادات احترافية.	يوجد لدى الأردن (14) اختصاصي معتمد يعملون في القطاع العام. وقد تم اعتمادهم بموجب برامج منح الشهادات المعترف بها دولياً في مجال الأمن السيبراني.
4-4 الوكالات الحكومية المعتمدة: عدد الوكالات الحكومية ووكالات القطاع العام المعتمدة بموجب المعايير المعترف بها دولياً في مجال الأمن السيبراني	يوجد في عمان 7 وكالات معتمدة وفقا للمعايير المعترف بها دوليا، منها ما هو تابع للحكومة ومنها ما يعمل في القطاع الخاص.	**لا يوجد** بالسعودية أي وكالة معتمدة – حكومية أو تابعة للقطاع العام– بموجب المعايير المعترف بها دوليا في مجال الأمن السيبراني	**لا يوجد** بالأردن أي وكالة معتمدة– حكومية أو تابعة للقطاع العام– بموجب المعايير المعترف بها دولياً في مجال الأمن السيبراني
5- التعاون			
5-1 التعاون الدولي: الشراكات الوطنية أو القطاعية المعترف بها	لتيسير تبادل موجودات الأمن السيبراني عبر الحدود مع الدول الأخرى فإن عمان لديها شراكات	**لا يوجد** إطار عمل لتقاسم موجودات	**لا يوجد** لدى الأردن أي شراكات وطنية أو قطاعية معترف

مؤشرات الأداء	عمان	السعودية	الأردن
رسمياً لتقاسم موجودات الأمن السيبراني عبر الحدود مع الدول الأخرى	رسمية معترف بها مع المنظمات الآتية: –ITU –APWG, Malware Alliance, FIRST, Estonia, – Malaysia (in progress), Honey Net Project, Singapore Korea (in progress), GCC CERT/OIC CERT, China (in progress	الأمن السيبراني عبر الحدود مع الدول الأخرى	بها رسمياً لتقاسم موجودات الأمن السيبراني عبر الحدود مع الدول الأخرى
2-5 التعاون الداخلي بين مؤسسات القطاع العام: البرامج الوطنية أو القطاعية المعترف بها رسمياً لتقاسم موجودات الأمن السيبراني داخل القطاع العام	قامت عمان بالاعتماد الرسمي لبرامج تقاسم موجودات الأمن السيبراني في القطاع العام، سواء على المستوى الوطني أو مستوى القطاعات، وذلك من خلال برنامج سفير للفريق العماني للاستجابة للطوارئ الحاسوبية والذي يخلق روابط دائمة بين الفريق وبين مكونات القطاع العام.	**لا يوجد** لدى السعودية أي برنامج رسمي معتمد لتقاسم موجودات الأمن السيبراني، سواء على المستوى الوطني أو على مستوى القطاعات.	لدى المركز الوطني لتقنية المعلومات في الأردن برنامج رسمي معتمد لتقاسم موجودات الأمن السيبراني داخل القطاع العام.
3-5 الشراكة بين القطاع العام والقطاع الخاص: البرامج الوطنية أو القطاعية المعترف بها رسمياً لتقاسم موجودات الأمن السيبراني بين القطاع العام والقطاع الخاص	قامت عمان بالاعتماد الرسمي لبرامج تقاسم موجودات الأمن السيبراني بين القطاعين العام والخاص، سواء على المستوى الوطني أو مستوى القطاعات. وعلى سبيل المثال يوجد تبادل للمعلومات بشأن الأمن السيبراني مع مركز أمن للقطاع الخاص، واتفاق خاص بالأمن السيبراني مع مقدمي	**لا يوجد** في السعودية أي برنامج رسمي معتمد لتقاسم موجودات الأمن السيبراني بين القطاع العام والقطاع	**لا يوجد** في الأردن أي برنامج رسمي معتمد لتقاسم موجودات الأمن السيبراني بين القطاع العام والقطاع الخاص، سواء على المستوى الوطني أو على

مؤشرات الأداء	عمان	السعودية	الأردن
	الخدمات الأمنية الخاصة (برنامج ميكروسوفت للتعاون الأمني)	الخاص، سواء على المستوى الوطني أو على مستوى القطاعات	مستوى القطاعات. إلا أنه سيتم معالجة هذا الأمر في إطار خارطة الطريق لإنشاء الفريق الأردني للاستجابة للطوارئ الحاسوبية CERT
4-5 المشاركات الدولية: المشاركة المعترف بها رسمياً في المنصات والمحافل الإقليمية و/أو الدولية للأمن السيبراني	عمان عضو في مبادرة ITU-IMPACT ، ولها حق الوصول إلى الخدمات ذات الصلة بالأمن السيبراني. كما أن الفريق العماني للاستجابة للطوارئ الحاسوبية OCERT عضو في FIRST. وقد شاركت عمان في أنشطة الأمن السيبراني الدولية التالية: - FIRST ، المؤتمر والاجتماعات السنوية في اليابان، مالطا، النمسا، الولايات المتحدة، بانكوك - اجتماعات CSIRT الدولية لـ CMU . اليابان، مالطا، النمسا، الولايات المتحدة، بانكوك - اجتماعات فرق الاستجابة للطوارئ الحاسوبية (CERT) بدول مجلس التعاون الخليجي. اجتماعات مستمرة، المملكة العربية السعودية، قطر، مسقط - فريق العمل المعني بالإطار القانوني لل COP في المنطقة العربية يونيو 2013 - القاهرة	السعودية عضو في مبادرة ITU-IMPACT، ولها حق الوصول إلى الخدمات ذات الصلة بالأمن السيبراني. وقد شاركت السعودية في الأنشطة الآتية التي تختص بالأمن السيبراني: - APWG - OIC-CERT - The Honeynet Project.	الأردن عضو في مبادرة ITU-IMPACT ، ولها حق الوصول إلى الخدمات ذات الصلة بالأمن السيبراني. كما أنه عضو في مجموعة عمل فرق الاستجابة للطوارئ الحاسوبية CERT التابعة لمنظمة المؤتمر الإسلامي والتي تهدف إلى توفير إطار للدول الأعضاء لاستكشاف وتطوير مبادرات تعاونية وشراكات في مجال الأمن السيبراني بحيث تعزز القدرة على الاعتماد على الذات في هذا

مؤشرات الأداء	عمان	السعودية	الأردن
	– اجتماع القمة بخصوص الدفاع السيبراني 2012 و 2013، مسقط – ITU–IMPACT التعلم التطبيقي لفرق الاستجابة لحالات الطوارئ، 17–15 يوليو 2012 – عمان، الأردن – المنتدى الأول للأمن السيبراني للطاقة والمرافق – أبو ظبي 2012 – الإطار القانوني للدول العربية COP – الجزائر 2012 – المنتدى العربي لحوكمة الانترنت – أكتوبر 2012 – الكويت – مؤتمر واجتماع سنوي لفرق الاستجابة للطوارئ الحاسوبية (CERT) في دول منظمة المؤتمر الإسلامي 2012 – مسقط – المؤتمر الخليجي للجريمة السيبرانية 2011، مسقط – ورشة عمل إقليمية للاتحاد الدولي للاتصالات بشأن "سياسة الدعوة وبناء القدرات في مجال حماية الأطفال على الإنترنت في المنطقة العربية" مسقط–عمان 30–31 أكتوبر 2011 – MIS – CISO، القمة التنفيذية–2010مسقط – مؤتمر لفرق الاستجابة للطوارئ الحاسوبية (CERT) في دول منظمة المؤتمر الإسلامي 2009، كوالالمبور، 2010 الإمارات العربية المتحدة ، 2011 مسقط – مؤتمر 2008 GOVCERT،		الشأن. كما استضاف الأردن – وشارك – في: ITU–IMPACT – التعلم التطبيقي لفرق الاستجابة لحالات الطوارئ، 17–15 يوليو 2012 – عمان، الأردن. كما شارك الأردن في تمرين الدرع السيبراني الدولي (ICSE) ، والذي عقد في تركيا عام 2014

مؤشرات الأداء	عمان	السعودية	الأردن
	روتردام، هولندا – ورشة عمل لفرق الاستجابة للطوارئ الحاسوبية (CERT) ، 2008، القاهرة، مصر – اجتماع فريق العمل للأمن السيبراني بالاتحاد الدولي للاتصالات ITU، 2007 جنيف، سويسرا		