PISSN : 2571-9904 - EISSN : 2602-7763

استراتيجيات الأمن السيبراني كتحدي للتحول الرقمي بالمنظمات الحكومية مع الإشارة لتجربة دولة الإمارات العربية المتحدة

Cybersecurity strategies as a challenge for digital transformation in government organizations

With reference to the experience of the United Arab Emirates

طواهير عبد الجليل.

جامعة قاصدي مرباح ورقلة -الجزائر touahir.abdeldjalil@gmail.com

تاريخ الاستلام: 09/ 01/ 2023 تاريخ القبول: 16/ 03/ 2023 تاريخ النشر: 31/ 03/ 2023

ملخص

تسعى الدراسة الى التعرف على استراتيجيات الأمن السيبراني بالنظر إلى خطورة التهديدات التي يمثلها انعدم الأمن الإلكتروني على الأفراد والمنظمات والدول و في ظل الحاجة المتزايدة لضرورة التحول الرقمي في خدمات المنظمات الحكومية، ؛ فقد أصبح الأمن السيبراني جزءاً لا يتجزأ من الأمن القومي للدول. ومن هذا المنطلق أولت دولة الإمارات اهتماماً كبيراً لهذا المجال، بل إنها أعطته أولوية قصوى في السنوات القليلة الماضية حيث تحاول الدراسة الوقوف على جوانب القوة في التجربة الإمارتية الناجحة استراتيجيا منها تبؤها مراتب أولى بالنسبة لمؤشر الأمن السيبراني وتوصلت الدراسة الى أن نجاح التجربة جاء نتيجة لتبني استراتيجية و خطوات مهمّة تهدف الى إيجاد بيئة سيبرانية آمنة وصلبة، مدعمة بمعايير وترسانة قانونية متطورة لمكافحة الجريمة الالكترونية من أجل ضمان تحول رقمي سلس.

الكلمات المفتاحية: أمن سيبراني،تحول رقمي، منظمات حكومية، امارات عربية متحدة، امن الكتروني

Abstract:

The study seeks to identify the importance of cybersecurity on a global level, given the seriousness of the threats posed by the lack of electronic security to individuals, organizations, and countries, and in light of the growing need for digital transformation in the services of government organizations; Therefore, cyber security has become an integral part of the national security of states. From this standpoint, the UAE has paid great attention to this field, and has even given it a top priority in the past few years.An abstract is a brief, comprehensive summary of the contents of the article It refers to the objective of the research, and the results reached in two paragraphs

The study concluded that the success of the experiment came as a result of adopting a strategy and important steps aimed at creating a safe and solid cyber environment, supported by advanced legal standards and arsenal to combat cybercrime in order to ensure a smooth digital transformation.

Keywords: *Cyber security, digital transformation, government organizations, United Arab Emirates, electronic security*

I. مقدمة

كلما كان التحول الرقمي متقدما في مراحله في بلد مّا، زاد تعرضه للتهديدات السيبرانية؛ ومن ثم فإن الدول ذات التحول الرقمي السريع والبنية التحتية المتقدمة، مثل دولة الإمارات العربية المتحدة، تحتاج بطبيعة الحال إلى إعطاء المزيد من الاهتمام لحماية الفضاء السيبراني، خاصة أن التحول الرقمي في الإمارات أصبح يشمل مختلف مناحي الحياة في المجتمع حيث أدى الاعتماد على التكنولوجيا ورقمنة الحياة بشكل كامل إلى ظهور بعض التهديدات السيبرانية التي تستهدف سلامة المجتمع الرقمي

حيث أدى تطور التكنولوجيا السريع إلى زيادة عدد الأجهزة المتصلة بشبكة الإنترنت، الذي وصل في عام 2021 إلى أكثر من 22 مليار جهاز؛ ما وفّر أرضية خصبة للجرائم الإلكترونية التي تتضمّن على سبيل المثال: الاحتيال، والنصب، والسرقة، والعمليات التي تهدف إلى جمع معلومات لدوافع سياسية أو لاستغلالها في التضليل وصولًا إلى استهداف المنشآت الحيوية وتعطيلها؛ ومن هنا يُعَدّ دور الأمن السيبراني محوريًّا بل حاسمًا؛ إذ يمنع أو -على الأقل- يحُدّ من خطر هذه الجرائم

هذا تتصدر دولة الإمارات دول المنطقة في مجال توظيف التقنيات الحديثة والذكاء الاصطناعي في مجال الأمن السيبراني، بفضل رؤية واستراتيجية الدولة على مستوى القطاعين الحكومي والخاص. وتشغل دولة الإمارات مكانة ريادية ضمن المراكز الخمسة الأولى على مؤشر الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة، بفضل بنيتها التحتية القوية المعنية بأمن البيانات، من خلال الهوية الرقمية الوطنية وبطاقة الهوية الإماراتية، أو نتيجة لتحسُّن مستويات الأمن السيبراني بفضل برامج مثل الشبكة الإلكترونية الاتحادية . الأمر الذي ، أدى إلى تسريع تبني الذكاء الاصطناعي في عمليات الأمن السيبراني خاصة مع اطلاقها لمبادرات تطوير الذكاء الاصطناعي في مجال الأمن السيبراني، كون أن استخدام العامل البشري في هذا المجال بطئ ومكلف. في ظل ارتفاع وتيرة الهجمات السيبرانية، ومحدودية سرعة الاستجابة من قبل الأطراف المعنية للتهديدات.

وبالإضافة إلى ما سبق، فقد أصبحت الهجمات الإلكترونية أيضاً تُستخدم في التنافس، وخاصة التنافس الاقتصادي بين الدول، بل ويمكن للنشاطات السيبرانية الخبيثة، وخاصة التي تهاجم البنى التحتية الحيوية للدول، أن تشعل فتيل النزاعات والحروب، ولاسيما في المناطق التي تعاني أصلاً التوتر، وهذا ما يشكل تهديداً للسلم والأمن الدوليين.

ولهذا كله يبدو من الطبيعي أن يُصبح الأمن السيبراني جزءاً لا يتجزأ من الأمن القومي للدول،عامة والتحول الرقمي بصفة خاصة وقد أدخلته بالفعل كثير من الدول في استراتيجياتها للأمن القومي.

من هنا تحاول الدراسة الإجابة على الإشكالية المتمثلة في

في ظل التحول الرقمي الذي تشهده الإمارات العربية المتحدة ماهي الاستراتيجيات المتبعة في مجال الأمن السيبراني باعتباره تحدٍ يواجه هذا التحول ؟

ومن أجل الإجابة على الإشكالية

مفهوم الأمن السيبراني وأهميته

يُعد مفهوم "الأمن السيبراني" حديثاً نسبياً، إذ ظهر في السياق الأمريكي في أواخر ثمانينيات القرن الماضي، لكنه لم يبدأ في الاستخدام والانتشار على نطاقٍ واسع إلا مع بداية العقد الأول من القرن الحالي، مع تزايد التطور التقني، وما رافقه من تزايد للمخاطر والتهديدات السيبرانية، بشكل باتت معه تشكل تهديداً للأمن لعالمي، (الكويتي، ترينذز للبحوث والاستشارات، 2022)

كما يُعرف الأمن السيبراني بأنه حماية الأنظمة والشبكات والبرامج والممتلكات والموقع الجغرافي من الهجمات الرقميةالتي تستهدف عادة الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين لها، ويطلق عليه أحياناً "أمن الحاسوب" أو "أمن المعلومات." (مفهوم الأمن السبراني ، بلا تاريخ)

توجد تعاريف متعددة للأمن السيبراني أو ما يسمى أيضًا "أمن تكنولوجيا المعلومات" أو "أمن المعلومات الإلكترونية"؛ ولكنها عمومًا تتفق في أنه ممارسة تتعلق بحماية أجهزة الحاسوب، والخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات من الاختراقات والسرقات. وينطبق استخدام الأمن السيبراني على فئات مختلفة منها أمن الشبكات؛ أي تأمين شبكات الكمبيوتر، سواء من المتطفّلين "الهاكرز" الذين يتلاعبون في السير الطبيعي لمنظومة الشبكات أو الأجهزة ويتحكمون فيها، أو من البرمجيات الخبيثة؛ وأمن التطبيقات الذي يركز على إبقاء البرامج والأجهزة محمية أو خالية من التهديدات. ويتعلق الأمن السيبراني كذلك بحماية أمن المعلومات وسلامة البيانات وخصوصيتها، سواء في التخزين أو أثناء عمليات النقل. (الحربي، 2021)

ويشمل الأمن التشغيلي العمليات والقرارات الخاصة بمعالجة أصول البيانات وحمايتها. ويحدد موضوع التعافي من الكوارث واستمرارية الأعمال كيفية استجابة الدولة أو الجهة أو المنظمة لحوادث الأمن السيبراني أو أي حدث آخر يتسبب في فقدان العمليات أو البيانات. وتُعَدّ توعية المستخدمين النهائيين (أي الأشخاص) بكيفية التعامل مع تهديدات الأمن السيبراني من الأمور المهمة التي يتعيَّن الاهتمام بها؛ إذ تُعَدّ أخطاء الأفراد من العوامل الأكثر تهديدًا للأمن السيبراني التي لا يمكن التنبؤ بها؛ إذ يستطيع أي شخص إدخال فيروس بالخطأ إلى نظام آمن إذا لم يتبع ممارسات أمان جيدة.

دواعي الاهتمام بالأمن السيبراني

ورغم أن الأمن السيبراني موجود منذ وجود الحاسوب نفسه، فقد بدأ هذا الموضوع يحظى باهتمام متزايدة وغير مسبوق على المستوى العالمي، وذلك بالنظر إلى:

أولاً، المخاطر التي تنطوي على التهديد الإلكتروني على مختلف نواحي الحياة (انواع الأمن السيبراني، بلا تاريخ)؛ حيث يمكن أن يتسبب في وقف قطاعات حيوية أو حتى تدميرها.

ثانياً، تنوع هذه التهديدات المتعلقة بالأمن السيبراني؛ حيث تشمل:

1. **الجرائم الإلكترونية**، التي تشمل قيام أفراد أو مجموعات باستهداف النظم الإلكترونية من أجل مكاسب مادية أو الحصول على فدية مالية أو لخلق اضطراب وخلل فيها. ووفقاً لتقرير صادر عن موقع متخصص في هذا المجال، فإن معدل تكلفة الجرائم الإلكترونية لأي منظمة زادت بنسبة 23% عن العام الماضي

   وقد تُكلف العالَم 10 تريليونات دولار سنوياً بحلول 2025 وفقاً لتقرير آخر
2. **الهجمات السيبرانية**، التي تهدف عادة إلى جمع معلومات لدوافع سياسية أو لاستغلالها في تضليل الناخبين مثلاً، كما حصل في الانتخابات الرئاسية في الولايات المتحدة عام 2016، حيث خلصت التحقيقات إلى أن دولاً تدخلت إلكترونياً للتأثير في توجهات الناخبين؛ ما ساهم بشكل أو بآخر في فوز أحد المرشحين وخسارة الآخر (ساعد، 2022)
3. **الإرهاب الإلكتروني**، الذي يهدف إلى تقويض النظم الإلكترونية بهدف إحداث الرعب أو الخوف، والذي قد يستخدمه أفراد أو جماعات إرهابية أيضاً.

باختصار، إن الأمن السيبراني مهم جداً، بل هو حيوي؛ لأنه يحمي الأفراد والشركات والمؤسسات من أي تهديد إلكتروني محتمل. فالتطور التكنولوجي الهائل ترك كثيراً من الناس والدول عرضة لهجمات إجرامية

سيبرانية؛ فمعدلات الجرائم الإلكترونية تزيد، ومن ثم فمن دون أمن سيبراني فإن الأفراد والشركات والمؤسسات، وكذلك الدول، قد تخسر المعلومات الحساسة والأموال وحتى السمعة والثقة.

أما أحدث التهديدات السيبرانية التي يحتاج الأفراد والمنظمات -على حد سواء- إلى الحماية منها، فهي: أولًا، البرامج الخبيثة التي تؤثر تأثيرًا خطِرًا في الحكومة والجمهور والبنية التحتية والشركات في جميع أنحاء العالم. ثانيًا، التحايل؛ إذ تُرتكَب كثير من الجرائم باستخدام مواقع معينة وعن طريق تطبيقات مختلفة منها تطبيقات "المواعدة"، وغرف الدردشة؛ وغير ذلك من التهديدات التي تصعب مواكبتها أو تجنبها أحيانًا. ولهذه التهديدات جميعها بالطبع تبعات خَطِرة اقتصاديًا واجتماعيًا وأمنيًا، (ادريس، 2019).

مهام الأمن السيبراني

ويضطلع الأمن السيبراني بمهام عدَّة ومتنوعة أهمها:

أولًا، حماية المستخدم وضمان أمن الأجهزة الإلكترونية؛ وذلك عبر بروتوكولات خاصة منها تشفير البريد الإلكتروني والملفات والبيانات المهمة الأخرى؛ ما يسهم ليس في حماية المعلومات أثناء النقل فقط، بل في حمايتها من الضياع أو السرقة أيضًا.

ثانيًا، حماية أنظمة أجهزة الكمبيوتر من الفيروسات التي تؤدي إلى مشكلات خَطِرة أحيانًا.

ثالثًا، الحدّ من الجرائم الإلكترونية التي تشهد تزايدًا كبيرًا، ولا سيَّما مع التطور التكنولوجي المتسارع، إلى جانب حماية المعلومات والبيانات الشخصية الحسّاسة من الاختراق والسرقة، وحماية المؤسّسات والشركات من هجمات البرمجيات الخبيثة التي تهدف إلى الاحتيال، والتصيّد، إضافة إلى منع وقوع محاولات الابتزاز.

رابعًا، منع استخدام المعلومات على نحو غير قانوني، والحيلولة دون إلحاق الأذى والضرر بالأفراد والكيانات.

خامسًا، المحافظة على سلامة المجتمع وأمنه بحماية معلوماته الخاصة في القطاعات كلها من دون استثناء، ولا سيَّما تلك المتعلقة بخدمات الرعاية الصحية، والتعليمية، والمالية، وخدمات الطاقة وغيرها. وثمَّة أهمية خاصة للأمن السيبراني في الاقتصاد، وخاصةً القطاع المالي؛ إذ يحمي المصارف والشركات من التهديدات التي قد تلحق الضرر بها وبعملائها؛ ما يؤدي إلى فقدان الثقة بها؛ ولذا فالأمن السيبراني ركيزة أساسية لمنع الخسائر المالية التي قد تصيب المصارف والشركات وغيرها من المؤسسات المالية؛ نتيجة تعرض بيانات عملائها لهجمات بهدف السرقة أو التلاعب. (ادريس، 2019).

سادسًا، الإسهام في تعزيز الأمن القومي مع تزايد اعتماد الدول على "الرقمنة" في مجالات محورية، مثل القطاع العسكري، سواء فيما يخص المعلومات، أو الأسلحة التي أصبح بعضها موجهًا، بل يحتاج استخدامه إلى برمجيات خاصة، ومن ثَم فإن الأمن السيبراني ضروري لحماية الأمن القومي للدول، بل أصبح جزءًا لا يتجزأ منه؛ ليس لدوره في حماية المعلومات والأسرار العسكرية فحسب، وإنما حماية مختلف القطاعات الحيوية من الهجمات الإلكترونية، وحفظ بياناتها، وضمان استمراريتها وتطورها.

التوجهات العالمية والاقليمية تجاه الأمن السيبراني

يتطور التهديد السيبراني على مستوى العالم بوتيرة سريعة مع تزايد عدد انتهاكات البيانات في كل عام؛ إذ كشف تقرير صادر عن مؤسسة (RiskBased Security)، الرائدة في مجال استكشاف نقاط الضعف وبيانات الاختراق وتصنيف المخاطر، عن تعرض 22 مليار سجل لانتهاكات البيانات في عام 2021. ويزيد هذا الرقم على ضعفَي ما كان عليه الأمر في عام 2019؛ إذ تعرض 7.9 مليار سجل لانتهاكات البيانات في الأشهر

التسعة الأولى فقط. وشهدت الخدمات الطبية وتجارة التجزئة والهيئات العامة أكبر عدد من الانتهاكات؛ نظرًا إلى أن هذه القطاعات تُعَدّ أكثر جذبًا لمجرمي الإنترنت؛ لكونها تتضمن بيانات مالية وطبية مهمة.

ومع استمرار تزايد حجم التهديد السيبراني تتوقع مؤسسة البيانات الدولية (International Data Corporation) وصل الإنفاق العالمي على حلول الأمن السيبراني إلى 133.7 مليار دولار في هذا العام (2022). وقد استجابت الحكومات في جميع أنحاء العالم للتهديد السيبراني المتزايد؛ وفي نهاية عام 2020 اعتمد ما يقرب من 64 في المئة من دول العالم استراتيجية وطنية للأمن السيبراني، كما نفَّذ أكثر من 70 في المئة منها حملات للتوعية بالأمن السيبراني، مقارنةً بـ58 في المئة عام 2018 وفقًا للبيانات المتاحة.

وقد ظهر مايعرف مؤشر الأمن السيبراني" يصدر عن الاتحاد الدولي للاتصالات التابع رسمياً للأمم المتحدة، ويرصد المؤشر التحسن في مستويات الوعي بأهمية الأمن السيبراني، والتدابير المتخذة لحمايته في 193 دولة من دول العالم استناداً إلى عدة مقومات عبر خمسة أركان رئيسية؛ وهي :التدابير القانونية، والتدابير التنظيمية، والتدابير التقنية، والتدابير الرامية إلى تعزيز القدرات في مجال حماية الأمن السيبراني، وأخيراً التدابير التي تهدف إلى تعزيز التعاون في هذا الشأن.

كما صنّف المؤشر العالمي للأمن السيبراني "جي سي آي (GSI) "الذي أصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة لعام 2021 أربع دول عربية فقط في المستوى المرتفع. وتصدرت دول السعودية وقطر والإمارات والبحرين وعُمان الجهود في تحقيق الأمن السيبراني عربيا وعالميا، في حين وقعت باقي الدول في مرتبة متوسطة عالميا، أو تذيلت القائمة وفق المؤشر الذي شمل 175 دولة وقاس مدى التزام البلدان في مجال الأمن السيبراني وفقا للدعائم الخمس للبرنامج العالمي للأمن السيبراني وهي التدابير القانونية والتقنية والتنظيمية وبناء القدرات والتعاون ومدى وجود إستراتيجيات وسياسات للأمن السيبراني، ومدى وجود خطط ومعايير وطنية يتم تنفيذها على أرض الواقع مثل توافر التدريب والتأهيل للكوادر في مجال الأمن السيبراني والجهود والمبادرات المبذولة في هذا الشأن، كما يشير إلى أحد أهم العوامل، وهو وجود بنية تشريعية وقانونية تدعم الأمن السيبراني.

من المعروف أن مجرمي وقراصنة الإنترنت يشكلون خطرًا على أي شخص لديه إمكانية الوصول إلى الشبكة العنكبوتية، ومع ذلك، فإنّ البعض أكثرا ستعدادًا لمكافحة الجريمة عبر الإنترنت من غيرهم.

العناصر أو المعايير أعلاه هي التي تحكم الاتحاد الدولي للاتصالات أثناء تقييم الدول وفقًا لمؤشر الأمن السيبراني. ومما يلاحظ وجود فجوات كبيرة في قدرات توفير وإتاحة الأمن السيبراني على مستوى العالم، إذ تمتلك مثلا الولايات المتحدة الأميركية والمملكة المتحدة بنى تحتية مغايرة تماما من حيث القدرة والكفاءة عن تلك الموجودة في دول مثل العراق وجيبوتي وبوروندي.

ومع ذلك، أظهرت دول مجلس التعاون الخليجي في هذا المؤشر أنها تفوقت بشكل جماعي على العديد من الدول الغربية الأخرى والبلدان الأكثر تقدما اقتصاديا من حيث قدراتها الأمنية السيبرانية واستدامة البنى التحتية البشرية وغيرها، بالإضافة إلى التدابير التعاونية لخلق بيئة تقنية آمنة.

يخلص المؤشر إلى تحذير مفاده أن "الأمن السيبراني يتطور باستمرار"، وستكون هناك حاجة إلى نُهج مستدامة ومطورة من قبل البلدان لضمان أن تظل كافة البرامج والحلول الرقمية آمنة وموثوقة وجديرة بالثقة، وأيضًا لعل "أحد الدروس المستفادة من أزمة وباء كورونا هو أن المشكلات الجماعية المرتبطة بتوفير الخدمات الصحية أو الأمن السيبراني تحتاج إلى معالجتها من خلال نهج تقنية متعددة شاملة تعمل على صياغتها البلدان المتقدمة والماهرة في إتقان آليات ومتطلبات الأمن السيبراني."

من المعروف أن مجرمي وقراصنة الإنترنت يشكلون خطرًا على أي شخص لديه إمكانية الوصول إلى الشبكة العنكبوتية، ومع ذلك، فإنّ البعض أكثرا ستعدادًا لمكافحة الجريمة عبر الإنترنت من غيرهم.

في الأشهر الستة الماضية فقط، زادت الهجمات الإلكترونية عالميا بنسبة 29%مع استمرار استغلال الجهات الفاعلة في التهديد لوباء كوفيد-19 حيث دخلت المجموعات التي تستخدم تكتيكات برامج الفدية عصرًا ذهبيًا، مع تزايد استخدام الابتزاز بوتيرة متسارعة بلغت ما يزيد عن 90% في أقل من عام.

ومع ذلك، فإن الدول القومية بدت وكأنها لا تقف مكتوفة الأيدي. إذ بدأت جهود للعديد من الأطراف الدولية في دفع بعض عصابات برامج الفدية إلى وضع عدم الاتصال بالإنترنت، بينما تعمل برامج الأمن السيبراني على تمكين الشركات والمؤسسات من مواجهة التهديدات التي تلوح في الأفق على الجانب المظلم للإنترنت.

في لغة الأرقام، بلغت قيمة سوق الأمن السيبراني العالمي 156.24 مليار دولار في عام 2020، ومن المتوقع أن تبلغ قيمة هذا السوق حوالي 352.25 مليار دولار، بمعدل نمو سنوي 14.5% بحلول عام 2026، حسب مؤسسة "موردر إنتيلجنس ."ومن المتوقع أن تصل قيمة سوق الأمن السيبراني العالمي 433.6 مليار دولار بحلول عام 2030، وتتوقع دراسات أن تكلف الجرائم الإلكترونية العالم ما يقرب من 600 مليار دولار كل عام.ومما يلفت الانتباه أن الإنفاق العالمي على المنتجات الأمنية بلغ 125.2 مليار دولار في عام 2020، مسجلاً زيادة بنسبة 6% عن عام 2019، ومن المقرر أن يبلغ الإنفاق العالمي على المنتجات والخدمات الأمنية 174.7 مليار دولار بحلول عام 2024، بمعدل نمو سنوي مركب قدره 8.1% من 2020 إلى 2024. مع العلم أن القطاعات الثلاثة الأكثر إنفاقًا على الأمن السيبراني هي البنوك والتصنيع والحكومة الفدرالية/المركزية.

كما بلغت قيمة سوق التأمين الإلكتروني العالمي 7.7 مليارات دولار أميركي في عام 2020، ومن المتوقع أن ينمو إلى 20.4 مليار دولار بحلول عام 2025 بمعدل نمو سنوي مركب قدره 21.2%. وتعتبر برامج الفدية نموذج الجرائم الإلكترونية المفضلة المتسللين والأسرع نموًا ، ومن المتوقع أن تكون الأضرار أعلى بعشرات المرات في السنوات القليلة القادمة، إذ بلغت تكلفة أضرار برامج الفدية في عام 2021 حوالي 20 مليار دولار، بحيث زادت 57 مرة عن التكلفة في عام 2015.

إلى جانب تهديدات القرصنة الأخرى، ستستمر أنشطة برامج الفدية في كونها مشكلة كبيرة للمنظمات في جميع أنحاء العالم. يعد تدريب المستخدمين على الطرق المناسبة لاكتشاف هذه التهديدات والرد عليها واستخدام حلول إدارة بريد إلكتروني قوية وآمنة من وسائل ردع برامج الفدية الفعالة (محمود، 2022)

أهم القطاعات المستهدفة

يأتي قطاع الرعاية الصحية يأتي على رأس القطاعات التي تعرضت للهجمات السيبرانية من خلال هجمات برامج الفدية، خاصة اثناء جائحة كوفيد19 خصوصا أن مرتكبي الهجمات الإلكترونية كانوا يعتقدون أن المؤسسات الصحية ستضطر إلى دفع الأموال "الفدية" لاستعادة أنظمتها التي تعتمد عليها في مواجهة انتشار الفيروس.حيث أن أعداداً كبيرة من المخترقين يستغلون أزمة الفيروس لبيع الأدوات الطبية المزيفة، وانتحال شخصيات لمسؤولين حكوميين ونشر ادعاءات بالتوصل إلى علاجات جديدة للفيروس والترويج لمنتجات طبية وهمية بملايين الدولارات.وكان القطاع المالي والنفطي في المرتبة الثانية للأهداف المفضلة للمخترقين، وأشار التقرير إلى تحذير المصارف المركزية من المحتالين الذين يسعون لاختراق الحسابات المصرفية، فيما يعد قطاع النفط من الأكثر تأثراً في منطقة الشرق الأوسط وشمال إفريقيا، إذ تعرضت شركاتٌ عديدة لرسائل بريد إلكتروني مخادعة، بهدف الحصول على تفاصيل ومعلومات عن الأفراد وعمليات إنتاج النفط، كما تعد منصات مؤتمرات الفيديو من أهم الأهداف المفضلة للمخترقين، إذ ظهرت فيها بعض

الثغرات الأمنية، مثل منصة "زوم" التي شهدت انضمام بعض الأشخاص عشوائياً إلى اجتماعات الفيديو وتعطيله بمحتوى غير مرغوب به، أو نشر فيديوهات مسجلة لم يتم حفظها في مساحات تخزين سحابية آمنة، وتم نشرها بعد ذلك على شبكة الإنترنت وشمل ذلك اجتماعات عمل خاصة، ومحادثات شخصية بين عائلاتٍ وأصدقاء، وتعرضت أيضاً منصاتٌ أخرى مثل منصات الألعاب عبر الإنترنت إلى هجماتٍ سيبرانية بهدف اختراق شبكة "نينتندو" للحصول على معلومات مالية شخصية.

أهمية المؤشر لدولة الإمارات

حققت دولة الإمارات العربية المتحدة إنجازاً جديداً تجسد هذه المرة في مجال الأمن السيبراني، حيث تبوأت مؤخراً المركز الخامس عالمياً في "مؤشر الأمن السيبراني"، (GCI)الصادر عن الاتحاد الدولي للاتصالات، التابع للأمم المتحدة، مسجلة بذلك قفزة هائلة في تصنيفها على إصدار 2020 من المؤشر، بالمقارنة مع إصدار 2019، التي نالت فيه المركز الـ 33، ومتفوقة على دول كبرى منها اليابان وكندا وفرنسا والهند .ويأتي هذا بعد أن حققت الدولة من قبل المركز الأول عالمياً في مؤشر الأمن السيبراني وفق تقرير الكتاب السنوي للتنافسية العالمية؛ ما يعد إنجازاً كبيراً بكل المقاييس، وخاصة أن الأمن السيبراني أصبح يحظى باهتمام عالمي، ويدخل ضمن استراتيجيات الأمن القومي.

حيث أعلنت دولة الإمارات عام 2021 عن معايير الأمن السيبراني الخاصة بالمؤسسات الحكومية، وخصصت لها أكبر ميزانية من نوعها في منطقة الخليج .(ابوغزالة، 2021)

وهذا الإنجاز ما كان ليتحقق لولا الجهود الكبيرة التي بذلت على مستويات مختلفة خلال السنوات القليلة الماضية، حيث تبنت الدولة عدداً من الاستراتيجيات المهمة والمبادرات الفعالة التي أسهمت بشكل أساسي في تحقيق هذا الإنجاز. (العربي، 2022)

نما حجم الإنفاق على برمجيات أمن المعلومات في دولة الإمارات العربية المتحدة خلال العام الجاري بنحو 13.4 % إلى مليار درهم (277.5 مليون دولار) سنة 2022 مقارنة بسنة 2021، حسب بيانات مؤسسة «أي دي سي» لأبحاث التكنولوجيا والاتصالات. (العربي، 2022)

.

لاشك في أن هذا الإنجاز ينطوي على دلائل مهمة كبيرة؛ فهو أولاً، وقبل كل شيء، يُضاف إلى سلسلة من إنجازات الدولة الحافلة ليس فقط في مجال الأمن السيبراني، بل أيضاً في مختلف المجالات من دون استثناء، حيث استطاعت أن تحتل المركز الأول عالمياً في 121 مؤشراً، والمركز الأول عربياً في 479 مؤشراً، فضلاً عن مجموعة كبيرة من المنجزات التي يصعب حصرها هنا.

أما في المجال السيبراني تحديداً، فهذا الإنجاز يُضاف إلى مجموعة من الإنجازات المهمة في هذا المجال؛ حيث تم إنشاء مجلس الأمن السيبراني، وتنفيذ شبكة إلكترونية اتحادية، وإنشاء السحابة الوطنية، وإطلاق مبادرات في السلامة الإلكترونية لكل فئات المجتمع، بما فيهم الأطفال، وإصدار شهادة المواطنة الرقمية، وإطلاق استراتيجيات الأمن السيبراني والإلكتروني، وغيرها من الإنجازات التي تؤكد ريادة الدولة في هذا المجال وقدرتها على تحقيق الكثير من الإنجازات، بل وتكون نموذجاً وقدوة لغيرها من دول المنطقة والعالم.

التجربة الإمارتية في إنجاح استراتيجية الأمن السيبراني

ما وصلت إليه دولة الإمارات من مراكز متقدمة في مجال الأمن السيبراني لم يأتِ من فراغ، ولم يكن بالطبع وليد الصدفة؛ وإنما هو في الحقيقة ثمرة لجهود كبيرة ولاستراتيجيات ومبادرات أثبتت فاعليتها حيث أحدثت بيئة عمل ذكية متكاملة تتمتع بالأمن والأمان، وهو ما ساعد على تعزيز أداء مختلف القطاعات،

ودفعها لتحقيق المزيد من التقدم، بما ينعكس إيجابياً على رخاء الإمارات وشعبها ويرسخ مكانتها العالمية في مجال الأمن السيبراني.، وفيما يلي أهمها:

أولاً، الاستراتيجية الوطنية للأمن السيبراني :أطلقت الدولة الاستراتيجية الوطنية للأمن السيبراني بهدف خلق بيئة سيبرانية آمنة وصلبة تساعد على تمكين الأفراد من تحقيق طموحاتهم، وتمكين الشركات أيضاً من التطور والنمو في بيئة آمنة ومستقرة ومزدهرة؛ وذلك من خلال تنفيذ 60 مبادرة ضمن خمسة محاور هي:

1. تصميم وتنفيذ إطار قانوني وتنظيمي شامل للأمن السيبراني لمعالجة جميع أنواع الجرائم السيبرانية، وبناء إطار تنظيمي لحماية التقنيات الحالية والناشئة، ووضع أنظمة داعمة لتمكين الشركات الصغيرة والمتوسطة وحمايتها من التهديدات السيبرانية.
2. تمكين منظومة حيوية للأمن السيبراني من خلال الاستفادة من سوق الأمن السيبراني في الدولة والمشاركة بفاعلية في سوق الأمن السيبراني في منطقة الشرق الأوسط وشمال أفريقيا، وتطوير قدرات أكثر من 40 ألف متخصص في الأمن السيبراني، وزيادة وعي أفراد المجتمع بالأمن السيبراني والمخاطر المتعلقة بالإنترنت، وتشجيع اتباع الممارسات الآمنة في التعامل مع التقنية، ومكافأة التميز في مجال الأمن السيبراني من خلال برامج الجوائز الوطنية، وتشجيع المؤسسات على إطلاق برامج حول الأمن السيبراني، وإلهام رواد الأعمال بالابتكار في مجالاتهم، ودعم الدراسات والأبحاث الخلاقة في المؤسسات الأكاديمية المختلفة في الدولة.
3. وضع خطة وطنية فعالة للتعامل مع الحوادث السيبرانية، لتمكين الاستجابة السريعة والفعالة على مستوى الدولة.
4. حماية الأصول الحيوية لدولة الإمارات في القطاعات الرئيسية.
5. دعم عمل منظومة الأمن السيبراني بأكملها من خلال شراكات محلية وعالمية، تسهم في تحقيق أهداف الدولة وطموحاتها في الأمن السيبراني.

ويجري تنفيذ هذه الاستراتيجية والمبادرات التي تضمنتها على مدار ثلاثة أعوام؛ ويتم تقييم نتائجها وتطويرها وفقاً لمتغيرات الأمن السيبراني عالمياً، وقد تم بالفعل هذا التطوير مؤخراً بناء على تحليل أكثر من 50 مصدراً من المؤشرات والمنشورات العالمية، والعمل مع فريق من الخبراء العالميين، وإجراء مقارنة معيارية مع عشرة دول رائدة في مجال أنظمة الأمن السيبراني؛ ولاشك في أن هذه الاستراتيجية، برغم أن مراحل تنفيذها لم تكتمل بعد، قد حققت العديد من أهدافها، حيث تبرز انعكاساتها على مختلف شرائح المجتمع، من خلال تعزيزها لثقة المواطنين والمقيمين في المشاركة بشكل آمن في العالم الرقمي، ودورها أيضاً في تعزيز الابتكار في هذا المجال، وترسيخ ثقافة الاستثمار فيه، فضلاً عن تمكين الشركات الصغيرة والمتوسطة من حماية نفسها ضد الهجمات السيبرانية.

ثانياً، مجلس الأمن السيبراني :اعتمد مجلس الوزراء مجلس الأمن السيبراني في نوفمبر 2020، حيث يضم في عضويته عدداً من الجهات الاتحادية والمحلية في الدولة، بهدف تطوير استراتيجية وطنية للأمن السيبراني وتعزيزه في القطاعات الحيوية كافة. ويختص المجلس ضمن مهامه باقتراح وإعداد التشريعات والسياسات، والمعايير اللازمة لتعزيز الأمن السيبراني للقطاعات المستهدفة في الدولة كافة، ووضع الآلية والإطار العام لتبادل ومشاركة وحوكمة المعلومات المرتبطة بالأمن السيبراني بين الجهات والقطاعات المختلفة محلياً ودولياً، وذلك بالتنسيق والتعاون مع الجهات المعنية.

ثالثاً، إطلاق مبادرات وحملات متنوعة :

علاوة على ما سبق، اتخذت الدولة العديد من الإجراءات والتدابير والمبادرات لتعزيز أمنها السيبراني وتتضمن: تنفيذ شبكة اتحادية معززة ببنية تحتية مشتركة تسمح بالتوصيل البيني، وتبادل البيانات بين جميع الجهات المحلية والاتحادية في الدولة، وتعزز قنوات التواصل فيما بينها باستخدام بنية تكنولوجية موحدة وآمنة؛ وتأسيس مركز الاستجابة الوطني لطوارئ الحاسب الآلي، بهدف تحسين معايير أمن المعلومات وممارساته، وحماية البنى التحتية لقطاع الاتصالات وتقنية المعلومات من مخاطر واختراقات الإنترنت؛ وتعزيز قانون مكافحة جرائم تقنية المعلومات والمساعدة في استحداث قوانين جديدة حول أمن المعلومات كما أطلقت العديد من المبادرات المهمة في السلامة الإلكترونية؛ ومنها على سبيل المثال: مبادرة موقع سالم للتوعية الإلكترونية (علي، 2022)لغرض توفير بيئة إلكترونية آمنة، لجميع مستخدمي الإنترنت، والجيل الصاعد على وجه الخصوص، وسفراء الإمارات للأمن الإلكتروني، والتي تهدف إلى تدريب نخبة من الطلبة في الدولة كسفراء في تعزيز ونشر الوعي الأمني الإلكتروني في جميع أنحاء دولة الإمارات، وحملة الابتزاز الإلكتروني التي تستهدف حماية المتضررين من الابتزاز، وملاحقة المبتزين في هذه القضايا في دول العالم كافة، وتُصدِر في حقهم نشرة طلب للإنتربول الدولي، وغيرها من المبادرات التي عززت من مستوى الأمن السيبراني في الدولة، وجعلتها من أكثر دول العالم أماناً.

رابعا مبادرة «النبض السيبراني

تبنى مجلس الأمن السيبراني لحكومة الإمارات، مبادرة «النبض السيبراني«Cyber Pulse ، التي تأتي لمراكمة الجهود التي باشرتها دولة الإمارات في مجال السلامة السيبرانية. وتهدف المبادرة إلى ضمان تحولٍ رقمي آمن، يمكن جميع الأفراد والقطاعات في الدولة من استخدام منجزات التكنولوجيا الرقمية في بيئةٍ أقل تهديداً، ويسهم في تحقيق أهداف الدولة في التنمية المستدامة. وفي تقديري أن هذه المبادرة مبتكرة، قدر ابتكار مسماها، حيث يسعى أصحابها إلى تحويل قضية الأمن السيبراني إلى همٍ مجتمعي مشترك ودائم، يتتابع الإحساس به ويتجدد الشعور بأهميته مع كل نبضٍ يصدر عن أفراد المجتمع، مواطنين ومقيمين، نساءً ورجالاً، شيبة وكهولاً وشباباً وناشئةٍ. وذلك أنّ أول ما تريد المبادرة غرسه هو أنّ تأمين الفضاء الإلكتروني لدولة الإمارات هو مسؤولية هؤلاء جميعاً، فالفرد والمجتمع هما حائط الدفاع الأول ضد أية تهديدات سيبرانية على الدولة ومؤسساتها والمجتمع وبنيته المعلوماتية الأساسية، سواء اتخذت صورة الجرائم الإلكترونية أو الإرهاب والتجسس السيبراني أو الحروب المعلوماتية.

وتتضمن المبادرة ورش عمل وبرامج تدريب على حوادث أمن المعلومات، وكيفية التعامل مع مراكز إدارة أمن المعلومات، ومحاكاة الهجمات الإلكترونية، موجهة لقطاعات الدولة جميعها وشرائح المجتمع كلها، ولا سيما السيدات والطلاب في مراحل التعليم العام والجامعي المختلفة. ويبتغي مجلس الأمن السيبراني إلى إعداد جيل من فرق العمل الإماراتية يمتلك أعلى مستوى من التدريب والتأهيل في مجال أمن المعلومات.

وقد تم إطلاق أولى مراحل المبادرة في يونيو 2022، بالتعاون مع الاتحاد النسائي العام، وحملت اسم «مبادرة النبض السيبراني للمرأة»، حيث تم تنظيم ورشة تدريبية لـ50 منتسبة لتأهيلهن بالخبرات والمعارف المتطورة بمجال الأمن السيبراني. وتمثل الغرض من هذه الورشة، التي يتلوها ورشات، أن تكون كل متدربة قناة تبث التوعية السيبرانية في أكبر عدد ممكن من أفراد المجتمع، وتصبح مدربة لطائفةٍ أخرى من المنتسبات. ومع استمرار التدريب وتواتر التوعية، تمتد مظلة الأمن السيبراني إلى كل شرائح المجتمع، ومناطقه.

ثم أعلن مجلس الأمن السيبراني، بالتعاون مع كليات التقنية العليا ومجموعة من الجامعات في الدولة، مبادرة «النبض السيبراني للطلبة»، التي يبدأ تنفيذها مع بداية العام الدراسي الجديد، وذلك. وتستهدف المبادرة الجديدة تأهيل 3000 طالب وطالبة في المرحلة الجامعية من تخصصات أمن المعلومات أو تقنية المعلومات للقيام بأدوار رئيسية في مجال الأمن السيبراني لمؤسسات الدولة.

وبصفة عامة، وفي سعيه لتنفيذ مبادرته المبتكرة على نطاقٍ واسع، يعمد مجلس الأمن السيبراني إلى تطبيقها عبر ثلاثة محاور، هي المحور الإعلامي والمحور التعليمي ومحور القطاع الخاص. يغطي المحور الأول وسائل الإعلام المختلفة التقليدية منها والجديدة، والإدارات الإعلامية في مراكز البحوث والدراسات. أما المحور التعليمي، فيستهدف تضمين التوعية السيبرانية في المناهج التعليمية وتدريب الطلاب. ويركز محور القطاع الخاص على استهداف الشركات الخاصة والمؤسسات الاقتصادية المختلفة في الدولة. الاتحاد (الأحبابي، 2022)

خامسا مبادرة « الولاء الوطني السيبراني.

«الولاء الوطني السيبراني»، يُقصد به أن يعكس التحول الرقمي وتوظيف التكنولوجيا الحديثة مجموعة من القيم والعادات والتقاليد الوطنية، ترسخ الولاء للوطن وقيادته السياسية.

ومن ثم، يجاهد أصحاب المبادرة، عن طريق سلسلة متواصلة من البرامج التدريبية لقطاعات الدولة المختلفة ولشرائح المجتمع المتباينة، إلى نشر التوعية الرقمية بين أعضاء المجتمع. وهي، بهذا المعنى، مبادرة وطنية شاملة. وعن طريق تعزيز ثقافة المسؤولية المجتمعية من خلال تأمين الفضاء الإلكتروني للدولة

كون هذا الأخير جزءاً لا يتجزء من إقليم الدولة، يجب أن تظلله سيادتها. كما أن قيمة الولاء تلك لا تقتصر فقط على المواطنين دون غيرهم، بل تنسحب على جميع أفراد المجتمع، مواطنين ومقيمين، وتتضمن أن يحرص كلٌ على تأمين نفسه بنفسه ومد مظلة الأمان إلى أفراد أسرته وجماعات الأصدقاء وزملاء العمل وهكذا... فهذا هذا الولاء يُتحصل عن طريق تطبيق المبادرة على نطاقٍ واسع في المجتمع، لإشراك أفراد المجتمع في تأمين أنفسهم والآخرين، وتأمين مجتمعهم وفضائهم السيبراني، وحماية مقدرات الدولة وبنيتها الحيوية.

سادسا، التعاون على المستوى الدولي :

وفي الوقت الذي عملت فيه دولة الإمارات على إنشاء بنية تحتية وآليات فعالة لتعزيز قدراتها في مجال الأمن السيبراني وحماية نفسها من التهديدات الإلكترونية، فإنها حرصت كذلك على العمل والتعاون مع الدول الأخرى وكل الجهات المعنية على مستوى العالم لمواجهة التحديات المشتركة، وهي تؤمن بأن على جميع الدول أن تتحمل مسؤولياتها في تعزيز السلم والأمن الدوليين، سواء عبر الإنترنت أو خارجه، وهي ترى أن أفضل ما يمكن فعله للبدء في ذلك يتمثل في الالتزام بمعايير سلوك الدولة المسؤولة، بالإضافة إلى التزاماتها الأخرى بموجب القانون الدولي، وهذا ما أكدته الدولة خلال المناقشة المفتوحة التي عقدها مؤخراً مجلس الأمن التابع للأمم المتحدة حول الأمن السيبراني، وهي المناقشة الأولى التي يجريها المجلس حول هذا الموضوع، وتدرك الإمارات تماماً أن هذا الموضوع معقد وأبعاده متشعبة، ولاشك في أنه يهم كل دول العالم، ولذلك لابد من تعزيز العمل الجماعي في هذا المجال وفي المجالات الأخرى كذلك؛ فالعمل المتعدد الأطراف أساسي للحماية من مخاطر التهديدات الإلكترونية. وفي هذا السياق تستضيف الدولة أكبر مؤتمرات الأمن السيبراني والتحول الرقمي، بما في ذلك جيتكس، وجيسيك، وسيبرتيك، لبناء القدرات المحلية، وعملت على تطوير منصة

للشراكة بين القطاعين العام والخاص لتسهيل تبادل المعلومات، وعززت الدولة كذلك تعاونها مع الدول والمنظمات الدولية وكيانات القطاع الخاص المعنية بهذا الموضوع (الكويتي، 2022)

سابعا دعم الترسانة التشريعية من أجل تحقيق الأمن السيبراني

منها قانون مكافحة جرائم تقنية المعلومات الجديد لسنة 2021. وفي هذا السياق جاء إعلان إنشاء مجلس للأمن السيبراني؛ بهدف إعداد سياسات وتشريعات لتعزيز الأمن السيبراني في الدولة، ورفع جاهزيَّة جميع القطاعات للاستجابة للتهديدات السيبرانية. وقد وقّع المجلس في مارس 2022 مذكرة تفاهم مع شركة "ديلويت"، إحدى كُبريات شركات الخدمات المهنية في العالم؛ لتنظيم أطر التعاون بين الطرفين، وبناء القدرات ليس داخل دولة الإمارات فقط؛ بل في المنطقة والعالم أيضًا؛ ما سيُمكّن المجلس من الإسهام بفاعليَّة في الجهود الدولية لمحاربة التهديدات السيبرانية والتصدّي لها.

II. نتائج الدراسة

إنّ الجرائم الإلكترونية لن تختفي قريبًا. وستكون تحد لتقدم التحول الرقمي ومن المتوقع أن ينمو عدد أكبر من هذه الجرائم في السنوات القادمة ما دام المكان المفضل في جميع أنحاء العالم لهذه الفئة هو الإنترنت، وسيستمر سوق الأمن السيبراني في تحقيق نمو أعلى، ومما يبدو أن تكاليف وأضرار الجرائم الإلكترونية أعلى من تلك الناجمة عن الكوارث الطبيعية، وسوف يزداد الطلب على وظائف الأمن السيبراني.

وفق هذه المعطيات يمكن القول بأن الاختراقات الإلكترونية والهجمات السيبرانية بمختلف أشكالها ستكون في المستقبل أكبر وأسوأ وأكثر كلفة، ولها تأثير مدمّر على البُنى التحتية الحرجة، خاصةً مع التزايد السريع للأجهزة المتصلة بالشبكة العنكبوتية، وانتشار المدن الذكية، ونمو استخدام إنترنت الأشياء والتكنولوجيا والمعاملات الإلكترونية والتطبيقات المتعلقة بها.

.

ضرورة مبادرة الجهات الحكومية والشركات الخاصة لإعادة تقييم استراتيجيات الأمن السيبراني وسياسات أمن شبكة الإنترنت لمواجهة هذه المخاطر، حيث عملت بعض الشركات على تعزيز أنظمتها الحالية، حيث أصدرت "جوجل" و"آبل" بياناً تؤكد فيه للمستخدمين أن نظامهم لتتبع الاتصال سيُشفر، وأن اتصال بلوتوث المستخدم لتتبع الموقع سيكون قوياً إلى درجة كافية كي لا يُخترق لتحديد الموقع والحصول على تفاصيل الجهاز.

استخدام تقنيات جديدة لتطوير منصات الأمن السيبراني الحالية، إذ تبحث العديد من المراكز العالمية في كيفية استخدام الذكاء الاصطناعي لمواجهة التهديدات السيبرانية. ومنها تعلم الآلة لتحليل مجموعات البيانات وتحديد الأنماط والصلات الخاصة بالهجمات بسرعة أكبر مما يمكن أن يفعله المحققون باستخدام الوسائل التقليدية.

III. خاتمة:

انطلاقا مما تم سرده وتحليله من خلال ماسبق تبين لنا أنه تزايد اعتماد البشرية جمعاء على خدمات الاتصالات والتقنية، إلى جانب التحول الرقمي الذي تشهده معظم القطاعات والمؤسسات والحكومات في المعمورة، سيُلزم بالاستعداد والتجهيز والاهتمام بالبنى التحتية الرقمية والعنصر البشري المؤهل، مع عدم إغفال تطبيق أقصى وأرقى المعايير الأمنية، دون إغفال التشريعات القانونية وتنظيم التعامل مع التحديات المُعقَّدة الناجمة عن تزايد الجرائم الإلكترونية للحيلولة دون وقوعها..

و أن -دولة الإمارات العربية المتحدة تعد من الدول التي تبنّت خطوات مهمّة لتعزيز ممارساتها في مجال الأمن السيبراني خاصة وأنها نجحت خلال عامين فقط في تعزيز تنافسيتها العالمية، من خلال رفع

مستويات الحماية السيبرانية وتكثيف الجهود في سبيل تحقيق الأمن في الفضاء الرقمي ، بالإعتمادعلى إعداد سياسات وتشريعات لتعزيز الأمن السيبراني في المنظمات المرتبطة برفع جاهزيَّة هذه الأخيرة للاستجابة للتهديدات السيبرانية. واقرار قوانين وأنظمة متطورة لمكافحة الجرائم الإلكترونية أن تعزيز الأمن السيبراني ، مسؤولية جميع أفراد المجتمع الذين يشكّلون خط الدفاع الأول، ومن ثم يأتي دور الجهات الحكومية والمؤسسات. الأمر الذي سمح لها بالإسهام بفاعليَّة في الجهود الدولية لمحاربة التهديدات السيبرانية والتصدّي لها. وهي الآن نموذج يحتذى ويشار إليه بالبنان في هذا المجال الذي يعتبر نحد للتحول الرقمي المنشود في حكومات ومنظمات جميع الدول في الوقت الحالي ومانوصي به في نهاية الدراسة الآتي:

1. ضرورة تفعيل منظومة الدفاع السيبراني لدى جميع الجهات والمؤسسات ونشر الوعي الأمني بين أفراد المؤسسة والتصدي لمثل هذه الهجمات، بالإضافة إلى التعاون مع الجهات المعنية لمشاركة مثل هذه البيانات باستباقية.
2. أهمية التصدي لمختلف الأنواع من الهجمات السيبرانية من قبل القطاعات الحيوية، بالإضافة إلى تفعيل منظومات الحماية وسياسات الأمن السيبراني ورفع وعي الجهات لأي نشاطات إلكترونية مشبوهة قد تضر في بيئات المنظمات الحكومية للدول.
3. وتأسيسا على ذلك، بات من الأهمية بمكان أن نوصي في نهاية الدراسة بضرورة تبنّي الدول والحكومات، خاصة العربية، إستراتيجيات تعززّ بها أمنها السيبراني، وإنشاء وحدات أو هيئات مختصة بحماية البنى التحتية من المخاطر الإلكترونية، وعلى رأس ذلك الاستثمار في البحث العلمي، وزيادة الوعي بهذا المجال بما يعزّز مستوى الأمن ومواكبة التكنولوجيا والتقنيات الحديثة التي من شأنها أن تجعل الأنظمة الإلكترونية أكثر أمنا وتماسكا وأكثر قدرة على مواجهة التحديات، وأهم هذه التحديات إنترنت الأشياء وتطبيقات الذكاء الاصطناعي بمختلف أنواعها.

الإحالات والمراجع

انواع الأمن السيبراني. (بلا تاريخ). تم الاسترداد من https://cutt.us/r1ZFY

ايمن الحربي. (2021). تم الاسترداد من https://2u.pw/h22ubj

بوقــرص ساعـد. (22 06, 2022). الأمن السيبراني : مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة. *Journal of social protection research*، الصفحات 61-76.

خالد وليد محمود. (16 02, 2022). *قراءة في مؤشر الأمن السيبراني لعام 2021*. تم الاسترداد من https://cutt.us/IJLY3

سعيد علي. (22 09, 2022). *أبرز التشريعات والمبادرات الإماراتية التي عززت الأمن السيبراني*. تم الاسترداد من https://2u.pw/kwkbN2

عطية ادريس. (1 جوان, 2019). مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. *مصداقية*، الصفحات 100-123. تم الاسترداد من مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري.

محمد ابوغزالة. (05 يوليو, 2021). *تصدُّر الإمارات المؤشرات العالمية في الأمن السيبراني.. الأهمية والدلالات والسياق والانعكاسات* . تم الاسترداد من https://cutt.us/qWshQ

محمد الكويتي. (22 05, 2022). تم الاسترداد من https://mufakirualemarat.ecssr.ae/publications/edaat/detail/603

محمد الكويتي. (23 نوفمبر, 2022). تم الاسترداد من تريندز للبحوث والاستشارات: https://cutt.us/UacmJ

محمد مسعود الأحبابي. (12 09, 2022). *نبض الأمن السيبراني*. تم الاسترداد من https://alwatan.ae/?p=1014125

مفهوم الأمن السبراني . (بلا تاريخ). تم الاسترداد من https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html

يوسف العربي. (13 أكتوبر, 2022). *مليار درهم الإنفاق على الأمن الإلكتروني في الإمارات*. تم الاسترداد من جريدة الاتحاد الاقتصادي: https://cutt.us/v7W3X