حوليات آداب عين شمس المجلد 51 (عدد يوليو – سبتمبر 2023)
http://www.aafu.journals.ekb.eg
(دورية علمية محكمة)
جامعة عين شمس
كلية الآداب

تحديات وتهديدات الأمن السيبراني وكيفية التغلب عليها

د/ بدر عدنان أحمد سعد الخبيزي*

عميد دكتور– أستاذ مشارك بأكاديمية سعد العبد الله للعلوم الأمنية بالكويت
Alkhubaizi@hotmail.com

تاريخ الاستلام: 2020/05/18
تاريخ قبول البحث: 2020/06/01
تاريخ النشر: 2023/09/30

المستخلص:

هدف البحث الحالي إلي رصد بعض التحديات والتهديدات التي تواجه الأمن السيبراني في الوقت الحالي. أيضا من أهداف البحث تقديم مجموعة من الإجراءات والتوصيات لكيفية التغلب علي هذه التحديات والتهديدات أو التخفيف من حدتها أو تقليل عددها.وهذا تطلب إلقاء الضوء علي ماهية الأمن السيبراني وذلك من حيث: التعريف والأهداف والأهمية.وكنوع من التمهيد لكل ذلك تم تعريف مفهوم الأمن وتوضيح أهميته وتحديد أنواعه. أيضا تم تعريف الجريمة السيبرانية وتحديد بعض خصائصها ووسائلها.والبحث يعتبر من البحوث النظرية المكتبية ومن نمط البحوث الوصفية الكيفية التي تهدف إلي وصف الظاهرة موضوع البحث من خلال الكتابات والأدبيات (مثل: الكتب والبحوث والرسائل العلمية) المتاحة عن الموضوع.ومن أهم نتائج البحث رصد بعض التحديات والتهديدات التي تواجه الأمن السيبراني في الوقت الحالي، وتقديم مجموعة من الإجراءات والتوصيات لكيفية التغلب عليها.

الكلمات المفتاحية:الأمن، الأمن السيبراني، الجرائم السيبرانية.

مقدمة:

يعتبر الأمنSecurity والاستقرار من المرتكزات الأساسية لبنيان أي مجتمع وتماسكه، وهو ما يحتاج إلى قيام جميع منظمات المجتمع وخاصة المؤسسات الحكومية والأجهزة الأمنية مراعاة ذلك. ولقد اصبح الأمن ليس منشغلا فقط بمكافحة الجريمة سواء بالوقاية منها أو العلاج لها، بل أيضا منشغلا بحياة الإنسان وكرامته والمساهمة في تحقيق التنمية البشرية المستدامة.

وفي الماضي كان الأمن قاصرا فقط علي المحافظة علي الأمن بمفهومه العسكري والعلاجي، إلا أنه في الوقت الحاضر أصبح الأمن له بعد وقائي وشريك للدولة في تحقيق التنمية، وأصبح له أنواع ومجالات عديدة، منها: الاجتماعي والاقتصادي والبيئي والسياسي والمعلوماتي ...

ونظرا لظهور عوامل عديدة تمثلت علي سبيل المثال في الثورة الرقمية المعاصرة والمتمثلة في الاستخدام الكثيف لتكنولوجيا الاتصالات والمعلومات والذكاء الاصطناعي وإنترنت الأشياء وزيادة انتشار واستخدام شبكة الإنترنت وتحول البيانات إلي بيانات ضخمة وخطورة سرقة هذه البيانات وظهور ما يسمي بالهجمات الرقمية الخطرة والفيروساتالخبيثة ... ظهور نوعا جديدا من الأمن يطلق عليه بالأمن السيبرانيCybersecurity أو الأمن الرقمي Digital security أو أمن المعلومات Information security أو أمن الحاسب الآلي Computer security كمجال من مجالات تكنولوجيا المعلومات يهدف إلي حماية البيانات والمحافظة علي سريتها وعدم سرقتها، وحتي لا يتم استخدامها ضد الأفراد والمؤسسات والشركات والدول.

بمعني أن الأمن السيبراني هدفه الرئيسي هو صد الهجمات السيبرانية ومكافحة الجرائم السيبرانية، وذلك من خلال حماية الأفراد والمؤسسات والأنظمة من حالات الاختراق الرقمي أو الدخول غير المصرح به أو التهديدات الأمنية الخطيرة، والتي قد تؤثر على خصوصية البيانات والمعلومات لاسيما الحساسة والخطيرة منها وكذلك إدارة عملية الإنتاج ذاتها، خاصة إن الصناعات بمختلف أنواعها الآن أصبحت مرتبطة ارتباطًا وثيقًا بالتكنولوجيا.

وكما كان لظهور شبكة الإنترنت وتدفق المعلومات أثرا إيجابيا في كافة مجالات الحياة، فقد شكل هذا الأمر مصدر تهديد لمستخدمي هذه الشبكة من خلال ما يعرف بالهجمات والجرائم السيبرانية، والتي من ضمن نتائجها إيقاع ضرر كبير وخسائر فادحة مثل: سرقة البيانات أو تزييفها أو محوها أو الابتزاز للضحية من قبل المهاجمين وجرائمي المعلومات والإنترنت.

ومن هنا زادت أهمية تحقيق الأمن السيبراني لحماية مستخدمي شبكة الإنترنت من هذه الهجمات والجرائم السيبرانية. وبالفعل أهتمت كل الدول تقريبا بذلك نتيجة هذه زيادة المخاطر المترتبة علي عدم الاهتمام بهذا النوع من الأمن. أيضا أغلب الدول في الوقت المعاصر جعلت التوعية الأمنية جزء أساسي للعاملين في جهات العمل

مهما كان تخصص الجهة، بسبب ارتفاع استخدام التقنية خلال العمل واعتماد الأنظمة الإلكترونية خلال العمل (الحسين: 2022، 10).

والمشكلة هي أن تحقيق الأمن السيبراني ليس بالعملية السهلة والبسيطة نظرا لعدة أسباب منها: أن الأمن السيبراني يواجه كل يوم بتحديات وتهديدات عديدة ومتنوعة وسريعة، مما يتطلب معه ضرورة اليقظة والسرعة والاستجابة الفعالة والواعية والتحديث التكنولوجي المستمر والقيام بالعمل المطلوب علي أعلي مستوي لمواجهة هذه التحديات والتهديدات.

والبحث الحالي يهدف إلي إلقاء الضوء علي ماهية الأمن السيبراني وذلك من حيث: التعريف والأهداف والأهمية والفوائد. أيضا البحث يهدف إلي رصد بعض التحديات والتهديدات التي تواجه الأمن السيبراني في الوقت الحالي، وتقديم مجموعة من الإجراءات والتوصيات لكيفية التغلب علي هذه التحديات والتهديدات أو التخفيف من حدتها أو تقليل عددها.وكنوع من التمهيد لكل ذلك سيتم تعريف مفهوم الأمن وتوضيح أهميته وتحديد أنواعه. أيضا تم تعريف الجريمة السيبرانية وتحديد بعض خصائصها ووسائلها.

والبحث يعتبر من البحوث النظرية المكتبية ومن نمط البحوث الوصفية الكيفية التي تهدف إلي وصف الظاهرة موضوع البحث من خلال الكتابات والأدبيات (مثل: الكتب والبحوث والرسائل العلمية) المتاحة عن الموضوع.

تعريف الأمن:

الأمن في اللغة هو الاطمئنان والثقة وعدم الخوف وعدم الخيانة (ابن منظور: 1990 ؛ مجمع اللغة العربية: 2004). والأمن الإنساني اصطلاحا هو شعور مرتبط بالبيئة الخارجية للإنسان بما فيها من استقرار وحماية ونظام توفرها له، فعندما يتحقق للمجتمع الأمن الداخلي (استقرار الأوضاع، نسبة جرائم قليلة، إخلال محدود بالقانون) والأمن الخارجي (عدم وجود أي تهديد أو غزو خارجي علي الدولة) فإن الإنسان يشعر بالأمان (أبو النصر: 2016، ص 88).

ومن تعريفات الأمن الإنساني:

1-هو الأمن البشري والحماية من التهديدات الواسعة الانتشار في مختلف المجالات، والتي تستهدف بقاء الناس وبخاصة أضعف الفئات في المجتمع في مستوي معيشي أفضل والمحافظة علي كرامتهم (حقي: 1999، 10).

2-هو أمن الإنسان من الخوف والقهر والعنف والتهميش والحاجة والحرمان وعدم التمكين الاجتماعي.وهو إي محاولة لخلق ديناميكية تدمج الإنسان في مشروعات التنمية، بدلا من التركيز على استقرار النظام السياسي (أمين: 2009، 8).

إن تحقيق الأمن الإنساني أو البشري سواء كان داخلياً أو خارجياً في أي مجتمع سيؤدي بلا شك إلى تحقيق الأمان لدى الإنسان والمجتمع بشكل كبير، يقول الله تعالى: (فليعبدوا رب هذا البيت الذي أطعمهم من جوع وأمنهم من خوف) سورة قريش الآيتان 3 ــ 4. ولا شك أن اقتران الإطعام من الجوع، والأمن من الخوف يوضح بجلاء أن الأمن شيء ضروري ومهم، لأنه تلى في الترتيب حاجة أساسية في حياة الإنسان، وهي الحاجة إلى المأكل.وتأكيدا علي ذلك يقول الرسول الكريم صلى الله عليه وسلم: " من بات آمناً في سربه، ومعافاً في بدنه، وعنده قوت يومه، فقد حيزت له الدنيا بحذافيرها " صدق رسول الله.

أهمية الأمن الإنساني:

يعزى تزايد الاهتمام بدراسة ظاهرة الأمن إلى حقيقة مركزية لم تعد ترى في مفهوم الأمن مفهوماً ضيقاً يقتصر على السياسة الدفاعية العسكرية فقط بل ترى فيه مفهوماً يتم بالشمول ليأخذ بنظر الاعتبار كل المتغيرات الداخلية الخارجية، ذلك أن الأمن بكل أبعاده يشكل الركيزة الأساسية لتقدم المجتمع ورفاهية أفراده(سالم: 2003، 30).إن تحقيق الأمن في أي مجتمع، يساعد على زيادة الإنتاج، فلا يمكن أن نتوقع من أي إنسان أن ينتج وهو في حالة خوف أو شعور بعدم الطمأنينة وعدم الحماية .. ويقول الله تعالى (الذين أمنوا ولم يلبسوا إيمانهم بظلم أولئك لهم الأمن وهم مهتدون) صدق الله العظيم، سورة الأنعام، الآية 82" . وفي هذه الآية يعد الله عباده بالأمن كثمرة للإيمان والعمل الصالح.

ولا يمكن لأي دولة أن تتطور وتتقدم وتحقق الرفاهية لمواطنيها إلا بتحقيق الأمن والاستقرار لهم . بل إن الأمن هو الركيزة الأولى التي تقوم عليها بناء الحضارات، ولولا الأمن لحلت الفوضى واستشرى الفساد في البر والبحر، ولأصبح الانحراف والتطرف والجريمة والإرهاب ظاهرة تودي بحياة الناس وبالتالي بحياة الأمم (أبو النصر: 2019، 120 ؛ العمرات: 2002، 100).

أنواع الأمن الإنساني:

هناك أنواع عديدة من الأمن، منها: الأمن الاجتماعيوالأمن الاقتصادي والأمن الثقافي والأمن الفكري والأمن السياسي...(الجوير: 2003، 5). أيضا هناك أنواع أخري حديثة من الأمن، مثل: الأمن البيئي والأمن

السياحي والأمن السيبراني. والبحث الحالي سوف يلقي الضوء علي النوع الأخير من الأمن، والذي يعتبر من أهم مجالات الأمن في القرن الحادي والعشرين.

تعريف الأمن السيبراني:

هناك تعريفات عديدة لمفهوم الأمن السيبراني منها:

1-الأمن السيبراني هو عملية حماية الأفراد والمؤسسات والأنظمة من حالات الاختراق الرقمي أو الدخول غير المصرح به أو التهديدات الأمنية الخطيرة، والتي قد تؤثر على خصوصية البيانات والمعلومات لاسيما الحساسة منها (Anderson : 2000، 15).

2-الأمن السيبراني هو مجموعة الإجراءات التقنية التي تهدف إلي حماية البيانات والمعلومات والهوية الشخصية والمعدات التقنية من أي شكل من أشكال الوصول غير المصرح به إلي تلك البيانات والمعلومات والمعدات (Pusey &Sadera: 2011، 82).

3-الأمن السيبراني هو فن وجود واستمرارية المعلومات من خلال ضمان وحماية المعلومات وأصولها وبنيتها التحتية في الفضاء السيبراني (MandarinoCanongia&: 2014، 63).

4-الأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية (Schneier: 2019، 10).

5-الأمن السيبراني هو ممارسة حماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة (Haag: 2020، 12).

6-الأمن السيبراني هو فن وعلم حماية البيانات والمعلومات وأجهزة الحاسب الآلي والشبكات من الدخول غير المصرح به أو غير المرخص به وصد الهجمات السيبرانية (Barker: 2020، 20).

7-الأمن السيبراني هو ممارسة الدفاع عن أجهزة الحاسب الآلي والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الخبيثة (الحربي: 2022، 5).

وفي ضوء ما سبق يمكن تعريف الأمن السيبراني بأنه مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به أو سوء الاستغلال للمعلومات التي يمتلكها فرد أو منظمة أو شركة

أو دولة، وذلك من قبل فرد أو مجموعة أو منظمة أو شركة أو دولة تهدف من ذلك إحداث الضرر أو الابتزاز أو التلاعب بالنظام الرقمي الخاص بالضحية.

والبحث الحالي كما سبق ذكره يهدف بشكل رئيسي إلي رصد بعض التحديات والتهديدات التي تواجه الأمن السيبراني في الوقت الحالي وكيفية التغلب عليها، لذا كان لزاما عرض بعض البحوث والدراسات السابقة المرتبطة بذلك، والاستفادة منها لاحقا في دراسة هذه التحديات والتهديدات، وفي تقديم بعض التوصيات في التعامل مع هذه التحديدات ومواجهة تلك التهديدات.

بحوث ودراسات سابقة في موضوع التحديات والتهديدات التي تواجه الأمن السيبراني:

1-دراسةPusey &Sadera (2011):وهي بعنوان أخلاقيات الأمن السيبراني وتحقيق متطلبات تحقيق ذلك. وهدفت الدراسة إلي تحديد درجة وعي المعلمين وطلبة كلية المعلمين بمفاهيم الأمن السيبراني والانتهاكات السيبرانية والسلامة السيبرانية، ودرجة معرفتهم بتدريس هذه المفاهيم. وأظهرت نتائج الدراسة أن درجةمعرفة 80 % من المعلمين وطلبة كلية المعلمين في عينة الدراسة بمفاهيم الأمن السيبراني والانتهاكات السيبرانيةوالسلامة السيبرانيةدرجة منخفضة جدًّا.

وأن 20 % منهم فقط لديه وعي بدرجة متوسطة بتلك المفاهيم. وأظهرت النتائج بأهمية توعية المعلمين والطلبة بمفاهيم والأمن السيبراني والانتهاكات السيبرانية والسلامة السيبرانية. أيضا أظهرت النتائج أنه لا يوجد لدى المعلمين تصور واضح لكيفية تدريس تلك المفاهيم في المناهج التعليمية للتلاميذ والطلاب.

2-دراسة الأطرش وعساف(2018):وهي بعنوانمعوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية.وهدفت الدراسة إلى التعرف على معوقات مكافحة الجرائم المعلوماتية أو السيبرانية في الضفة الغربية بفلسطين. وبينت نتائج الدراسة أن معوقات مكافحة الجرائم المعلوماتية المتعلقة بالجريمة المعلوماتية ذاتها كانت بدرجة كبيرة، في حين جاءت درجة المعوقات المتعلقة بالمجني عليه بدرجة متوسطة، أما درجة المعوقات المتعلقة بالتحقيق الجنائي كانت كبيرة.ومن توصيات الدراسة: ضرورة تدريب وتأهيل العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية، وضرورة التنسيق بين الأجهزة الأمنية لمكافحة تلك الجرائم، وتشجيع المواطنين عن الإبلاغ عن الجرائم المعلوماتية، وزيادة وعي المواطنين بمخاطر تلك الجرائم.

3-دراسة الشهري (2019):وهي بعنوان رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية. سعت الدراسة إلي وضع رؤية استراتيجية للحد من الجرائم الإلكترونية من خلال

التعرف علي طبيعة تلك الجرائم وأسبابها ورصد التهديدات والتحديات والمخاطر التي تواجه الأمن السيبراني في المملكة العربية السعودية. واستخدمت الدراسة المنهج الوصفي، واعتمدت علي الاستبيان ونموذج SWOT كأداتي لجمع البيانات المطلوبة. ومن أهم نتائج الدراسة تحديد بعض خصائص الجريمة السيبرانية، ومنها: تنوع أشكالها؛ وعدم اعترافها بأي حدود مكانية أو زمنية ؛ زيادة انتشارها ؛ ويترتب عليها خسائر فادحة؛ وأن التقنيات الحديثة وفرت لها فرصا غير مسبوقة لانتشارها... وأن انتهاك السياسات الأمنية يمثل أهم التهديدات التي تواجه الفضاء السيبراني.

4-دراسة حبيباتي (2019): وهي بعنوان معوقات مكافحة الجريمة المعلوماتية. وهدفت الدراسة إلى التعرف على المشكلات والصعوبات القانونية والفنية التي تعترض سبل مكافحة الجريمة المعلوماتية أو السيبرانية. وبينت النتائج أن الصعوبات التي تعترض سبل مكافحة الجريمة المعلوماتية متعددة، وكلها تنبع من كون هذه الجرائم تختلف جملة وتفصيلا عن الجرائم العادية، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحتها، سواء أثناء إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمه للعدالة، أو خلال ملاحقة الجناة وكشف جرائمهم عبر الحدود.

5-دراسة سعود (2019): وهي بعنوان عوامل ارتكاب الجريمة الالكترونية وسبل مواجهتها – دراسة تحليلية في قانون مكافحة الجرائم الالكترونية الكويتي. وهدفت الدراسة إلي التعرف على العوامل المؤدية لارتكاب الجريمة الالكترونية أو السيبرانية في المجتمع الكويتي وسبل مكافحتها في ضوء قانون مكافحة الجرائم الالكترونية الكويتي. وقد توصلت الدراسة إلى أن أكثر العوامل التي تؤدي إلى ارتفاع معدل الجرائم الالكترونية في المجتمع الكويتي هي: سرعة حدوث التغيرات التقنية وعدم مواكبة الثقافة المجتمعية لتلك التغيرات، وضعف مستوى فاعلية وكفاءة قانون مكافحة جرائم تقنية المعلومات رقم (63) لسنة 2015. أيضا من نتائج الدراسة عدم وجود فروق ذات دلالة إحصائية في اتجاهات أفراد العينة حول العلاقة ما بين العوامل الاجتماعية وارتكاب الجريمة تعزى للمتغيرات الديمغرافية(الجنس، مكان الإقامة، العمر، الحالة الاجتماعية، المؤهل العلمي، طبيعة العمل،الانفاق الشهري).

6-دراسة الزرفي (2020):وهي بعنوان الجريمة المعلوماتية الماسة بالحياة الخاصة، دراسة مقارنة. وهي دراسة قانونية أوضحت الركن المعنوي والمادي والشرعي للجريمة المعلوماتية، ومقارنتها بالجريمة التقليدية. أيضا رصدت الدراسة مجموعة من وسائل ارتكاب الجريمة المعلوماتية (مثل: الحاسب الآلي وشبكة الإنترنت والهاتف الذكي والتصوير والتسجيل الصوتي ...). ومن توصيات الدراسة: أن المشرع العراقي عليه الإسراع

بإصدار قانون الجرائم المعلوماتية لوضع تعريف محدد وشامل لهذه الجريمة وأشكالها وأنواعها وكيفية مكافحتها سواء علي مستوي الوقاية أو العلاج.

7-دراسة كل من الحسيني ومرعي (2020):وهي بعنوان الجرائم الإلكترونية الواقعة علي الأموال، دراسة مقارنة. وهي دراسة قانونية قدمت تعريفات عديدة للجرائم الإلكترونية، ومنها: كل سلوك إجرامي يتم بمساعدة الحاسبات الآلية ضد البشر أو ضد المنظمات أو ضد الدول سواء ما يخص الأموال أو المعلومات. أيضا حددت الدراسة بعض خصائص الجرائم الإلكترونية ومنها: جريمة غير تقليدية، جريمةذكية، جريمة منظمة، جريمة عابرة للحدود، تستخدم أعلي مستوي من التكنولوجيا، صعب إثباتها، صعب القبض علي المجرم، صعوبة معاقبة المجرم، تتضمن تحايل وتلاعب في المعلومات والأموال،...وفي نهاية الدراسة تم توضيح كيفية مكافحة الجرائم الإلكترونية من خلال المواجهة الدولية للجريمة والمواجهة الوطنية للجريمة، مع توضيح موقف المشرع العراقي من ذلك.

8-دراسة بوجداىن (2021): وهي بعنوان تحديات مواجهة الجرائم المعلوماتية وآليات الحماية. وهدفت الدراسة إلى التعرف على التحديات التي تطرحها الجرائم المعلوماتية أو السيبرانية والتي تجعل عملية الحد منها مستعصية، والكشف عن آليات تحقيق الأمن السيبراني والحد من الحروب السيبرانية. وأوضحت نتائج الدراسة أن هناك العديد من التحديات السيبرانية على المستوى الدولي من بينها: أن الجريمة السيبرانية عابرة للحدود لا تعترف بوجود الحواجز الجغرافية، وهذا صعب من عملية التحقيق والتقاضي، والتحدي الثاني هو ازدياد عدد المستخدمين وارتفاع مستوى الثقة في وسائل التكنولوجيا حيث أصبحت معظم المعاملات والاتصالات تتم عن طريق وسائل تكنولوجيا المعلومات الاتصال، وهذا يزيد من إمكانية التعرض للمخاطر المعلوماتية.

9-دراسة سيد (2021):وهي بعنوان استراتيجية مكافحة الجرائم الإلكترونية في العصر المعلوماتي لتعزيز رؤية مصر 2030. سعت الدراسة إلي وضع استراتيجية مكافحة الجرائم الإلكترونية أو السيبرانية في العصر المعلوماتي لتعزيز رؤية مصر 2030 وذلك من زوايا مختلفة وعلي كافة المستويات، والتي من شأنها تساهم في حماية المجتمع من الشائعات والأخبار المضللة المثارة علي مواقع وسائل التواصل الاجتماعي، وتأمين قطاعات الدولة المختلفة من الجرائم السيبرانية بواسطة تحقيق الأمن السيبراني لحماية المعلومات من الاختراقات والقرصنة. وتم جمع البيانات في الدراسة من خلال استطلاع رأي الخبراء المختصين عبر أسلوب دليفي وأسلوب التخطيط الاستراتيجي. وقدمت الدراسة آليات مقترحة لمكافحة تهديدات وتحديدات الأمن السيبراني سواء كانت آليات: قانونية وأمنية وتقنية وإعلامية وتربوية وتعليمية.

10-دراسة هيراس وآخرونHerath& .et. al (2022): وهي بعنوان ممارسات الأمن السيبراني لمستخدمي وسائل التواصل الاجتماعي.والتي استهدفت التعرف على مستوى الوعي بممارسات الأمن السيبراني والسلوك السيبراني لدى مستخدمي وسائل التواصل الاجتماعي. وقد توصلت الدراسة إلى أن هناك العديد من التهديدات السيبرانية الموجودةداخل منصة وسائل التواصل الاجتماعي، مثل: التسلط عبر الإنترنت، والمطاردة عبرالإنترنت، وسرقة الهوية، والانتشار الزائد للمعلومات الاجتماعية، وتلف السمعة الشخصية، وخرقالبيانات الخصوصية، والبرمجيات الخبيثة، وانقطاع الخدمة، والقرصنة، والوصول غير المصرح به إلى المعلومات حسابات وسائل التواصل الاجتماعي، والإضرار بصحة وحياة الآخرين.

11-دراسة المنتشري وحريري (2022): وهي بعنوان درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جده من وجهة نظر المعلمات. ولتحقيق أهدافالدراسة تم اتباع المنهج الكمي الوصفي التحليلي، وتم جمع البيانات بواسطة استبيان طبق علي عينة عشوائية مكونة من362 من معلمات المرحلةالمتوسطة بمدينة جدة. وأظهرت النتائج أن معلمات المرحلة المتوسطة على درجة متوسطةمن الوعي بكل من مفاهيم الأمن السيبراني ومخاطر الأمن السيبراني، وانتهاكات الأمنالسيبراني.وتوصلت الدراسة إلى بعض التوصيات أهمها عقد دوراتتدريبية للمعلمات في مجال الأمن السيبراني، وورش عمل حول إجراءات الحماية ضد الهجمات السيبرانية، والتنسيق بين وزارة التعليم والجهات المشرفة على الأمنلسيبراني والهيئة الوطنية في السعودية للأمن السيبراني لاتخاذ الإجراءات اللازمة ولتنمية الوعي لدىالمعلمات في مجال الأمن السيبراني.

12-دراسة محمد وأحمد (2022): وهي بعنوان الأمن المعلوماتي ومواجهة تهديدات البيئة الرقمية لدي الشباب الجامعي نحو رؤية مقترحة من منظور الخدمة الاجتماعية. وأوضحت الدراسة مفهوم الأمن المعلوماتي وخصائصه وأهدافه. أيضا عرضت الدراسة مجموعة من التهديدات التي تواجه البيئة الرقمية. وتوصلت الدراسة أن للبيئة الرقمية العديد من الإيجابيات علي عقول الشباب الجامعي وأنماط تفكيرهم وما يتبنونه من أساليب علمية وحياتية، ومع ذلك قد يصاحب ذلك العديد من الآثار السلبية التي أصبحت تمثل تحديدات وتهديدات كبيرة للمجتمع بصفة عامة وللشباب بصفة خاصة. وفي نهاية الدراسة تم تقديم رؤية مقترحة من منظور مهنة الخدمة الاجتماعية في معالجة تلك القضية.

التعقيب علي البحوث والدراسات السابقة:

1-تم عرض 12بحث ودراسة سابقة مرتبطة بشكل مباشر بموضوع البحث الحالي.

2-هذه البحوث والدراسات تم اجراؤها في دول عديدة، هي: الكويت والسعودية والعراق وفلسطين ومصر والجزائر وبريطانيا والولايات المتحدة الأمريكية.

3-أوضحت البحوث والدراسات السابقة معظم خصائص الجريمة السيبرانية.

4-أوضحت البحوث والدراسات السابقة أن درجة الوعي والمعرفة بموضوع الأمن السيبراني لدي عينات هذه البحوث والدراسات يتراوح ما بين منخفض ومتوسط.

5-أوضحت البحوث والدراسات السابقة أن الأمن السيبراني يواجه العديد من التحديات والتهديدات والمخاطر، وتم عرض معظمها.

6-ندرة البحوث والدراسات السابقة التي تناولت تحديات وتهديدات الأمن السيبراني، مما دفع الباحث إلي دراسة هذه النقطة البحثية.

7-اقترحت البحوث والدراسات السابقة عدد كبير من المقترحات والتوصيات التي يمكن الاستفادة منها في مواجهة التحديات والتهديدات والمخاطر التي تواجه الأمن السيبراني.

8-استفاد البحث الحالي من هذه البحوث والدراسات السابقة في نقاط عديدة منها: تعريف الأمن السيبراني ورصد التحديات والتهديدات التي تواجه الأمن السيبراني وفي تقديم مجموعة من التوصيات للتغلب علي هذه التحديات والتهديدات.

أهداف الأمن السيبراني:

يمكن تحديد الهدف الرئيسي وراء ظهور الأمن السيبراني هو ظهور ما يعرف بالهجمات الرقمية الخطرة أو الفيروسات الخبيثة أو المنيعة وفيها يتم الهجوم على الأنظمة الرقمية الخاصة بالأفراد أو المنظمات أو بالدول والسيطرة على ما تمتلكه من بيانات هامة وحساسة وخطيرة، وخضوعها للضرر ولعمليات الابتزاز والسرقة وكذلك التخريب المتعمد للمعلومات أو تزيفيها أو تحريفها أو محوها (Barker: 2020، 25).وجراء الخسائر الفادحة التي تسببها هذه الهجمات والجرائم السيبرانية، ظهر الأمن السيبراني، لا بهدف الدفاع أو الحماية فقط من هذه الهجمات والجرائم، بل أيضًا من أجل القيام اكتشاف الثغرات الموجودة في النظام والعمل على إصلاحها فور اكتشافها.وبكلمات أخري فإن هدف الأمن السيبراني هو صد الهجمات السيبرانيةومكافحة الجرائم السيبرانية التي

عادةً تهدف إلى الوصول إلى المعلومات الهامة أو الحساسة أو الخطيرة أو تغييرها أو تدميرها ؛ بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية لديهم أو إفساد عمليات التواصل مع العملاء وتوصيل المنتجات لهم...

أهمية الأمن السيبراني:

في عالم اليوم المتصل، يستفيد الجميع من برامج الدفاع الإلكتروني المتقدمة. على المستوى الفردي، يمكن أن يُسفر الهجوم علي الأمن السيبراني عن الكثير من الأشياء، بدءًا من سرقة الهوية الشخصية وسرقة بيانات الحسابات في البنوك، ومرورًا بمحاولات الابتزاز، ووصولًا إلى فقدان البيانات المهمة، وإحداث الضرر بأعمال المستخدمين ومصالحهم. وتستخدم الشركات والمؤسسات في مختلف القطاعات، مثل الطاقة والنقل وتجارة التجزئة والتصنيع، الأنظمة الرقمية والاتصال عالي السرعة لتوفير خدمة عملاء فعّالة وإجراء عمليات تجارية ميسورة التكلفة. لذا علي هذه الشركات والمؤسسات أن تؤمّن أصولها التكنولوجية أو الرقمية وحماية أنظمتها من أي ضرر أو خلل أو اختراق أو قرصنة أو دخول غير مصرّح به إلى الحاسبات الآلية أو للشبكات. وفي حال حدوث ذلك فإنه يطلق عليه بالهجوم السيبراني. ويؤدي هذا الهجوم في حال نجاحه إلى الكشف عن البيانات السرية أو سرقتها أو حذفها أو تغييرها.

وبإيجاز فإن أهمية الأمن السيبراني تكمن في كونه يحمي ويحافظ على المعلومات الخاصة بالمستخدمين، وخاصة المعلومات التى قد تعرض الأشخاص أو الشركات أو المؤسسات أو الدول للخطر. والقاعدة هنا هو أن أى معلومة قد تكون هامشية أو غير مهمة بالنسبة لبعض المستخدمين قد تكون مهمة للمخترق.ويساعد الأمن السيبراني الدول على المحافظة على سرية معلوماتها من الاختراق من قبل الدول المعادية أو التعرض للهجمات السيبرانية مما يسبب الشلل أو الخسائر أو الفضائح لاقتصادها، وهو بدوره ما يمكن تصوره بكونه نوع من أنواع الحروب الحديثة في عصرنا الحالي.

الجريمة السيبرانية:

هناك تعريفات عديدة لمفهوم الجريمة السيبرانية Cyber Crime منها:

1-كل نشاط غير مشروع موجه لنسخ أو تغيير أو الوصول إلي المعلومات المخزونة داخل النظام التي تحوي علي كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجات الآلية للبيانات (مكاوي: 2010، 27).

2-كل سلوك إجرامي يتم بمساعدة الحاسبات الآلية ضد البشر أو ضد المنظمات أو ضد الدول سواء ما يخص الأموال أو المعلومات (الحسيني ومرعي: 2020، 22-23).

3-هي ممارسة غير شرعية تستهدف التحايل علي نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونيا، وذلك من خلال قراصنة الكتابة أو استخدام برامج الحاسب الآلي الجاهزة (الحربي: 2022، 6).

4-هي مجموعة من الهجمات المنظمة والتي يتم فيها التلاعب بالنظام الرقمي الخاص بالضحية والسيطرة التامة عليه فيما يعرف باسم الهجمات السيبرانية، ولكى يتم حماية الضحية من هذه الهجمات، يجب أن يتم وضع ما يعرف باسم الدرع السيبراني.https://aws.amazon.com/ar/what-is/cybersecurity

أمثلة علي الجرائم السيبرانية:

هناك أنواع عديدة من الجرائم السيبرانية، منها علي سبيل المثال: الجرائم الإلكترونية الواقعة علي الأموال، والابتزاز الإلكتروني، والتحرش الإلكتروني، والتنمر الإلكتروني، والتجسس الإلكتروني، والتزوير المعلوماتي، والإتلاف المعلوماتي...(انظر: صالح: 2021، 8 ؛ السالمي: 2022،124 -139؛ اللقاني: 2023، 193 - 194).

خصائص الجريمة السيبرانية:

للجريمة السيبرانية خصائص عدة منها:جريمة غير تقليدية، وجريمة ذكية، وجريمة منظمة، وجريمة معلوماتية، وجريمة إلكترونية تستخدم أعلي مستوي من التكنولوجيا، وجريمة تستخدم وسائل تقنية ورقمية حديثة وعديدة مثل: الحاسب الآلي وشبكة الإنترنت والهاتف الذكي والتصوير والتسجيل الصوتي، وجريمة متنوعة الأشكال، وجريمة عابرة للحدود الزمانية والمكانية، وجريمة قد تمارس ضد الأفراد أو الجماعات أو المنظمات أو الدول، وجريمة زادت معدلاتها في الوقت الحالي، والتقنيات الحديثة وفرت لها فرصا غير مسبوقة لانتشارها، وجريمة صعب إثباتها، وجريمة صعب القبض علي المجرم فيها، وجريمة فيها صعوبة في معاقبة المجرم، وجريمة تتضمن تحايل وتلاعب في المعلومات والأموال، وجريمة لها آثار سلبية كثيرة وخسائر فادحة... (انظر: مكاوي: 2010، 27-28؛ الحسناوي: 2009، 46 -47؛ الحسيني ومرعي: 2020، 26-28 ؛ الزرفي: 2020، 20-21؛ صالح: 2021، 8؛ السالمي: 2022، 136؛ اللقاني: 2023، 189).

أنواع التحديات والتهديدات التي تواجه الأمن السيبراني:

هناك تحديات challenges وتهديدات threatsعديدة تواجه الأمن السيبراني، تمثل أكبر آفة يتعامل معها العالم الرقمي، والتي غالبًا ما تتسبب في خسائر فادحة يصعب التعامل معها، ودور الأمن السيبراني هنا ألا يقوم

بالدفاع ضد هجماتها فحسب، بل أن يقوم بمنع حدوثها من الأساس. وفي ضوء نتائج البحوث والدراسات السابقة وأدبيات أخري مرتبطة يمكن رصد أبرز هذه التحديات والتهديدات وأكثرها شيوعا كالتالي:

1- البرمجيات الخبيثة:

البرامج الخبيثة أو البرامج الضارة هي نوع من البرامج المصممة للوصول غير المصرح به إلى جهاز الكمبيوتر أو إلحاق الضرر به. بمعني أنها تتضمّن مجموعة من البرامج التي تم إنشاؤها من أجل منح أطراف ثالثة إمكانية الوصول غير المصرّح به إلى المعلومات الحساسة أو السماح لها بتعطيل سير العمل العادي للبنية الأساسية بالغة الأهمية. تشمل الأمثلة الشائعة للبرمجيات الخبيثة أحصنة طروادة وبرامج التجسس والفيروسات.وبكلمات أخري فإن البرمجيات الخبيثة هي فيروسات متقدمة يتم تصميمها بهدف الالتفاف عن أنظمة الحماية المثبتة على النظام والعمل على إحداث ضرر أو خلل فيها، مما يسمح بالتلاعب أو السيطرة على البيانات الحساسة معتمدة في الأساس على الثغرات التي يمكن استغلالها(انظر: الأطرش وعساف: 2018 ؛ حبيباتي: 2018؛ الحسين: 2022).

2- فيروس الفدية الخبيث:

تشير برامج الفدية الخبيث إلى نموذج عمل ومجموعة واسعة من التقنيات ذات الصلة التي تستخدمها الجهات المسيئة لابتزاز الأموال من الكيانات.ويعد فيروس الفدية الخبيث واحد من أخطر الهجمات الإلكترونية في عالمنا الرقمي الحالي والتي طبقًا للإحصائيات العالمية الأخيرة فإن هناك هجوم من نوع الفدية الخبيث تقريبًا كل 10 ثواني على الأقل، وفيه يتم حجب كافة البيانات الخاصة بالضحية وتشفيرها، وعدم السماح له بالدخول عليها إلا بعد دفع فدية مالية كبرى، وكلما كانت هذه البيانات سرية وحساسة، كلما أستغل أصحاب هذه الفيروسات الأمر وفرضوا أوامر تعجيزية كبرى، والتي لا يملك فيها الضحية إلا الرضوخ لها في النهاية (انظر: السالمي: 2022، 119).

https://aws.amazon.com/ar/what-is/cybersecurity

3- تصيد البيانات والمعلومات:

تصيد البيانات والمعلومات هو عملية إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني من المصادر الموثوقة. والهدف هو سرقة المعلومات الحساسة مثل أرقام بطاقة الائتمان ومعلومات تسجيل

الدخول.بمعني أن تصيد المعلومات عملية يتم من خلالها استغلال قلة الثقافةالإلكترونية للضحية أو عدم انتباه لما يعرض أمامه من معلومات، وجعله يشارك بمحض إرادته معلومات حساسة خاصة ببطاقته الائتمانية أو معلومات سرية لا يجب مشاركتها مع العوام ككلمة السر الخاصة بتسجيل الدخول في المنصات الرقمية أو غير من المواقع.وتعد عملية تصيد المعلومات من أكثر أنواع الهجمات الإلكترونية شيوعًا، حيث بلغت نسبة 80% من نسبة الهجمات التي تتم على الأفراد والمؤسسات، وطبقًا لجوجل تم تقدير أكثر من 2.1 مليون موقع مخصص لذلك في عام 2020 م وحده (انظر: الأطرش وعساف: 2018 ؛ حبيباتي: 2019 ؛ الحسين: 2022).

4- استغلال البرامج الثنائية أو ما يعرف بهجوم الوسيط:

في الهجوم الوسيط، يحاول طرف خارجي الوصول بشكل غير مصرّح به إلى الاتصالات في شبكة أثناء تبادل البيانات. تزيد مثل هذه الهجمات من المخاطر الأمنية للمعلومات الحساسة، مثل البيانات المالية. ويعد هجوم الوسيط واحد من الأدوات الشائعة المستخدمة في عمليات الهجمات السيبرانية، وفيها يستغل المهاجم لجوء الضحية إلى مصدر تقني ثاني ضعيف الحماية، ويقوم بالدخول إلى النظام من خلاله كاستغلال شبكة الوايفاي والعمل على اختراق النظام الخاص بالأجهزة المشتركة فيها والعمل على تثبيت برامج خبيثة تساعد في السيطرة عليها.
https://aws.amazon.com/ar/what-is/cybersecurity

5- التصيد الاحتيالي أو المباشر أو ما يعرف بالتصيد بالرمح:

التصيد الاحتيالي أو هجمات التصيد Phishing attacks أو التصيد بالرمح هو تهديد سيبراني يستخدم تقنيات الهندسة الاجتماعية من أجل خداع المستخدمين للكشف عن معلومات التعريف الشخصية. على سبيل المثال، يرسل المهاجمون السيبرانيون رسائل إلكترونية تستدرج المستخدمين للنقر عليها وإدخال بيانات بطاقة الائتمان في صفحة ويب وهمية لإتمام الدفع. يمكن أن تؤدي هجمات التصيد الاحتيالي أيضًا إلى تنزيل مرفقات ضارة تثبّت برامج ضارة على أجهزة المؤسسة أو الشركة.وفي التصيد الاحتيالي يتم استهداف فرد أو مؤسسة بحد ذاتها، والعمل على دراسة كل أنظمة الدفاع والحماية الخاصة بها بالتفصيل، ثم العمل على اكتشاف الثغرات التي يحتويها النظام وآلية تطويعها لصالح عملية اختراق وسيطرة ممنهجة (انظر: الربيعة: 2018، 20 ؛ شلوش: 2018، 190).

6- التسلسل المتقدم طويل الأمد:

وفيها يتم اختراق أنظمة الحماية بشكل خفي وتدريجي، بحيث لا يتم اكتشافه إلا بعد مرور فترة زمنية طويلة، والتي من خلالها يكون الضرر قد تم بالفعل وتمت السيطرة الكلية على النظام بنجاح.

https://aws.amazon.com/ar/what-is/cybersecurity

7- هجمات رفض الخدمة:

وفيها يتم إمطار النظام بوابل من حركات المرور والرسائل والمستخدمين الوهميين، بحيث ينشأ نوع من الضغط على الخوادم وتعطيلها أو التسبب في بطئها، مما يتسبب بوقوع خسائر فادحة ولاسيما إذا كان هذا الهجوم في وقت خاص تتوقع فيه الشركة تحقيق مكاسب كبيرة من إقبال الزائرين عليها وخاصة في وقت المواسم أو التخفيضات أو بعد الإعلان على عروض تنافسية قوية.

https://aws.amazon.com/ar/what-is/cybersecurity

8- **التحايل باستخدام الهندسة الاجتماعية**

الهندسة الاجتماعية ويطلق عليها أحيانا بعلم وفن اختراق العقول. ولقد انتشر هذا المصطلح مع انتشار وسائل التواصل الاجتماعي Social media وتعددها. ويشير التحايل باستخدام الهندسة الاجتماعية إلي مجموعة الأساليب التي يستخدمها المجرمون في الحصول علي المعلومات الحساسة، أو اقناع الضحايا بتنفيذ بعض الإجراءات التي تساعد علي اختراق أنظمتهم والإضرار بهم. وهناك من عرف التحايل باستخدام الهندسة الاجتماعية بأنها نوع من أنواع الهجوم علي السرية، وتنطوي علي عملية التلاعب النفسي في أداء الأعمال، أو دفع الضحية للتخلي عن معلومات مهمة (انظر: عبد الصادق: 2014، 30 ؛ السالمي: 2022، 124).بمعني أنها أسلوب يستخدمه الخصوم لاستدراج البعض إلى الكشف عن المعلومات السرية أو الحساسةالخاصة بهم، بقصد الضرر أو طلب مبالغ نقدية.

https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html#~types-of-threats

ويعتبر التحاليل باستخدام الهندسة الاجتماعية من أخطر التحديات والتهديدات للأمن السيبراني وأكثرها انتشارا لأنها لا تقتصر علي الاتصال عبر شبكة الإنترنت، بل قد تتم من خلال المواقف الحياتية للضحية، ويستغل المهاجمون ما ينشره رواد وسائل التواصل الاجتماعي من معلومات للإيقاع بهم وايذائهم بشكل أو بآخر)Jonson: 2013، 40). أيضا ترجع خطورة التحايل باستخدام الهندسة الاجتماعية إمكانية دمجه مع أي من التهديدات المذكورة آنفا.

9- هجمات البلوكتشين والعملات المشفرة:

تستهدف هجمات البلوكتشين والعملات المشفرة Block chain and crypto currency attacks :بيانات الشركات الكبيرة الأمر الذي من شأنه أن يُعرّض بيانات العملاء فيها والعمليات التجارية التي تقوم بها إلى مخاطر كبيرة وآثار كارثية لا حصر لها.

1- هجمات الذكاء الاصطناعي:

ببساطة يعرف الذكاء الاصطناعي Aartificial Intelligence بأنه عمل برامج حاسب آلي قادرة علي محاكاة السلوك الإنساني المتسم بالذكاء. وهو أيضا دراسة القدرات الذهنية من خلال استخدام النماذج الحاسوبية (Computational model انظر: Dean: 1994، 10). ويستخدم منفذي هجمات السيبرانية هجمات الذكاء الاصطناعيAartificial Intelligence attacks : كوسيلة للوصول إلى المعلومات والبيانات الخاصة بالشركات والتي تكون ذات قيمة عالية من أجل تحقيق مكاسب مادية على حساب هذه الشركات (انظر: أبو النصر: 2020، 80).

2- الهجمات الداخلية:

تُعد الهجمات الداخلية Insider attacks من التحديات الكبيرة التي تواجه الأمن السيبراني لا سيما أنها عمليات تخريب تصدر من داخل الشركة أو المؤسسة ذاتها ومن قِبل أشخاص يعملون فيها بهدف تسريب بعض البيانات لشركات منافسة أخرى. وتؤدي الهجمات الداخلية إلى إلحاق خسائر مالية كبيرة في الشركة التي تتعرض لها.

3- هجمات إنترنت الأشياء:

يقصد بإنترنت الأشياء إلى مجموعة من الأجهزة المتصلة والوسائل التكنولوجية التي تيسر الاتصال بين الأجهزة والشبكات الإلكترونية، وكذلك بين الأجهزة نفسها. وبفضل ظهور رقائق الكمبيوتر ميسورة التكلفة واتصالات النطاق الترددي العالي، أصبحت لدينا الآن مليارات الأجهزة المتصلة بالإنترنت. وهذا معناه أن الأجهزة التي نستخدمها يوميًا يمكنها استخدام أدوات الاستشعار لجمع البيانات والتجاوب بذكاء مع المستخدمين (الظفري: 2022، 6). بمعني أن إنترنت الأشياء يُدمج الأشياء التي نستخدمها يوميا مثل: مثل: مصابيح الإنارة وأجهزة التكييف والمكانس الكهربائية والأبواب والسيارات والآلات مع الإنترنتحتي يمكن إعطاء الأوامر لها لتستجيب وتنفذ هذه الأوامر. وتُشكّل أجهزة إنترنت الأشياء أجهزة حوسبية، ورقمية، وميكانيكية يُمكنها نقل البيانات بشكل مستقل عبر الشبكات الإلكترونية، ومن الأمثلة على هذه الأجهزة أجهزة الكومبيوتر المكتبية

والمحمولة، والهواتف المحمولة الذكية، وأجهزة الأمان الذكية وغيرها من الأجهزة، ومع تزايد استخدام أجهزة إنترنت الأشياء من قِبل الناس والشركات تزايدت التحديات التي يمكن أن تواجه الأمن السيبراني أيضاً، إذ إنّ الوصول إلى هذه الأجهزة من قِبل المخترقين يفسح مجالاً واسعاً أمام القيام بهجمات مُضرّة تُعرف باسم هجمات إنترنت الأشياء.

: https://sotor.com/%D9%85%D8%A7_%D9%87%D9%8A_%D8%A3%D9%86%D9%88%D8%A7%D8%B9_%D8%

هذا ويمكن إضافة تحديات وتهديدات أخري تواجه الأمن السيبراني هي كالتالي:

1-سرعة حدوث الجرائم والهجمات السيبرانية.

2-كون الجرائم والهجمات السيبرانية عابرة للحدود ولا تعترف بالحواجز الجغرافية.

3-مخاطر صعوبة تحديد الكيان المنفذ للجرائم والهجمات السيبرانية في الكثير من الحالات.

4-ارتفاع الخسارة الناجمة عن الجرائم والهجمات السيبرانية مقارنة بالجرائم التقليدية.

5-عدم وجود اختصاص قضائي خاص بهذه النوعية من الجرائم والهجمات السيبرانية.

6-الافتقار إلى رؤية واضحة للشؤون الإلكترونية على المستوى الوطني، بحيث لا تمتلك معظم الدول النامية سياسات وطنية متماسكة في ما يتعلق بفضائها السيبراني.

7-غياب أو عدم كفاية أو ضعف التشريعات الدولية والإقليمية والوطنية في موضوع الأمن السيبراني، مما يعني صعوبة أو عدم قدرة الجهات الرقابية والحكومية والمنظمات من ملاحقة المهاجمين وجرائمي المعلومات والإنترنت وحسابهم.

8-الاعتماد الكبير على الأجهزة والبرامج المستوردة، إذ تعتمد عديد من الدول على استيراد التقنيات والتكنولوجيات الحاسوبية من دول متقدمة بهذا المجال مثل الصين وأميركا، وتستخدمها في قطاعاتها الحيوية مثل الدفاع والأمن والمؤسسات المالية الاقتصادية والحكومية، وبالتالي فإن هذه التبعية تشكل تهديدا خطيرا للأمن القومي لهذه الدول.

كيفية التغلب علي تحديات وتهديدات الأمن السيبراني:

في البداية تم الاستفادة من نتائج البحوث والدراسات السابقة وأدبيات أخري مرتبطة في طرح كيفية التغلب علي تحديات وتهديدات الأمن السيبراني، وخاصة دراسات كل من: سعود (2019) والشهري (2019) وبوجداين

(2021)والخبيزي (2021) والحسين (2022).ويجب التأكيد هنا علي نهج الأمن السيبراني الناجح يجب أن يحتوي على طبقات متعددة من الحماية تنتشر عبر أجهزة الحاسب الآلي أو الشبكات أو البرامج أو البيانات التي يرغب المرء في الحفاظ عليها وحمايتها من أي تلاعب أو ضرر. وبالنسبة للأشخاص والعمليات والتكنولوجيا فإنه يجب أن يكمل كل منها الآخر داخل الشركة أو المؤسسة لإنشاء نظام دفاع متكامل وفعال في مواجهة الهجمات والجرائم السيبرانية. ويمكن لنظام إدارة التهديدات السيبرانية الموحد تسريع وظائف عمليات الأمان الرئيسية التالية: الاكتشاف Discovery والتحقق Investigation والمعالجة Treatment والدفاع Defence والمواجهة Confrontation. وهناك أمور عديدة إذا تم مراعاتها وتطبيقها يمكن في هذه الحالة الوقاية من تحديات الأمن السيبراني أو مواجهة هذه التحديات في حال حدوثها، من هذه الأمور:

أولا: الأشخاص

1-ضرورة عقد دورات تدريبية للمستخدمين في مجال الأمن السيبراني، علي أن تتناول مفاهيم وأهداف وأهمية وفوائد وأنواع الأمن السيبراني والتحديات التي تواجهه وكيفية التغلب عليها.

2-ضرورة عقد ورش عمل حول إجراءات الحماية ضد تحديات وتهديدات ومخاطر الأمن السيبراني تحت اشراف مدربين مختصين في الأمن السيبراني.

3-يجب على المستخدمين فهم المبادئ الأساسية لأمان البيانات والمعلومات والامتثال إليها مثل اختيار كلمات مرور قوية والحذر من المرفقات الموجودة ضمن البريد الإلكتروني والنسخ الاحتياطي للبيانات.

ثانيا: العمليات

1-يجب أن تمتلك المؤسسات إطار عمل حول كيفية التعامل مع الهجمات السيبرانية غير المكتملة أوالناجحة.

2-وضع إطار عمل موحد يوضح كيف يمكنك تحديد الهجمات السيبرانية وحماية الأنظمة واكتشاف التهديدات والتصدي لها والتعافي من الهجمات الناجحة.

ثالثا: التقنية

1-توفير التكنولوجيا هو أمر ضروري لمنح المؤسسات والأفراد أدوات الأمن السيبراني اللازمة لحماية أنفسهم من الجرائم والهجمات السيبرانية.

2-يجب أن توجه الحماية للكيانات التالية: الأجهزة الطرفية مثل أجهزة الكمبيوتر والأجهزة الذكية والموجّهات والشبكات والسحابة.

3-ومن أشكال التكنولوجيا الشائعة المستخدمة لحماية هذه الكيانات، الجيل التالي من الجدران النارية وتصفية DNSوالحماية ضد البرامج الضارة وبرامج مكافحة الفيروسات وحلول أمان البريد الإلكتروني.

https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html#~how-cybersecurity-works

رابعا: المجتمع

1-ضرورة توعية المجتمع بأهمية الأمن السيبراني وبأساليب الحماية من التهديدات والمخاطر التي تواجه الأمن السيبراني، وذلك من خلال وسائل الاتصال الجماهيرية وخاصة التليفزيون والصحف.

2-ضرورة تشجيع المواطنين عن الإبلاغ عن الجرائم السيبرانية.

3-ضرورة وضع وتطوير تشريعات حديثة لمكافحة الهجمات والجرائم السيبرانية.

4-إعداد مصفوفة للمعايير الأخلاقية فيما يتعلق باستخدام النظم الإلكترونية.

5-تخصيص اختصاص قضائي خاص بهذه النوعية من الهجمات والجرائم السيبرانية.

6-ضرورة التنسيق بين الأجهزة الأمنية لمكافحة الهجمات والجرائم السيبرانية.

7-إنشاء مراكز وطنية مسئولة عن حماية الأمن السيبراني للدولة وتدعيمها بالخبراء من مختلف التخصصات المرتبطة (مثل: المركز الوطني للأمن السيبراني بالكويت والمركز الوطني الارشادي للأمن السيبراني بالمملكة العربية والسعودية والهيئة الوطنية للأمن الإلكتروني بالإمارات ...).

خاتمة:

في الختام إن الفضاء السيبراني أو الإلكتروني سلاح ذو حدين لما يتضمنه من إيجابيات من جهة ومن تحديات وتهديدات من جهة أخرى، ولا سيما أن الهجمات والجرائم السيبرانية أصبحت مركّبة ومعقدة ومتسارعة وخطيرة، ويصعب على الكثير من المؤسسات التغلب والدفاع عن أمنها السيبراني دون وجود إستراتيجيات عمل وطنية واقتناء تقنيات وتطبيقات متطورة وممارسات سليمة ضمن إستراتيجية شاملة للأمن السيبراني تأخذ بعين الاعتبار كل الاحتمالات للوقاية من مخاطر وتهديدات هذا الفضاء العالمي المتسع الذي أصبح دون شك ميدان الحرب الجديد بين أطراف القوى العالمية العظمى.

توصيات البحث:

1-إدراج موضوع الأمن السيبراني ضمن بعض المقررات الدراسية المرتبطة في المدارس والكليات لتوعية التلاميذ والطلاب لعدم الوقوع فريسة أو ضحية للمخاطر والجرائم السيبرانية.

2-إصدار نشرات دورية في كل منظمة تشرح مفاهيم وأهداف وأهمية وأنواع وتحديات الأمن السيبراني وكيفية التغلب عليها.

3-أهمية تبادل المعلومات بين المنظمات والدول حول تحديات وتهديدات الأمن السيبراني وكيفية التغلب عليها.

4-أهمية تبادل الخبرات في مواجهة تحديات وتهديدات الأمن السيبراني بين المنظمات والدول.

5-أهمية تبادل البرامج التعليمية والتدريبية في مجال الأمن السيبراني.

6-ضرورة الاطلاع والاستفادة من التشريعات المتعلقة بالأمن السيبراني في الدول الأخرى.

7-أهمية وضع استراتيجية متكاملة متعلقة بالأمن السيبراني وبكيفية تحقيقه ومواجهة التحديات والتهديدات التي تواجهه، وفي حالة وجودها ضرورة تطويرها وتحديثها بما يتناسب مع التغييرات السريعة التي تحدث في هذا المجال.

8-ضرورة استصدار التشريعات وتطويرها في حالة وجودها المتعلقة بالأمن السيبراني لحماية المنظمات والمؤسسات والشركات والدولة من الهجمات والجرائم السيبرانية، وتغليظ عقوبات الجرائم والهجمات السيبرانية.

9-ضرورة تضمين المناهج التعليمية في كليات الشرطة والقانون موضوعات عن الأمن السيبراني.

10-ضرورة توعية وتدريب ضباط الشرطة وأجهزة القضاء والعدالة بأهداف وأهمية وأنواع الأمن السيبراني وتعريفهم بالتحديات والتهديدات التي تواجه الأمن السيبراني وكيفية مواجهتها سواء علي مستوي الوقاية أو العلاج.

11-أهمية التنسيق والتعاون مع الانتربول Interpol (منظمة الشرطة الجنائية الدولية) لتعقب المهاجمين والقراصنة وجرائمي المعلومات والإنترنت عبر الحدود والقبض عليهم.

12-ضرورة استخدام برامج حماية قوية ومتعددة المستويات وليس من السهل اختراقها سواء من الداخل أو من الخارج، ووضع كلمات سر لها صعبة، مع تغيير كلمات السر لها بشكل دوري.

13-أهمية دعم وتشجيع وتمويل البحث العلمي في موضوعات الأمن السيبراني، والاستفادة من نتائجه.

Abstract

Cybersecurity challenges and threats and how to overcome them

By Bader Adnan Ahmed Alkhubaizi

The current research aimed to monitor some of the challenges and threats facing cybersecurity at the present time. The research also aimed to provide a set of procedures and recommendations for how to overcome these challenges and threats, mitigate their severity, or reduce their number.This required shedding light on what cybersecurity is, in terms of: definition, objectives, and importance. As a prelude to all of this, the concept of security was defined, its importance clarified, and its types presented.Also, cybercrime was defined and some of its characteristics and methods were identified.The research was considered a library theoretical research and a type of qualitative descriptive research that aimed to describe the phenomenon that is the subject of research through writings and literature (such as: books, research and scientific theses) available on the subject.One of the most important results of the research is monitoring some of the challenges and threats facing cybersecurity at the present time, and presenting a set of procedures and recommendations for how to overcome them.

key words:Security, cyber security, cyber crimes.

مراجع البحث

أولا: المصادر

1- القرآن الكريم.

2- الأحاديث النبوية الشريفة.

ثانيا: المراجع العربية

1- ابن منظور، جمال الدين محمد . (1990) .*لسانالعرب* . الدار المصرية للتأليف والترجمة. القاهرة . مصر.

2- أبو النصر، مدحت محمد . (2020) . *الذكاء الاصطناعي* . المجموعة العربية للتدريب والنشر . القاهرة . مصر.

3- أبو النصر، مدحت محمد . (2022) .*الدفاع الاجتماعي، المفهوم والمجالات*. كلية الخدمة الاجتماعية . جامعة حلوان . القاهرة. مصر.

4- الجمل، حازم حسن . (2022) . *الحماية الجنائية للأمن الإلكتروني* . دار الفكر والقانون . المنصورة . مصر.

5- الجوير، سعود فارس . (2023) . *الأمن الاجتماعي* . أكاديمية سعد العبد الله للعلوم الأمنية، معهد الشرطة . الكويت.

6- الحربي، عادل راضى . (2020) . *القيادة الرقمية والمستقبل* . كلية محمد بن راشد . دبي . الإمارات.

7- الحسناوي، علي جبار . (2009) . *جرائم الحاسوب والإنترنت* . دار اليازوري العلمية للنشر والتوزيع . عمان . الأردن.

8- الحسين، حسن محمد . (2022) . *أساسيات الأمن السيبراني* . المؤلف . القاهرة . مصر

9- الحسيني، نسرين محسن نعمة و مرعي، محمد حسن . (2020) . *الجرائم الإلكترونية الواقعة علي الأموال، دراسة مقارنة* . المكتب الجامعي الحديث . الإسكندرية . مصر.

10- الربيعة، صالح بن علي . (2018) . " الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت " . *الملتقي الأول للإدارة العامة للتعليم بمحافظة جده* . 27 أبريل . جده . السعودية.

11- الزرفي، علي نعمة جواد . (2020) . *الجريمة المعلوماتية الماسة بالحياة الخاصة، دراسة مقارنة* . المكتب الجامعي الحديث . الإسكندرية . مصر.

12- السالمي، علاء عبد الرزاق محمد . (2022) . *المدخل إلي الأمن السيبراني* . الذاكرة للنشر والتوزيع . بغداد . العراق.

13- الشهري، علي . (2019) . *رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني* . رسالة دكتوراه . كلية العلوم الاستراتيجية . جامعة نايف العربية للعلوم الأمنية . الرياض . السعودية.

14- الظفري، عبد الجبار حسين . (2022) . *إنترنت الأشياء* . المؤلف . صنعاء . اليمن.

15- العمرات، أحمد. (2002). *الأمن والتنمية: منظومة الأمن الشامل كبيئة حاضنة للتنمية المستدامة في ظل ظروف العولمة* . عمان. الأردن.

16- اللقاني، عبد الرحمن علي . (2023) . *إدارة مخاطر الأمن السيبراني المتكامل* . دار اليازودي . عمان . الأردن.

17- المنتشري، فاطمة يوسف وحريري، رنده . (2022) . " درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جده من وجهة نظر المعلمات " . *المجلة العربية للتربية النوعية* . المؤسسة العربية للتربية والآداب والعلوم . المجلد 4 . العدد 13 . يوليو . بنها . مصر.95-140.

18- أمين، خالد . (2009) . *الأمن الإنساني المفهوم والتطبيق والواقع العربي الدولي* .جامعة نايف العربية للعلوم الأمنية . الرياض . السعودية .

19- بوجداين، مارية . (2020) . " تحديات مواجهة الجرائم المعلوماتية وآليات الحماية " . *مجلة العلوم الجنائية* . المركز المغربي للدراسات والاستشارات القانونية وحل المنازعات . العدد 7 . المغرب.

20- حبيباتي، بثينة (2019) . " معوقات مكافحة الجريمة المعلوماتية . *مجلة العلوم الإنسانية* . جامعة الجزائر . المجلد 30 . العدد 1 . يونيه. الجزائر.

21- حقي . ح. (1999) . *النظام الدولي الجديد* . الأهلية للنشر والتوزيع . بيروت . لبنان .

22- خليفة، إيهاب . (2017) . *القوي الإلكترونية كيف يمكن أن تدير الدول شئونها في عصر الإنترنت* . العربي للنشر والتوزيع . القاهرة . مصر.

23- داود، حسن طاهر . (2000) . *جرائم نظم المعلومات* . أكاديمية نايف العربية للعلوم الأمنية . الرياض . السعودية.

24- سالم، صلاح . (2003) . " تكنولوجيا المعلومات الاتصالات والأمن القومي للمجتمع " . *مجلة عين للدراسات والبحوث الإنسانية والاجتماعية*. عمان. الأردن.

25- سعود، فهد صحن مزبان. (2019) .*عوامل ارتكاب الجريمة الالكترونية وسبل مواجهتها: دراسة تحليلية في قانون مكافحة الجرائم الالكترونية الكويتي* . رسالة ماجستير.كلية الدراسات العليا . جامعة مؤتة . الأردن.

26- سيد، أميرة محمد محمد . (2021) . " استراتيجية مكافحة الجرائم الإلكترونية في العصر المعلوماتي لتعزيز رؤية مصر 2030 " . *مجلة البحوث الإعلامية* . كلية الإعلام . جامعة الأزهر . العدد 58 . الجزء 4 . يوليو . القاهرة . مصر.

27- شلوش، نوره . (2018) . " القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول " . *مجلة مركز بابل للدراسات الإنسانية* . جامعة بابل . مركز بابل للدراسات الحضارية والتاريخية . المجلد 8 . العدد 2 . يونيو . بابل . العراق. 185-206.

28- صالح، تامر محمد . (2021) . *الابتزاز الإلكتروني* . دار الفكر والقانون . المنصورة . مصر.

29- عبد الصادق، عادل . (2014) . *الفضاء الإلكتروني والثورة في شئون أجهزة الاستخبارات الدولية* . مركز الأهرام للدراسات السياسية والاستراتيجية . القاهرة . مصر.

30- فهمي، نانيس عبد الرازق . (2023) . " مستقبل الأمن السيبراني في عصر الميتافيرس " . *مجلة آفاق مستقبلية* . مركز معلومات مركز الوزراء المصري . العدد 3 . يناير . القاهرة . مصر.

31- مجمع اللغة العربية . (2004) . *المعجم الوسيط*. ط 4 . مجمع اللغة العربية . القاهرة . مصر.

32- محمد، محمود فتحي وأحمد، حنان طنطاوي . (2022) . " الأمن المعلوماتي ومواجهة تهديدات البيئة الرقمية لدي الشباب الجامعي نحو رؤية مقترحة من منظور الخدمة الاجتماعية " . *المجلة العربية للمعلوماتية وأمن المعلومات*، المؤسسة العربية للتربية والعلوم والآداب . المجلد 3 . العدد 9 . بنها: أكتوبر.

33- مكاوي، محمد محمود . (2010) . *الجوانب الأخلاقية والاجتماعية لجرائم المعلوماتية وجرائم الكومبيوتر والإنترنت* . المكتبة العصرية . المنصورة . مصر.

ثالثا: المراجع الأجنبية

1- Anderson, Ross J. (2000). *Cybersecurity: A Guide to Building Reliable Distributed Systems*, ISBN 0-471-38922-6

2- Barker , Jissica . (2020) . *Confident Cyber Security* . Kogan Page Ltd. N. Y. USA.

3- Canongia , C. &Mandarino . (2014) . *Cybersecurity , the New Challenge of the Information Society* . Routledge . N.Y. USA.

4- Dean, Thomas . (1994) . *Artificial Intelligence , Theory and Practice* **.** Addison Wesley . N.Y. USA.

5- Haag, Stephen &et. al. (2020). *Managing Information Systems for the Information Age*, ISBN 0-07-091120-7.

6- Herath Thilini B. & et. al. (2022) . " Cybersecurity Practices for Social Media Users: A Systematic Literature Review " . *Journal of Cybersecurity* . Vol. 2 . No. 5 -18.

7- Johnson , M. (2013) .*Cybercrime , Security and Digital Intelligence* . Routledge . N.Y. USA.

8- Maury Jacir, Maury. (1988). *Building a secure computer system.* ISBN 0-442-23022-2 1988.

9- Pusey , P. &Sadera, W. (2011) . " Cyberethics , Cypersafety , and Cybersecurity " . *Journal of Digital Learning in Teacher Education* . Vol. 28 . No. 2. 82-88.

10- Schneier, Bruce. (2019). *Secrets and Lies: Digital Security in a Networked World*, ISBN 0-471-25311-1.

رابعا: مواقع شبكة المعلومات الدولية (الإنترنت)

1- https://ar.wikipedia.org/wiki/%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D8%AD%D8%

2- https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html

3- https://www.e3melbusiness.com/blog/cyber-security

4- https://aws.amazon.com/ar/what-is/cybersecurity/

5- https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html#~types-of-threats