التهديدات السيبرانية الناجمة عن تقنيات الثورة الصناعية الرابعة

Cyber Threats Caused by Fourth Industrial Revolution Technologies

لويزة فرحاتي [1*]، مختار قنيش [2]

Louiza Ferhati[1], Mokhtar Kenniche[2]

[1] جامعة باتنة1 (الجزائر)، louiza.ferhati@univ-batna.dz

[2] جامعة مصطفى اسطمبولي معسكر (الجزائر)، Mokhtar.kenniche@univ-mascara.dz

تاريخ الاستلام: 21-12-2021 تاريخ القبول: 02-02-2022 تاريخ النشر: 31-03-2022

ملخص:

ثورة صناعية رابعة تتسم بالتقنيات الرقمية (الذكاء الاصطناعي AI، إنترنيت الأشياءIOT، البيانات الضخمة BIG DATA، الطباعة ثلاثية الأبعاد، الحوسبة السحابية، تقنية البلوكشين)، زعزعت كل القطاعات وجعلت جل المنظمات والهيئات تعيش حالة من اللاتأكد، وأحدثت ضررا جسيما بمنظمات راسخة في العديد من الصناعات، وأزاحت من طريقها أخرى عمرت لأكثر من قرن، ونفس الوقت نجمت عنها تهديدات سيبرانية أضرت بالدول، الهيئات والأفراد على حد سواء.

تسلط هذه الورقة البحثية الضوء على التهديدات السيبرانية الناجمة عن تقنيات الثورة الصناعية الرابعة التي تعاني منها جل القطاعات والصناعات، حيث أصبحت من التحديات الكبرى التي تواجهها الدول على الصعيدين الإقليمي والعالمي، وشكلت سبقا في القضايا ذات الأهمية بالنسبة للأمن الدولي.

كلمات مفتاحية: التهديدات السيبرانية، الأمن السيبراني، الثورة الصناعية الرابعة، التقنيات الرقمية.

تصنيفات JEL : M19، O39، Q59

Abstract:

A fourth industrial revolution pregnant with digital technologies (AI, Internet of Things, IOT, BIG DATA, 3D printing, cloud computing, and blockchain technology), destabilized all sectors and made most organizations and bodies live in a state of uncertainty, and caused severe damage to well-established companies in many industries, and removed others that have lived for more than a century, and at the same time created cyber threats that harmed states, organizations and individuals alike.

This research paper sheds light on the cyber threats resulting from the technologies of the Fourth Industrial Revolution that most sectors and industries suffer from, as they have become one of the major challenges faced by countries at the regional and global levels, and constituted a precedent in issues of importance to international security.

Keywords: *Cyber threats, : Cybersecurity, :Fourth Industrial Revolution, : Digital Technologies.*

Jel Classification Codes: M19, O39, Q59.

[*] **المؤلف المرسل**

1. مقدمة

تعتبر الثورة الصناعية الرابعة ثورة شاملة شأنها شأن الثورات الصناعية (الأولى، الثانية، الثالثة) التي سبقت و انعكس تأثيرها على كافة نواحي الحياة، من خلال تقنيات رقمية غيرت وستغير كثيراً من الأنماط والعادات القديمة، وستزعزع الكثير من القطاعات والصناعات، كما نجم عنها تهديدات سيبرانية تعاني منها الدول والهيئات والأفراد.

هذه التهديدات السيبرانية أصبحت مشكلة تتفاقم يوما بعد يوم بدلاً من أن تُحل، خصوصاً في ظل انتشار فيروس كورونا، حيث أنه في الوقت الذي يركز العالم فيه على التهديد الشامل لجائحة كوفيد19 ، استغل المجرمون السيبرانييون حول العالم هذه الأزمة الصحية لإطلاق تهديداتهم المختلفة، ويبدو أن هذه التهديدات السيبرانية تشكل تحدياً مستحيلاً، فهي بطبيعتها سريعة التغير، ولا محدودة وغير متماثلة، ولذلك أصبح التنبؤ بها وإدارتها في غاية الصعوبة.

انطلاقا مما سبق، يمكن طرح إشكالية هذا البحث في السؤال الرئيسي التالي:

ما هي التهديدات السيبرانية الناجمة عن تقنيات الثورة الصناعية الرابعة؟

وتندرج تحت هذه الإشكالية مجموعة من الأسئلة الداعمة:

- ما هي الثورة الصناعية الرابعة؟
- ماهي التقنيات الرقمية؟
- ما هو الأمن السيبراني؟
- ماهي التهديدات السيبرانية؟

وللإجابة على هذه الإشكالية تم تقسيم البحث إلى المحاور الآتية:

1. الثورة الصناعية الرابعة.
2. التقنيات الرقمية للثورة الصناعية الرابعة.
3. الأمن السيبراني.
4. التهديدات السيبرانية.

- **أهداف البحث:**

تهدف هذه الورقة البحثية إلى:

- التعرف على مفهوم الثورة الصناعية الرابعة، التقنيات الرقمية، الأمن السيبراني؛
- معرفة التهديدات السيبرانية، أنواعها وخصائصها؛
- التعرف على آثارها؛

- **أهمية البحث:**

تكمن أهمية هذا البحث في كونه يتناول موضوع التهديدات السيبرانية الناجمة عن التقنيات الرقمية للثورة الصناعية الرابعة، والذي يعتبر حديث الساعة نظرا لأهميته وخطورته على الأمن الدولي والإقليمي، خاصة في ظل الأزمة الصحية **(كوفيد19)** التي يعيشها العالم.

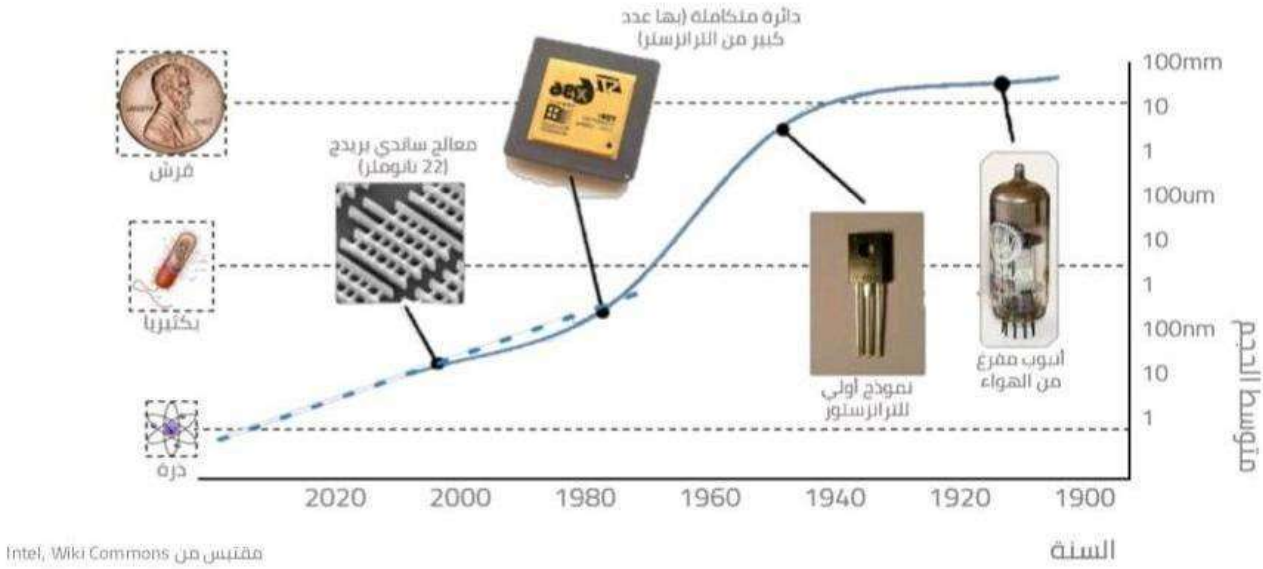
- **منهج البحث:**

تم استخدام في هذه الدراسة المنهج الوصفي، لأنه الأنسب لطبيعة الدراسة مع إشكالية البحث.

2. مفهوم الثورة الصناعية الرابعة

مع بداية الثورة الصناعية الثالثة تسارع نمو التقنية وتطبيقاتها بشكل أسي (Exponentiel) – أي تزايد بوتيرة متسارعة مع مرور الوقت–وأوضح مثال على ذلك هو قانون مور الذي تنبأ عام 1965 أن كثافة الترنزستور (Transistor) وهو "مكون أساسي لجميع الأجهزة الإلكترونية يستخدم لنقل وتضخيم الإشارة الكهربائية" داخل الدوائر الكهربائية ستتضاعف كل عام إلى عامين أي بمعدل 18 شهر، مما يعني قدرة أعلى وتكلفة أقل لهذه الأجهزة وهو ما أثبت صحته ليومنا هذا[1].

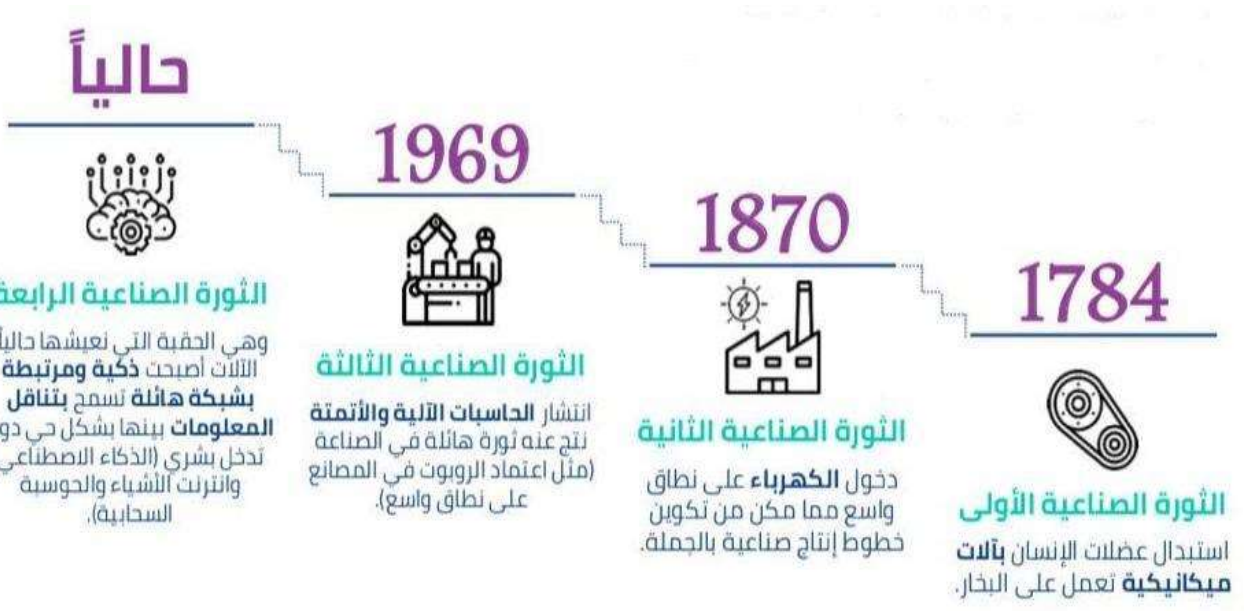
الشكل رقم (01): النمو الأسي للتقنية وتطبيقاتها وفق قانون مور



المصدر: د. معاذ الدهيشي، ما هو التحول الرقمي؟ وكيف تحققه؟ دليل إرشادي للقادة الإداريين، ص 2.

تسارع وتيرة التقنية الأسي أدى إلى نشوء الثورة الصناعية الرابعة في فترة وجيزة نسبيا، وهي الثورة التي نشهدها حاليا نتيجة نمو التقنية بشكل هائل وبالتالي نمو تعقيدها، فالذكاء الاصطناعي هو نتيجة البيانات الضخمة المتراكمة والقدرة التحليلية المتزايدة، وانترنيت الأشياء هي نتيجة لتزايد عدد الأجهزة بشكل مطرد وتطور إمكانية الاتصال فيما بينها بشكل كبير، وأيضا الحوسبة السحابية التي نشأت بسبب تنامي إمكانية الاتصالات وسرعتها وكذلك القدرة التخزينية الرهيبة[2].

الشكل رقم (02): التطور التاريخي للثورات الصناعية الأربع



المصدر:د. معاذ الدهيشي، ما هو التحول الرقمي؟ وكيف تحققه؟ دليل إرشادي للقادة الإداريين، ص 2.
تاريخ الاطلاع: 2021/05/28 على الساعة 12:00

2.2 تعددت تعريفات الثورة الصناعية الرابعة، ومن هذه التعريفات:

يقول البروفيسور **كلاوس شواب** الرئيس التنفيذي للمنتدى الاقتصادي العالمي **(منتدى دافوس):** " مزجت الثورة الرابعة بين ما هو فيزيائي وما هو بيولوجي وما هو تكنولوجي لتحدث تحولات عميقة في كل مناحي الحياة الاقتصادية والثقافية والصناعية بشكل ينذر بعصر جديد وتحولات لم نشهدها من قبل، كما عرّفها تقرير إستراتيجية الإمارات للثورة الصناعية الرابعة بأنها: "ثورة تدمج كل من التقنيات المادية والرقمية والحيوية لإنتاج خدمات ومنتجات غير مسبوقة في قطاعات جديدة".وقد حدد التقرير أبرز خصائص هذه الثورة والتي وصفها بأنها ستكون متسارعة وبنطاق واسع وبتأثير كبير، ما يسبب تحول كبير في الأنظمة والإجراءات وينشأ عن هذا كله: تعقيد أنشطة بيئة العمل بسبب طمس وإزالة الحدود بين العوالم المادية والرقمية والحيوية. ولا يمكن أن نعرف تحديداً ما ستفرزه هذه الثورة من مجالات وقطاعات جديدة، لكننا نستطيع تحديد الإطار العام لها عبر معرفة أهم خصائصها وطابعها المميز للعمل على تمكين أكبر عدد من الأفراد من الإحاطة بمختلف جوانبها من أجل احتواء التغييرات التي ستطرأ ليستعدوا لها بكفاءة[3].

ستخلق هذه الثورة فرصاً عدة، لكنها تضم تحديات كبرى أمنية وسياسية واقتصادية، فمن المرجح أن تظهر ريادة أعمال جديدة بينما ستندثر الكثير من الريادات الحالية خصوصاً تلك التي لا تستثمر في التكنولوجيات الجديدة أو التي تقاوم التغيير والتحولات العميقة التي يعرفها الاقتصاد والمعرفة والصناعة والتواصل[4].

يتجاوز تأثيرها مجرد تقييم تقليدي لأهمية تكنولوجيا المعلومات، وبالتالي التغيير ليس مجرد استخدام برمجيات متطورة، أو أجهزة حديثة، لأنها وكما تصفه شركة "**آي دي سي**" بأنها عملية مستمرة من التغيير المُزعزع.

ويمثل التحول الرقمي القلب النابض للثورة الصناعية الرابعة للشركات ، وعلى الرغم من اتفاق المؤسسات في القطاع الحكومي وغير الحكومي على أهميته إلا أن بعضها مازال متحفظا حيال الانطلاق في مسيرة التحول الرقمي؛ لأنه يعني التزامًا جادًا ودائمًا بالتغيير الشامل، إضافة إلى فشل العديد من المؤسسات التي تبنت التحول الرقمي.

3.2 مفهوم التقنيات المزعزعة

كل ثورة صناعية تمتاز بسمات تقنية معينة تتدرج تحتها عدة أدوات، الثورة الصناعية الرابعة تمتاز بالأنظمة المادية السيبرانية (أي التي لها وجود مادي وترتبط بالعالم الافتراضي) والشبكات وكذلك البيانات (التي تعتبر النفط الجديد)، بحكم القدرة التخزينية الهائلة المتاحة تفرعت عن هذه السمات التقنية عدة أدوات وتقنيات رقمية لها تطبيقاتها المستخدمة حاليا أو محتملة مستقبلا وما يحدد فائدتها هو القيمة المضافة على مستوى تجربة المستفيد وكذلك على مستوى المنظمة ككل[5].

1.3.2 البيانات

لا يمكن تصور الثورة الصناعية الرابعة بدون بيانات، فالقدرة الهائلة على التخزين بالإضافة إلى تسارع وتوسع إمكانيات الاتصال – بالذات شبكة الإنترنيت العالمية – وفر كما عظيما من البيانات تشكل ما يسمى بمجال البيانات العالمي (Global DataSphere)، هذا المجال بلغ حجم بياناته عام 2020 – 40 زيتابايات (40 أس 21 من البايت)، ارتباط التقنيات بمجال البيانات يكون عبر وسيط سواء الربط مباشرة بقواعد البيانات الفرعية أو عن طريق الحوسبة السحابية عبر شبكة الإنترنيت من أي مكان في العالم.

الشكل رقم (03): مجال البيانات العالمي(Global DataSphere)

المصدر:د. معاذ الدهيشي، ما هو التحول الرقمي؟ وكيف تحققه؟ دليل إرشادي للقادة الإداريين، ص 5
تاريخ الاطلاع: 2021/05/28 على الساعة 12:15

تنقسم هذه البيانات إلى بيانات غير منظمة (Unstructured Data) وهي البيانات العشوائية المتراكمة صعبة القراءة والتحليل، وبيانات منظمة (Structured Data)وهي البيانات المرتبة التي يمكن تحليلها عبر أدوات التحليل الرقمي، في كل الأحوال تشكل البيانات منجما ضخما أشبه بـ"المادة الخام "، يمكن تحويله إلى معرفة ذات قيمة عالية لا نستوعب إلى الآن أثرها المستقبلي لذلك تسمى البيانات بالنفط الجديد[6]. وهو ما يوضحه الشكل الموالي.

الشكل رقم (04): حجم البيانات المنظمة وغير المنظمة

المصدر: د. معاذ الدهيشي، ما هو التحول الرقمي؟ وكيف تحققه؟ دليل إرشادي للقادة الإداريين، ص 10.
تاريخ الاطلاع: 2021/05/28 على الساعة 12:25

2.3.2 الشبكات

في الماضي كان الاتصال عبارة عن ارتباط مباشر من جهاز لآخر، لكن ما نشهده في الثورة الصناعية الرابعة أمر مختلف تماما. أحد العناصر الرئيسية للثورة الحالية هو التواصل السلس والمتشعب الذي يسمح بحركة البيانات بين مختلف الأطراف والأجهزة بشكل سريع وفعال، الآن نحن نعيش في عالم مترابط لا سلكيا بشكل شبه تام، كل جهاز محمول أو هاتف ذكي مرتبط بشبكة الإنترنيت، بل وأصبحت الأجهزة الكهربائية التقليدية (مثل المصابيح وأجهزة المطبخ) متصلة بالشبكة العالمية، لتتمخض لنا تقنية انترنيت الأشياء (IOT) حيث يتوقع أن تصل الأشياء المرتبطة بالإنترنيت إلى 50 مليار جهاز بحلول عام 2030[7].

3.3.2 الأنظمة المادية السيبرانية

يمكن تصوير وتخيل هذه الأنظمة كجسور بين العالم الحقيقي الذي يعيش ويعمل فيه الإنسان والمعدات والأجهزة الكهربائية والعالم الافتراضي الذي أوجدته شبكات الاتصال ومستودعات البيانات

الهائلة، بعكس الآلات التقليدية التي تعمل بشكل مستقل عن محيطها، تدمج الأنظمة المادية السيبرانية القدرة على الاستشعار والحوسبة والتحكم وكذلك الاتصال الشبكي بالأجهزة والبنية التحية لتوصلها بشبكة الإنترنيت ويبعضها البعض وعلى سبيل المثال نجد الطائرات بدون طيار، السيارات ذاتية القيادة، الطابعات ثلاثية الأبعاد وغيرها[8].

هذه هي السمات التقنية للثورة الصناعية الرابعة التي ولدت تقنيات رقمية زعزعت كل القطاعات وكل الصناعات وأعادت تعريف نموذج الأعمال (Business Model) من جديد في إطار نظام بيئي (Ecosystem)، ويمكن توظيف هذه التقنيات الرقمية لضمان البقاء وتحقيق الاستدامة من خلال: [9]

الجدول رقم (01): توظيف التقنيات الرقمية

التقنية	لماذا؟ كيف؟
الحوسبة السحابية	للتطوير والتشغيل السريع للبرامج والخدمات التقنية، وخفض التكلفة ودعم إستمرارية الأعمال
إنترنيت الأشياء	لجمع البيانات والمراقبة عن بعد
البيانات الضخمة وتحليل البيانات	للتنبؤ وفهم أعمق للأعمال والعميل وأصحاب المصلحة
الذكاء الاصطناعي وتعلم الآلة والتعلم العميق	الابتكار وزيادة النمو وتحس ز ي تجربة المستخدم وكفاء التشغيل والتنبؤ واتخاذ القرار
تقنية البلوكشين	الأمان والحماية والخصوصية
تطبيقات الأجهزة الذكية	للوصول والنفاذ
الأمن السيبراني والخصوصية	للحماية المادية والمعلوماتية
روبوتات أتمتة العمليات	لترابط العمليات ودعم الأتمتة بين الأنظمة وميكنة الأعمال المكتبية وإستخراج التقارير
التواصل الإجتماعي	للتواصل مع أصحاب المصلحة والعملاء والتسويق والنفاذ

المصدر: عدنان مصطفى البار، القيادة الرقمية في عصر التحولات الرقمية الحكومية، معهد الإدارة العامة – منصة" إثرائي"، سبتمبر 2019، ص 34

هذه التقنيات على سبيل المثال لا الحصر تعتبر أهم تقنيات العقد القادم، يتوجب على المؤسسات والهيئات الانتباه لها ومواكبتها إن هي أرادت البقاء والتقدم في رحلة التحول الرقمي ومواكبة هذه الثورة الصناعية الرابعة.

وفيما يلي الشكل الموالي: [10]

الشكل رقم (05): إطار الثورة الصناعية الرابعة والتقنيات الرقمية المساهمة

المصدر: د. محمد مراياتي، الثورة الصناعية الرابعة آفاقها ومستلزمتها في الوطن العربي.متاح على الموقع: www.taqadom.aspdkw.com تاريخ الاطلاع: 2021/07/30 على الساعة 00:33

3.الأمن السيبراني

1.3 مفهوم الأمن السيبراني (Cybersecurity)

حسب التعريف الموسع للأمن السيبراني المعتمد لدى الإتحاد الدولي للاتصالات هو: " مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية والتقنيات التي يمكن استخدامها لحماية البيئة الإلكترونية وتنظيم أصول المستخدم، تشمل توصيل أجهزة الحوسبة والموظفين والبنية التحتية والخدمات ونظم الاتصالات السلكية و واللاسلكية ومجمل المعلومات المرسلة أو المخزنة في البيئة الإلكترونية"[11].

يُطلق عليه أيضاً" أمن المعلومات "و"أمن الحاسوب"، وهو فرع من فروع التكنولوجيا يُعنى بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية والتهديدات السيبرانية التي تهدف عادة للوصول إلى المعلومات الحساسة، أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل العمليات التجارية.

يعرّفه "إدوارد أموروسو (Edward Amoroso) "صاحب كتاب" الأمن السيبراني "الذي صدر عام 2007 بأنه "مجموع الوسائل التي من شأنها الحدّ من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات"، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات الرقمية ووقفها، وتوفير الاتصالات المشفرة[12].

يحتوي نهج الأمن السيبراني الناجح على طبقات متعددة من الحماية تنتشر عبر أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي يرغب المرء في الحفاظ عليها. بالنسبة للأشخاص والعمليات

والتكنولوجيا، يجب أن يكمل كل منها الآخر داخل المؤسسة لإنشاء دفاع فعال في مواجهة الهجمات السيبرانية يمكن لنظام إدارة التهديدات الموحد أتمتة عمليات التكامل على مستوى منتجات Cisco Security المحددة وتسريع وظائف عمليات الأمان الرئيسية: الاكتشاف والتحقيق والمعالجة[13].

- الأشخاص:

يجب على المستخدمين فهم المبادئ الأساسية لأمان البيانات والامتثال إليها مثل اختيار كلمات مرور قوية والحذر من المرفقات الموجودة ضمن البريد الإلكتروني والنسخ الاحتياطي للبيانات. تعرف على المزيد حول المبادئ الأساسية الأمن السيبراني[14].

- العمليات:

يجب أن تمتلك المؤسسات إطار عمل حول كيفية التعامل مع الهجمات السيبرانية غير المكتملة والناجحة. يمكن لـ إطار عمل واحد يحظى بقدر من الاحترام أن يرشد المؤسسات. يوضح كيفية تحديد الهجمات وحماية الأنظمة واكتشاف التهديدات والتصدي لها والتعافي من الهجمات الناجحة[15].

- التقنية:

توفير التكنولوجيا هو أمر ضروري لمنح المؤسسات والأفراد أدوات الأمن السيبراني اللازمة لحماية أنفسهم من الهجمات السيبرانية. يجب حماية ثلاثة كيانات رئيسية: الأجهزة الطرفية مثل أجهزة الكمبيوتر والأجهزة الذكية والموجّهات والشبكات والسحابة. تتضمن أشكال التكنولوجيا الشائعة المستخدمة لحماية هذه الكيانات، الجيل التالي من الجدران النارية وتصفية DNS والحماية ضد البرامج الضارة وبرامج مكافحة الفيروسات وحلول أمان البريد الإلكتروني[16].

يتبّع **الأمن السيبراني** نهجاً محدّداً يتكون عادة من عدّة طبقات للحماية تُثبَت في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المستخدم حمايتها. توجد العديد من المصطلحات المرتبطة بالأمن السيبراني نذكر منها:

1- الفضاء السيبراني (Cyberspace): عبارة عن بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية، مكوّنة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين. ويُطلق عليه "الذراع الرابعة للجيوش الحديثة".

2- الردع السيبراني (Cyber Deterrence): يعرّف على أنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي والأصول التي تدعم العمليات الفضائية.

3- الهجمات السيبرانية (Cyber Attaks): أيّ فعل يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض شخصي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام.

4- الجريمة السيبرانية (Cybercrime): مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية عبر شبكة الإنترنت، وتتطلب تحكماً خاصاً بتقنيات الكمبيوتر ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها[17].

2.3 أهمية الأمن السيبراني

في عالم اليوم المتصل، يستفيد الجميع من برامج الدفاع الإلكتروني المتقدمة. على المستوى الفردي، يمكن أن يُسفر هجوم الأمن الإلكتروني عن الكثير من الأشياء، بدءًا من سرقة الهوية ومرورًا بمحاولات الابتزاز ووصولًا إلى فقدان البيانات المهمة مثل صور العائلة. يعتمد الجميع على بنية أساسية حيوية مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية، وتأمين هذه المؤسسات وغيرها هو أمر ضروري للحفاظ على سير عمل المجتمع لدينا.

كما يستفيد الجميع من عمل الباحثين في مجال التهديدات السيبرانية، مثل فريق Talos المكون من 250 باحثًا، والذين يحققون في التهديدات الجديدة والناشئة وإستراتيجيات الهجوم السيبراني. وهم يعملون على كشف الثغرات الأمنية الجديدة وتثقيف الجمهور حول أهمية الأمن السيبراني ودعم الأدوات مفتوحة المصدر، تجعل جهودهم من الإنترنت مكانًا أكثر أمنًا للجميع[18].

تتبع أهمية الأمن السيبراني من ثلاثة محاور رئيسية هي[19]:

1. **السرية (Confidentiality)**: أي التحكم في الولوج إلى البيانات وإتاحتها لم يُسمح لهم فقط.
2. **السلامة (Integrity)**: الحفاظ على سلامة البيانات والمعلومات وحمايتها من الهجمات التخريبية أو السرقة.
3. **الجاهزية (Availability)**: جاهزية جميع الأنظمة والخدمات والمعلومات وإتاحتها حسب طلب الشركة أو عملائها.

3.3 فوائد الأمن السيبراني:

يمكن تلخيص أهم فوائد الأمن السيبراني فيما يلي:

1) حماية الشبكات والبيانات من الدخول غير المصرح به.
2) تحسين مستوى حماية المعلومات وضمان استمرارية الأعمال.
3) تعزيز ثقة المساهمين وأصحاب المصلحة في الشركة.
4) استرداد البيانات المُسربة في وقت أسرع في حالة حدوث خرق للنظام الأمني السيبراني[20].

4. التهديدات السيبرانية:

تعرف على أنها أيّ فعل يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض شخصي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام. هي استغلال الحاسبات وتكنولوجيا المعلومات في تخريب وتدمير البنية المعلوماتية للخصوم، بل وتعطيل شبكات الدفاع الجوي واختراق أنظمة المعلومات للبريد الإلكتروني لمكاتب رؤساء الدول والتجسس عليهم وفق خطة ممنهجة[21].

إذًا، التهديدات السيبرانية أو الهجمات السيبرانية هي التي تهدد أمن المجتمع وأمن الاقتصاد الوطني والجانب الأمني والعسكري للدول، كما أن للتهديدات السيبرانية أهداف مسطّرة، حيث تمس كلا من الجانب المعنوي والجانب المادي وعلى جميع الأصعدة[22]، لكن ما يتوجب على الدول المعرضة لتلك

التهديدات وضع خطط إستراتيجية من أجل مكافحتها والتخلص منها ويمكن التوضيح أكثر من خلال الجدول الآتي:

الجدول رقم (02): طرق استخدام التهديدات السيبرانية وكيفية التعامل معه

	الدفاع المجتمعي	الدفاع الاقتصادي السيبراني	الدفاع العسكري السيبراني
القيم المهددة	الدين – الشباب– التراث– الأخلاق	الجودة– السرعة– التنافسية – الاختراعات التنموية – المعاملات المالية – التطوير الاقتصادي	العقيدة العسكرية– ميزان الرعب – ثقة الشعب بالجيش والأمن
أهداف التهديدات السيبرانية	نشر الانحراف لتشكيل خلايا مشوشة للدولة– الحصول على معلومات من الأفراد– التحريض على العنف– تشكيك الشعب بقدراته	تدمير التنمية الاقتصادية الإلكترونية– سرقة الأموال – تدمير التجارة الإلكترونية – إيقاف التصدير الاستيراد – إلحاق الخسائر الاقتصادية	الحصول على معلومات تخص التسليح – التجسس على الاستخبارات– إمكانية إعادة توجيه القتال والصواريخ الذكية– التجسس على البيانات الرقمية
استراتيجيات الدفاع الوطني	توصية الهيئات الشخصية والأجهزة الأمنية المختصة الوطنية – توجيه وتركيز الدفاع الشعبي الكتروني والتخطيط له	ضرورة توعية الخبراء والمختصين بمخاطر التهديدات السيبرانية – الحرص على استمرار عدم انقطاع الاتصال بشبكة الانترنيت	الهجوم الإلكتروني المضاد– محاكاة عملية الاختراق الأمني العملياتي– ولاء مسؤولي الأجهزة الأمنية– تطوير ترسانة السلاح الرقمي
أدوات الدفاع السيبراني	الشبكات الاجتماعية الالكترونية – البريد الالكتروني– مواقع وسائل الإعلام – تقنيات الحماية الالكترونية	مواقع الحماية من الفيروسات – إدخال نشاط أمن المعلومات إلى الشركات– تحفيز مواقع الانترنيت الاحتياطية وتجهيز البريد الالكتروني	توفير برامج الحماية– تجهيز منشآت الهجوم الإلكتروني– توظيف الأنظمة الإلكترونية في الهجوم على مواقع العدو
المسؤول عن الدفاع	كل من لديهم القدرة على عمل السلاح الرقمي	مديرية المعلوماتية في المؤسسات	وحدات خاصة بتقييم إحداثيات داخل الجيش والمخابرات، تكون مهمتها الدفاع والهجوم

المصدر :أحمد السيد النجار، محمد عبد الهادي علام، حروب المعلومات :من يواجهها؟،

مجلة الأهرام، العدد 139 ، 13 (يوليو) 2015 ، ص. 26

1.4 أنماط التهديدات السيبرانية:

تتعدد أشكال التهديدات السيبرانية وتختلف من حيث الطبيعة والمصادر والأهداف كالتجسس وسرقة المعلومات وشن الحروب وبالتالي بات العديد من الفواعل الدوليين يلجئون إلى آليات إلكترونية لتحقيقها. وعلى الرغم من تعدد صور وأشكال الهجمات الإلكترونية، غير أنه من الممكن تقسيمها إلى المجموعات رئيسية التالية:

1.1.4 خطر الكوارث الطبيعية أو(العرضية للكابلات البحرية):

تعد الكبلات (Submarine Cable) جزءً هامًّا لتوفير خدمة الاتصالات بين دول العالم في مجال الإنترنت، وشبكات الكمبيوتر وغيرها، فمنذ عام 2005 أصبحت الكابلات البحرية مأهولة على مجال الاتساع والانتشار، أما على نطاق التقدم والتطور تحولت إلى تقنيات أخف وزنا وأصغر حجما، كما تعرضت تلك الكابلات إلى عدد من المشكلات التي تؤثر سبا على أعمال البنى التحتية بالضرر، حيث لا تقع في مياه المحيط العميق[23].

2.1.4 التجسس الإلكتروني (Cyber Espionage):

يعد أحد أنواع التجسس التقليدي، باستخدام وسائل التكنولوجيا الفائقة، ومعظم الهجمات السيبرانية المتطورة التي تقع ضمن هذه الفئة، حيث يتم الحصول على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضلية اقتصادية، أو إستراتيجية أو عسكرية [18] . فالتجسس السيبراني هو ذلك التجسس الذي يعتمد على استخدام التقنيات الإلكترونية في الحصول على معلومات، ويختلف التجسس السيبراني من حيث النوع، فهناك التجسس عن طريق الأفراد، ومن خلال الشبكات السلكية أو التجسس من خلال الأقمار الصناعية[24].

3.1.4 الجريمة السيبرانية (Cyber Crime):

تتكون الجريمة السيبرانية أو الافتراضية من مقطعين هما: الجريمة (crime) والسيبرانية (cyber) ويستخدم مصطلح السيبرانية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجية على القانون. والجرائم السيبرانية هي المخالفات التي ترتكب ضد الأفراد أو مجموعات من الأفراد بدافع الجريمة قصد إيذاء سمعة الضحية بأذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصال مثل(الإنترنت) كغرف الدردشة، البريد الإلكتروني والموبايل فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح الجريمة السيبرانية[25].

4.1.4 الإرهاب السيبراني (Cyber Terrorism):

المقصود بالإرهاب المعلومات أو الإرهاب السيبراني هو ذلك الاستخدام للموارد المعلوماتية، المتمثلة في الإعلام وأجهزة الحاسوب وشبكة الإنترنت والفضائيات من أجل أغراض التخويف أو الإرغام لأغراض

سياسية، أو الإقناع الفكري والتثقيف السلبي والعدواني[26]، ويرتبط الإرهاب المعلوماتي إلى حد كبير بالمستوى المتقدم للغاية والذي باتت تكنولوجيا المعلومات والإعلام تؤديه في جميع مجالات الحياة في العالم، ويمكن أن يتسبب الإرهاب المعلوماتي في إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو قطع شبكات الاتصالات بين الوحدات والقيادة المركزية وتعطيل أنظمة الدفاع الجوي وغيرها[27].

5.1.4 الحروب السيبرانية (Cyber Warfare)

تشمل الحروب السيبرانية الناجحة على أكثر من "مشغلي" الحروب الإلكترونية، وتعتمد على فريق من المختصين في المعارك الإلكترونية، حيث كل منهم يتميز بمسؤولياته ومهاراته الخاصة لترسيخ القدرة على القتال والتحكم بها وإبرازها ضمن الفضاء السيبراني، ويقوم مشغلو الحروب السيبرانية بالتخطيط للنشاطات الهجومية والدفاعية وإدارتها وتنفيذها عبر الفضاء السيبراني[28].

2.4 الأنواع الشائعة من الهجمات السيبرانية:

1.2.4البرامج الضارة:

البرامج الضارة هو مصطلح لوصف البرمجيات الخبيثة، بما في ذلك برامج التجسس spyware وبرامج الفدية الضارة والفيروسات وكذلك الفيروسات المتنقلة. تحاول البرامج الضارة اختراق الشبكة من خلال استغلال الثغرات الأمنية، ويتم ذلك عادةً عندما ينقر مستخدم ما على رابط خطير أو مرفق بريد إلكتروني يعمل على تثبيت البرامج الخطرة. وبمجرد الوصول إلى النظام، يمكن للبرامج الضارة تنفيذ الآتي:

- حجب الوصول إلى المكونات الرئيسية للشبكة (برامج الفدية الضارة).
- تثبيت البرامج الضارة أو غيرها من البرامج المؤذية.
- الحصول على المعلومات بشكل خفي من خلال نقل البيانات من محرك الأقراص الثابتة (برامج التجسس).
- تعطيل مكونات محددة وجعل النظام غير صالح للعمل[29].

2.2.4 تصيّد المعلومات:

تصيد المعلومات هو عملية إرسال أشكال احتيالية من الاتصالات التي قد تبدو أنها تأتي من مصدر موثوق، ويتم عادةً عبر البريد الإلكتروني. والهدف هو سرقة البيانات الحساسة مثل بيانات بطاقة الائتمان ومعلومات تسجيل الدخول أو تثبيت برامج ضارة على جهاز الضحية. تصيد المعلومات هو أحد أشكال التهديد السيبراني الشائعة بشكل متزايد[30].

3.2.4 هجوم الوسيط (Man-in-the-Middle):

تحدث هجمات الوسيط (MitM)، والمعروفة أيضًا بهجمات التنصت، عندما يُدخل المهاجمون أنفسهم ضمن معاملة ثنائية الأطراف. بمجرد أن يتمكن المهاجمون من اعتراض حركة مرور البيانات، يمكنهم حينها تصفية البيانات وسرقتها.

نقطتا دخول مشتركتان لهجمات:MitM

1- يمكن للمهاجمين التسلل بين جهاز الزائر والشبكة عند الاتصال بشبكة Wi-Fi عامة غير آمنة. ويعمل الزائر على تمرير جميع المعلومات إلى المهاجم دون أن يدرك ذلك.

2- بمجرد نجاح البرامج الضارة في اختراق الجهاز، يمكن للمهاجم تثبيت برامج لمعالجة جميع معلومات الضحية[31].

4.2.4 هجوم رفض الخدمة

يعمل هجوم رفض الخدمة على إغراق الأنظمة أو الخوادم أو الشبكات بسيل من حركة مرور البيانات لاستنفاد الموارد والنطاق الترددي. ونتيجة لذلك، يتعذر على النظام تنفيذ الطلبات المشروعة. كما يمكن للمهاجمين استخدام العديد من الأجهزة المخترقة لشن هذا الهجوم. ويُعرف هذا بهجوم رفض الخدمة الموزّع (DDoS)[32]

5.2.4 حقن (SQL)

يحدث حقن لغة الاستعلامات المركبة (SQL) عندما يُدرج المهاجم تعليمات برمجية ضارة إلى خادم يستخدم لغة SQL ويجبر الخادم على الكشف عن المعلومات التي لا يُظهرها في العادة. يمكن للمهاجم تنفيذ حقن SQL ببساطة عن طريق إرسال تعليمات برمجية ضارة إلى أحد مربعات البحث على الويب التي تحتوي على ثغرات أمنية[33].

6.2.4 الهجوم دون انتظار

يحدث الهجوم دون انتظار بعد اكتشاف وجود ثغرة أمنية بالشبكة ولكن قبل تنفيذ أحد التصحيحات أو الحلول. يستهدف المهاجمون الثغرات الأمنية التي تم الكشف عنها خلال هذه الفترة الزمنية الصغيرة. يتطلب اكتشاف الثغرات الأمنية التي تسهل الهجوم دون انتظار وجود وعي دائم[34].

7.2.4 الاتصال النفقي عبر DNS

تستخدم عملية الاتصال النفقي عبر DNS بروتوكول DNS لتوصيل حركة مرور البيانات غير التابعة لـ DNS عبر المنفذ 53. وتعمل على إرسال حركة مرور بروتوكول HTTP والبروتوكولات الأخرى عبر DNS توجد العديد من الأسباب المشروعة لاستخدام الاتصال النفقي عبر DNS ومع ذلك، توجد أيضًا أسباب ضارة لاستخدام خدمات VPN المستندة إلى الاتصال النفقي عبر .DNS يمكن استخدامها لتمويه حركة المرور الصادرة في صورة DNS مما يعمل على إخفاء البيانات التي تتم مشاركتها عادةً من خلال الاتصال بالإنترنت. أما بالنسبة للاستخدام الضار، فيتم التلاعب بطلبات DNS لنقل البيانات من النظام الذي تم اختراقه إلى البنية الأساسية للمهاجم. كما يمكن استخدامها في تمرير الأوامر إلى الاستدعاءات التي يتم إرسالها من جانب البنية الأساسية للمهاجم إلى النظام الذي تم اختراقه والتحكم بها[35].

5. خاتمة

إن التهديدات السيبرانية الناجمة عن تقنيات الثورة الصناعية الرابعة هي خطر آني ومستقبلي يهدد البشرية جمعاء ولم تسلم منه لا الدول الضعيفة ولا المتطورة، وبات خطراً مدمراً لمختلف القطاعات الحياتية الاقتصادية منها والاجتماعية والسياسية، وحتى الشخصية. وسيبقى الأمن السيبراني مشكلة عصية على الحل. حيث أن التهديدات الإلكترونية (السيبرانية) تشكل تحدياً مستحيلاً، فهي بطبيعتها سريعة التغير، ولا محدودة وغير متماثلة، ولذلك أصبح التنبؤ بها وإدارتها في غاية الصعوبة، حيث كشف استبيان عالمي حول كبار المدراء التنفيذيين وصناع القرار في مجال تكنولوجيا المعلومات (ITDMs) عن وجود فجوة كبيرة بين تقييمات التهديدات السيبرانية وتكاليفها ومجالات مسؤوليتها.

لذا وجب على الحكومات أن تتحمّل مسؤولية حماية المواطنين والمؤسسات من خطر التهديدات الرقمية، كما يجب على الشركات والموظفين توخي أقصى درجات الحذر من أجل حماية أنفسهم وحماية المعلومات السرية الخاصة بهم.

ومع استمرار جائحة فيروس كورونا (كوفيد 19) في جميع أنحاء العالم أصبحت التهديدات السيبرانية الناجمة عن التقنيات المزعزعة والناشئة عن الثورة الصناعية الرابعة ذات أهمية بالغة أكثر من أي وقت مضى.

التوصيات:

من خلال ما سبق نورد بعض التوصيات التي يمكن الاستفادة منها:

- الاستفادة من التجارب الناجحة التي احتضنت هذه الثورة الصناعية الرابعة وطريقة تعاملها مع تقنياتها المزعزعة؛
- ضخ مزيد من الاستثمارات في مجالات الأمن السيبراني؛
- إبرام الشراكات الدولية وتطوير العلاقات مع مراكز البحث والجامعات التي تهتم بالبحث في هذا القطاع.
- تقييم مخاطر التهديدات السيبرانية التي تتعرض لها مختلف الصناعات وقطاعات الأعمال؛
- إنشاء بيئات آمنة للبنية الأساسية لتقنية المعلومات وقواعد البيانات؛
- إجراء مراجعة منتظمة لتحديد الثغرات المحتملة و اتخاذ الإجراءات المناسبة؛
- وضع خريطة للتهديدات الناجمة من خلال تحديد جميع التقنيات الرقمية وكذا المخاطر الكامنة عنها.

6. قائمة المراجع:

[1] د. معاذ الدهيشي. (2019). ماهو التحول الرقمي؟ وكيف تحققه؟ دليل إرشادي للقادة الاداريين. الرياض، وحدة التحول الرقمي، المملكة العربية السعودية.

[2] نفس المرجع السابق، ص 2

[3] ابراهيم الكصب. (2019). آلية مبتكرة للإحاطة بنموذج الأعمال الخاص بالثورة الصناعية الرابعة. تم الاسترداد من: Harvard Business Review Arabia: https://hbrarabic.com

[4] لحسن حداد. (2017). كيف لريادة الأعمال أن تستفيد من الثورة الصناعية الرابعة؟ تم الاسترداد من: Harvard Business Review Arabia: https://hbrarabic.com

[5] د. معاذ الدهيشي، مرجع سبق ذكره، ص 9

[6] د. معاذ الدهيشي، مرجع سبق ذكره، ص 10

[7] د. معاذ الدهيشي، مرجع سبق ذكره، ص 10

[8] نفس المرجع السابق، ص 10

[9] د.عدنان مصطفى البار، القيادة الرقمية في عصر التحولات الرقمية الحكومية، معهد الإدارة العامة – منصة" إثرائي"، سبتمبر 2019، ص 34

[10] د. محمد مراياتي، الثورة الصناعية الرابعة آفاقها ومستلزمتها في الوطن العربي.متاح على الموقع: www.taqadom.aspdkw.com تاريخ الاطلاع: 2021/07/30

[11] الاتحاد الدولي للإتصالات. (2010)" الأمن السيبراني ". تم الاسترداد من: https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-ar.pdf

[12] هارفارد بزنس ريفيو.(2021). دليل مصطلحات هارفارد بزنس ريفيو، مفاهيم إدارية،(Cybersecurity)، تم الاسترداد من: Harvard Business Review Arabia: https://hbrarabic.com ، تاريخ اخر زيارة: 2021/12/05

[13] سيسكو Cisco. (2020)، كيف يعمل الأمن السيبراني؟، تم الاسترداد من: https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html#~how-cybersecurity-works ، تاريخ اخر زيارة: 2021/12/05

[14] سيسكو Cisco. (2020)، مرجع سبق ذكره، تم الاسترداد من:-https://www.cisco.com/c/ar_ae/products/security/what-is cybersecurity.html#~how-cybersecurity-works ، تاريخ اخر زيارة: 2021/12/05

[15] سيسكو Cisco. (2020)، مرجع سبق ذكره، تم الاسترداد من:-https://www.cisco.com/c/ar_ae/products/security/what-is cybersecurity.html#~how-cybersecurity-works ، تاريخ اخر زيارة: 2021/12/12

[16] سيسكو Cisco، نفس المرجع السابق

[17] هارفارد بزنس ريفيو.(2021). دليل مصطلحات هارفارد بزنس ريفيو، مفاهيم إدارية،(Cybersecurity)، تم الاسترداد من: Harvard Business Review Arabia: https://hbrarabic.com ، تاريخ اخر زيارة: 2021/11/29

[18] سيسكو Cisco، مرجع سبق ذكره، تم الاسترداد من:-https://www.cisco.com/c/ar_ae/products/security/what-is cybersecurity.html#~how-cybersecurity-works ، تاريخ اخر زيارة: 12/12/

[19] هارفارد بزنس ريفيو.(2021). دليل مصطلحات هارفارد بزنس ريفيو، مفاهيم إدارية،(Cybersecurity)، تم الاسترداد من: Harvard Business Review Arabia: https://hbrarabic.com ، تاريخ اخر زيارة: 2021/12/12

[20] هارفارد بزنس ريفيو، نفس المرجع السابق

[21] نانسي البنا، " الأمن السيبراني بيئة تكنولوجية أكثر امنا"، تم الإسترداد من: http//boutiqueceena325. ezez/rdoc329.eg ، تاريخ أخر زيارة: 2021/12/05

[22] حسن بن أحمد الشهري، " الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس "، مركز النور للأبحاث

الإلكترونية، (2010)، ص 11.

[23] ذياب موسى البداينة، " الجرائم الالكترونية :المفهوم والأسباب، ملتقى علمي حول :الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية "، كلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية، (2014)، ص 05.

[24] أمجد المنيف، " الإرهاب الالكتروني – معركة حديثة "، المجلة العربية العربية، العدد 07، (يوليو) 2015 ، ص 02.

[25] إدريس بن الطيب عطية، " الظاهرة الإرهابية في زمن ما بعد الحداثة، دراسة تحليلية في الأشكال والأساليب والإجراءات المضادة "، المجلة العربية للدراسات الأمنية والتدريب، المجلد 31 ، العدد63، الرياض، (2015)، ص ص 24 25.

[26] Timothy Franz.TheCyber Warfare professionnel Realization for Devloping the Next Generation. Summer 2011.p 04.

[27] عادل عبد الصادق، " أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي"، مجلة الاتجاهات النظرية، البنك العربي الافريقي، (14 ماي 2017)، ص 32.

[28] عزيز ملحم بربر، " أمن الشبكات والانترنت"، (جامعة نايف العربية للعلوم الأمنية، 2008)، ص 04.

[29] سيسكو Cisco. (2020)، ماهو الهجوم السيبراني؟، تم الاسترداد من:
https://www.cisco.com/c/ar_ae/products/security/common-cyberattacks.html، تاريخ اخر زيارة: 2021/12/05

[30] سيسكو Cisco. (2020)، نفس المرجع السابق

[31] سيسكو Cisco. (2020)، مرجع سبق ذكره، تم الاسترداد من: https://www.cisco.com/c/ar_ae/products/security/common-cyberattacks.html، تاريخ اخر زيارة: 2021/12/12

[32] سيسكو Cisco. (2020)، نفس المرجع السابق

[33] سيسكو Cisco. (2020)، نفس المرجع السابق

[34] سيسكو Cisco. (2020)، نفس المرجع السابق

[35] سيسكو Cisco. (2020)، ماهو الهجوم السيبراني؟، تم الاسترداد من:
https://www.cisco.com/c/ar_ae/products/security/common-cyberattacks.html، تاريخ اخر زيارة: 2021/12/12