المعهد السياسي لإعداد القيادات الشبابية
Political Institute For The Preparation Of Youth Leaders

المنظومة الأمنية الإلكترونية في المملكة الأردنية الهاشمية

قطاع الإتصالات وتكنولوجيا المعلومات وتطوير القطاع العام
مشروع الحكومة الشبابية
٢٠٢١

إعداد :

- عيد مسلم
- أحمد رجوب
- رعد الصمادي
- رغداء الزعبي
- يونس الرواشدة

وزارة الشباب
قراراتنا... مستقبلنا

المعهد السياسي لاعداد القيادات الشبابية – وزارة الشباب
www.shababgovjo.org

الملخص التنفيذي

لقد تم إعداد ورقة السياسات من خلال أعضاء قطاع الإتصالات وتكنولوجيا المعلومات وتطوير القطاع العام في مشروع برنامج الحكومة الشبابية والبرلمان الشبابي التابع إلى المعهد السياسي لإعداد القيادات الشبابية، بهدف بيان مدى فعالية المنظومة الأمنية الإلكترونية في المملكة الأردنية الهاشمية، وذلك لتسهم في تحسين وتطوير مستوى المنظومة الأمنية الإلكترونية لمكونات المملكة، وبذات الوقت إعداد كوادر وطنية ذات كفاءات عالية متخصصة في مجالات أمن المعلومات والأمن السيبراني.

وقد أعُدت هذه الدراسة وفقاً لمنهجية إعتمدت منهج دراسة الحالة لمنظومة الأمن السيبراني الوطنية، وتم إجراء المقابلات المعمقة للحصول على المعلومات والبيانات من قبل المختصين في الجهات المعنية.

وتتضمن هذه الدراسة إستعراضاً لواقع الحال للمنظومة الأمنية السيبرانية في المملكة، حيث أدى التقدم التكنولوجي الشامل والتحول الرقمي إلى الحاجة لوسائل الإتصال الإلكترونية الحديثة لممارسة المهام والوظائف في أغلب القطاعات في حياتنا اليومية، كما ساهمت جائحة كوفيد19 في الأونة الأخيرة إلى الإعتماد بشكل شبه كلي على القطاع الرقمي، مما فتح المجال أمام المهاجمين وقراصنة الإنترنت على شن الهجمات الإلكترونية وتعريض سلامة أمن المعلومات إلى الخطر بشكل مستمر، وهذا بدوره قد ينتج عنه آثار سلبية على كافة المجالات.

ومن خلال المقابلات التي أجريت تبين وجود إجماع حول أهمية مجالات الأمن السيبراني على جميع الأصعدة، وقد توصلت الدراسة إلى مجموعة من النتائج أهمها قلة الوعي الأمني الإلكتروني مع وجود نقص حاد في الكوادر الوطنية المتخصصة في مجالات الأمن السيبراني لتلبية الإحتياجات الملحة والمتزايدة في القطاعات المختلفة خصوصاً مع الاتجاه نحو رقمنة الخدمات الحكومية والتجارة الإلكترونية والدراسة عن بعد

وبذات الوقت عدم القدرة على إستقطاب المختصين في هذا المجال بسبب الكلف والرواتب المرتفعة لأصحاب الخبرة مما يؤدي أيضاً إلى هجرة الكفاءات الحالية. وبدورها عملت الجهات المعنية على دعم هذا القطاع لجعل الفضاء الإلكتروني أكثر أماناً، ولكن الدعم وحده غير كافي دون وجود مجتمع واع ومدرك لماهية التهديدات والمخاطر الإلكترونية المختلفة ووفقاً لذلك يجب أن يكون العمل منسجماً ومتكاملاً في هذا القطاع.

وتتلخص مقترحات الدراسة حول ضرورة العمل على زيادة نشر ثقافة التوعية الأمنية الإلكترونية من المخاطر والتهديدات الرقمية لتشمل الجهات الحكومية والجهات الخاصة وكافة مكونات المجتمع من خلال تطوير منظومة توعوية شاملة وممنهجة، بالإضافة إلى إدماج ثقافة التوعية بالمناهج التعليمية وتحفيز الطلبة للتوجه إلى هذه الإختصاصات، وبذات الوقت العمل على تأسيس مراكز تدريبية متخصصة في مجالات الأمن السيبراني لتأهيل وإعداد الكوادر الوطنية القادرة على إدارة ومتابعة البنية التحتية للأمن السيبراني. كما توصي الدراسة بوجوب زيادة الدعم الحكومي لقطاعات الأمن السيبراني وإستثناء الكوادر الوطنية ذات الكفاءات من موظفي قطاع الأمن السيبراني من هيكلة الرواتب بما يتواءم مع سوق العمل. كما حثت التوصيات على تشجيع الإستثمار في مجالات الأمن السيبراني إضافة إلى سد الفراغ التشريعي وتغليض العقوبات للحد والتخفيف من الجرائم الإلكترونية.

الكلمات المفتاحية: الأمن السيبراني، أمن المعلومات، الجرائم الإلكترونية، المملكة الأردنية الهاشمية

المقدمة

يعتبر الأمن السيبراني واحد من مستحدثات التطور التكنولوجي والرقمي الذي يعيشه العالم اليوم، حيث شهد العالم تطور رقمي بكافة مجالاته وقطاعاته، ومن هنا تبرز الحاجة إلى فهم ماهية الأمن السيبراني ودراسته بشكل مستفيض كمتغير جديد في العلاقات الدولية.

ويتألف الفضاء السيبراني من بيئة تتكون من تفاعل الأشخاص والبيانات والمعلومات ونظام المعلومات والبرامج على الشبكات المعلوماتية وأنظمة الإتصالات والبنى التحتية المرتبطة بها، وأصبح الفضاء السيبراني أحد أهم سمات المجتمع الحديث، حيث أصبح يشكل عاملاً أساسياً في حياتنا اليومية كالأعمال التجارية والدراسة والعمل عن بعد، كما أصبح يعتمد عليه في المجالات العسكرية حيث تعتمد الإتصالات والقيادة والتحكم والإستخبارات على النظم السيبرانية.

وتعتبر عمليات التخريب والسرقة من أقدم الأخطار التي يتعرض لها الإنسان وتختلف هذه الدوافع من شخص لأخر، ومع التقدم العلمي والتطور التقني في وسائل الإتصال الحديثة وظهور شبكة الإنترنت وإتساع نطاق إستعمالها، أصبحت شبكة الإنترنت ووسائل التواصل الإلكترونية الحديثة أحد ركائز العالم الحديث وأهم الإستخدامات اليومية في حياة الإنسان والذي بدوره أدى إلى ظهور تغيرات في مفهوم الجرائم التقليدية إلى الجرائم الإلكترونية التي تعرف بأنها نشاط إجرامي يستخدم فيه شبكات الإتصال الحديثة بطريقة مباشرة أو غير مباشرة كوسيلة وهدف لتنفيذ الفعل الإجرامي.

يعتبر التغير التكنولوجي من المحركات الأساسية للنمو والتنمية وقد شهد هذا العصر إنفجار معلوماتي هائل بسبب التغيرات العالمية، فالدخول في عصر الإنترنت جعل المؤسسات والأفراد في مواجهة حادة مع المخاطر الناجمة عن التهديدات الرقمية الجديدة، حيث أنه ما بعد مرحلة السبعينات والثمانينات،

ازدادت أهمية استخدام وسائل الإتصال الحديثة وتكنولوجيا المعلومات والتي أدت إلى ظهور مفاهيم جديدة في طرق إختراقها مما تطلبت الحاجة إلى وجود اجراءات تضمن صحة وسلامة أمن وسائل الإتصال الحديثة، حيث أن الإجراءات الأمنية الإلكترونية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة والتقليص من عمليات إختراق المعلومات أوالتلاعب بها.

ومع تطور العلم والتكنولوجيا ووسائل تخزين المعلومات وتبادلها بالطرق الإلكترونية المختلفة، أو ما يسمى نقل البيانات عبر وسائل الإتصال الحديثة من موقع لآخر، أصبح النظر إلى أمن تلك البيانات والمعلومات أمر في غاية الأهمية لأنه وبكل بساطة يفتح الباب على مصرعيه أمام ضعاف النفوس ممن لديهم الرغبة في التجسس والتخريب وسرقة البيانات حيث دعت الحاجة إلى إنشاء وتطوير ما يسمى بأمن وحماية الفضاء الإلكتروني (الأمن السيبراني).

بناء على ذلك سوف نقوم في هذه الورقة ببيان ماهية الأمن السيبراني في المملكة الأردنية الهاشمية، من خلال توضيح الآليات المقررة لحماية الفضاء الإلكتروني، إضافة إلى توضيح التحديات والصعوبات التي تواجه تطوير منظومة الأمن السيبراني.

المحتوى البحثي ذو العلاقة

مشكلة الدراسة

أدت التحديات الناجمة عن التطور التقني والتكنولوجي في وسائل الإتصال الرقمي إلى بروز مخاطر وصراعات دولية جديدة من نوعها أو ما يسمى بالتهديدات والحوادث السيبرانية التي تؤثر بشكل مباشر على الأمن القومي، حيث أن الإعتماد على الفضاء الإلكتروني يؤدي إلى وجود علاقة طردية ما بين التهديدات السيبرانية وتحقيق الأمن القومي، ومن هنا تبرز مشكلة الدراسة في التركيز على مجال الأمن السيبراني في المملكة الأردنية الهاشمية، وإبراز مدى فعالية المنظومة الأمنية السيبراني في المملكة والتحديات والعوائق التي تواجهها لنستطيع إيجاد حلول حقيقية فعالة يمكن تطبيقها على أرض الواقع في سبيل تطوير المنظومة لتتماشى مع المؤشرات العالمية للأمن السيبراني.

أهداف الدراسة

هدفت الدراسة إلى التعرف على مدى فعالية وجاهزية المنظومة الأمنية السيبرانية في المملكة الأردنية الهاشمية، وعلى وجه التخصيص سوف تقوم الدرسة بما يلي :

- إبراز التحديات التي تواجه قطاع الأمن السيبراني في المملكة الأردنية الهاشمية
- قياس مدى فعالية المنظومة الأمنية السيبرانية في المملكة الأردنية الهاشمية
- تحسين وتطوير المنظومة الأمنية السيبرانية في المملكة الأردنية الهاشمية
- الحد والتخفيف من الجرائم الإلكترونية في المملكة الأردنية الهاشمية
- الوصول إلى فضاء أمني سيبراني أكثر أماناً محُفزاً للإستثمار، وإبراز صورة مشرقة عن فعالية القطاع الأمني السيبراني في المملكة الأردنية الهاشمية

أهمية الدراسة

إن العالم يشهد تقدماً تكنولوجياً وتقنياً هائلاً، وقد أصبح الفضاء السيبراني ساحة التفاعلات سواء من الناحية المدنية أو العسكرية، حيث أصبح الصراع اليوم يأخذ الشكل الرقمي

وكون المملكة الأردنية الهاشمية جزءاً من هذا العالم لابد من التقصي والبحث وسؤال أنفسنا عن مدى فعالية و جاهزية قطاع الأمن السيبراني في المملكة، وتتمركز أهمية الدراسة في إبراز وإظهار الواقع الفعلي للمنظومة الأمنية السيبرانية في سبيل معالجة التحديات التي تعيق تطورها.

منهجية الدراسة

تم إستخدام منهج دراسة الحالة لمنظومة الأمن السيبراني في المملكة الأردنية الهاشمية وقد تم العمل على إخضاعها للدراسة لبيان مدى فعاليتها، من خلال الجانب التطبيقي عبر منهج المقابلات الشخصية مع المختصين في مجالات الأمن السيبراني ومن خلالها تم التوصل إلى النتائج والتوصيات.

محددات وصعوبات الدراسة

يعتبر الأمن السيبراني حديث العهد في المملكة وهذا بدوره أدى إلى وجود عدد من التحديات والصعوبات التي واجهت الدراسه يمكن إيجازها على النحو التالي:

- محدودية المراجع والدراسات المحلية الدقيقة ذات الصلة بالمنظومة الأمنية السيبرانية في المملكة.
- قلة وصعوبة الحصول على المعلومات والإحصائيات المتعلقة بواقع الحال والمخاطر الإلكترونية التي تتعرض لها المملكة من قبل الجهات المعنية وهذا يعود إلى طبيعة المعلومات وحساسيتها.

المفاهيم والمصطلحات ( )

البيانات: الأرقام أو الحروف أو الرموز أو الأشكال أو الأصوات أو الصور أو الرسومات التي ليست لها دلالة بذاتها.

المعلومات: البيانات التي تمت معالجتها وأصبحت لها دلالة.

التصريح: الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو إلى الجمهور للدخول إلى أو إستخدام نظام المعلومات أو الشبكة المعلوماتية بقصد الإطلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول اليها أو ايقاف عمل الاجهزة أو تغيير موقع الكتروني أو إلغائه أو تعديل محتوياته.

أمن المعلومات: الحفاظ على سرية وتوفر وسلامة المعلومات كأصل في مراحل المعالجة والحفظ والنقل، ويتحقق ذلك عن طريق التطبيق الفعلي للسياسات الأمنية من خلال تعزيز الوعي والتعلم والتدريب.

الفضاء السيبراني: بيئة تتكون من تفاعل الأشخاص والبيانات والمعلومات ونظام المعلومات والبرامج على الشبكات المعلوماتية وانظمة الإتصالات والبنى التحتية المرتبطة بها.

الأمن السيبراني: الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على إستعادة عملها وإستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء إستخدام أو نتيجة الإخفاق في إتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك.

حادث الأمن السيبراني: الفعل أو الهجوم الذي يشكل خطراً على البيانات أو المعلومات أو نظم المعلومات أو الشبكة المعلوماتية أو البنى التحتية المرتبطة بها ويتطلب إستجابة لإيقافه أو للتخفيف من العواقب أو الآثار المترتبة عليه.

خدمات الأمن السيبراني: الأنشطة الفنية والإدارية والإستشارية في مجال الأمن السيبراني بما فيها خدمات التقييم الأمني والمراقبة والتدقيق والخدمات الإستشارية.

الوسائل الإلكترونية: تقنية إستخدام وسائل كهربائية أو مغناطيسية أو ضوئية أو كهرومغناطيسية أو شبكة معلومات أو أي وسيلة مشابهة.

الدراسات السابقة

1. دراسة بانقا،علم الدين،المعهد العربي للتخطيط، 2019،بعنوان(مخاطر الهجمات الالكترونية السيبرانية وآثارها الاقتصادية): دراسة حالة دول مجلس التعاون الخليجي، عملت هذه الدراسة على تسليط الضوء لبيان أهمية المخاطر الإلكترونية و آثارها الإقتصادية من خلال تقييم أوضاع الدول الخليجية، حيث هدفت إلى زيادة الإهتمام بالأمن السيبراني و الإستثمار به و معرفة مواضع الخلل وسد الثغرات فيها، وتوصلت إلى أنه لابد من تحسين الأداء و الوعي إضافة إلى زيادة الإنفاق حتى تتحق التكاملية فالإنفاق غير كافي دون وجود وعي مجتمعي حول أهمية الأمن السيبراني على الإقتصاد والدولة، كما بينت الدراسة أن صانعو القرار في الدول يواجهون تحديات عظيمة في المحافظة على الإستقرار المالي و الإقتصادي في ضوء تنامي المخاطر الإلكترونية وتنوعها.( )
2. دراسة الأسكوا،الأمم المتحدة،2015،بعنوان (الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية)، جاءت هذه الدراسة إستكملاً لأنشطة الإسكوا التي بدأت عام 2007، بهدف تطوير التشريعات السيبرانية، وقد هدفت الدراسة إلى بيان الوضع الراهن إقليمياً ودولياً في الجهود المبذولة في تعزيز حماية الفضاء السيبراني وضمان سلامته، إضافة إلى وضع مقترح توجيهي من أجل تعزيز الأمان السيبراني وبناء الثقة بتكنولوجيا المعلومات والفضاء السيبراني، وقد توصلت الدراسة إلى أن عملية توفير الأمان في الفضاء السيبراني عملية معقدة وصعبة ومكلفة، كما أنها تحتاج إلى تضافر الجهود في ظل تعدد وسائل الجرائم السيبرانية.( )

الإطار النظري للدراسة

بدأت الحاجة واضحة إلى سد الفجوة الرقمية والقيام بالمزيد من العمل لحماية المجتمعات من الهجمات السيبرانية والتصدي لعواقبها على أسواق العمل والأمن العالمي، وقد أكدت الدول على وجوب تحقيق أهداف التنمية المستدامة بشأن الأمن السيبراني ، كما يجب العمل على صقل المهارات الرقمية من أجل توظيف الشباب، والهيئات الأكاديمية والاستفادة من تكنولوجيا المعلومات والإتصالات والأمن السيبراني بهدف دفع عجلة التحول الرقمي.( )

المحور الأول: أمن المعلومات والأمن السيبراني

ظهرت علاقة وطيدة ما بين المعلومات والأمن بإعتبارهما وحدة واحدة لاغنى عنهما، ومع تتالي العصور لم يعد الأمن محصوراً بالحماية من الهجمات المفاجئة من قبل الأعداء على الحدود البرية والبحرية والجوية، بل تعدى الأمر إلى أن المعلومات خرجت من مكامنها التقليدية من داخل الأوراق والكتب وأتخذت شكلاً رقمياً لها أبعاد ورهانات إستراتيجية.
ويعرف أمن المعلومات بأنه الحفاظ على سرية وتوفر وسلامة المعلومات وعناصرها بما في ذلك الأجهزة والمعدات المستخدمة كأصل في مراحل المعالجة والحفظ والنقل، لمكافحة أنشطة الإعتداء عليها سواء كانت إلكترونية أو ورقية.( )

اما بالنسبة للأمن السيبراني فهو الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على إستعادة عملها وإستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء إستخدام أو نتيجة الإخفاق في إتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك.( )

وبالرجوع إلى محور دراستنا المتعلق بالأمن السيبراني يظهر بأن العلاقة ما بين أمن العلومات والأمن السيبراني هو أن كلاهما يعمل على توفير الحماية للبيانات والمعلومات من الإختراقات والهجمات من أي مخاطر محتملة، ولكن على الرغم من ذلك ففي الوقت الذي يعمل أحدهما على حماية البيانات في مكان واحد، يقوم الآخر بحمايتها بشكل أوسع وأعم، فالأمن السيبراني يهتم بحماية البيانات والمعلومات ونزاهتها وسريتها من الأخطار والتهديدات والوصول غير المصرح به عبر وسائل الاتصال الرقمي، بينما أمن المعلومات يهتم بحماية البيانات والمعلومات ونزاهتها وسريتها أينما وجدت سواء كانت مادية أو الكترونية.

عناصر أمن المعلومات والأمن السيبراني:

يهدف أمن المعلومات و الأمن السيبراني إلى حماية البيانات والمعلومات وتوفير بيئة أمنة من خلال وضع إطار قوي وشامل ليكون قادراً على تغطية جميع جوانب الأمان ووفقاً لذلك يجب توافر العناصر التالية: ( )

1. السرية أو الموثوقية: ويقصد بها منع الوصول إلى البيانات والمعلومات إلا من خلال الأشخاص المصرح لهم فقط سواء عند تخزينها أو عند نقلها عبر وسائل الاتصال الحديثة.
2. تكاملية البيانات وسلامتها: وهي ضمان سلامة محتوى المعلومات، ويقصد بها الحفاظ على البيانات والمعلومات من التغيير أو التعديل من الأشخاص غير المخولين.
3. التوافرية والإتاحة: قصد بها أن تكون البيانات والمعلومات والخدمات متوفرة عند الحاجة إليها دون وجود أي عوائق لوصولها بالشكل المطلوب.

المحور الثاني: الإطار التشريعي للأمن السيبراني في المملكة الأردنية الهاشمية

تكمن أهمية التشريع كمصدر رئيس ومهم للقاعدة القانونية، حيث يحتل التشريع مركز الصدارة في أغلب دول العالم، كأول مصدر من المصادر الرسمية، ويتضح من ذلك أن التشريع يعني عمليه سن النص التي يخرج بها مضمونه إلى حيز الوجود والإلزام.

بناء على ذلك، سوف يتم توضيح الدور الذي تقوم به المملكة لتنظيم قطاع الأمن السيبراني من خلال إستعراض النصوص التشريعية والقانونية المتعلقة بالأمن السيبراني.

يعد الأمن السيبراني في المملكة حديث العهد، حيث عمل المشرع الأردني على سن القانون الخاص بالأمن السيبراني في عام 2019، فيما تم سن النظام الخاص به في عام 2020 .( ) وتهدف هذه التشريعات للحماية من التهديدات الإلكترونية المحيطة والمحتملة، إضافة إلى بناء القدرات الوطنية القادرة على مواجهة التهديدات التي تعترض أنظمة المعلومات والبنى التحتية.

وقد عرف المشرع الأردني الأمن السيبراني بأنه "الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على إستعادة عملها وإستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء إستخدام أو نتيجة الإخفاق في إتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك"( )

بناء على ذلك، سوف يتم توضيح الدور الذي تقوم به المملكة لتنظيم قطاع الأمن السيبراني من خلال إستعراض النصوص التشريعية والقانونية المتعلقة بالأمن السيبراني.

أولا: قانون الأمن السيبراني رقم 16 لسنة 2019

هو القانون المعني بالفضاء السيبراني في المملكة، حيث يعتبر القانون الأول من نوعه في تاريخ التشريعات الأردنية، ويعمل هذا القانون على تنظيم الفضاء السيبراني وحمايته من التهديدات الرقمية، كما أنه يعتبر جزءاً أساسياً من السياسات الأمنية الوطنية إذ أصبح صناع القرار يعتمدون عليه كأولوية في سياستهم الدفاعية كونه يمنح صلاحيات للجهات المسؤولة عن الأمن السيبراني في المملكة، ويشكل القانون بداية لبناء قدرات مختصة بالأمن السيبراني.

إضافة إلى ذلك يعمل القانون على وجود مرجعية لمراقبة الفضاء السيبراني وتوثيق الهجمات السيبرانية في المملكة وتنفيذ السياسات العامة التي تنبثق عن الإستراتيجية الوطنية للأمن السيبراني، ويعرف المشرع الأردني الفضاء السيبراني بأنه "بيئة تتكون من تفاعل الأشخاص والبيانات والمعلومات ونظام المعلومات والبرامج على الشبكات المعلوماتية وانظمة الإتصالات والبنى التحتية المرتبطة بها."( )

وقد نص قانون الأمن السيبراني في المملكة على تشكيل مجلس يسمى (المجلس الوطني للأمن السيبراني) يتألف من رئيس يعين بإرادة ملكية سامية وعدد من الاعضاء يمثلون الجهات التآلية:( )

1. وزارة الإقتصاد الرقمي والريادة.
2. البنك المركزي الاردني.
3. القوات المسلحة الاردنية - الجيش العربي.
4. دائرة المخابرات العامة.
5. مديرية الأمن العام.
6. المركز الوطني للأمن وإدارة الأزمات.
7. ثلاثة اعضاء يسميهم مجلس الوزراء بناء على تنسيب رئيس المجلس لمدة سنتين قابلة للتجديد لمرة واحدة على أن يكون اثنان منهم من ذوي الخبرة من القطاع الخاص.

وللمجلس مهام وصلاحيات حددها القانون:

1. اقرار الإستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني.
2. إقرار الخطط والبرامج اللازمة لقيام المركز بمهامه وواجباته بما فيها برامج التعاون الدولي والإقليمي.
3. اعتماد التقارير ربع السنوية عن الوضع الأمني السيبراني للمملكة والتقرير السنوي عن أعمال المركز.
4. تشكيل اللجان التنسيقية من ذوي العلاقة لتمكين المركز من تحقيق أهدافه على أن تحدد في قرار تشكيلها مهامها وواجباتها وكيفية انعقاد اجتماعاتها وإتخاذ قراراتها.
5. إقرار الموازنة السنوية للمركز.

وفي سبيل إدامة تفعيل القانون وتحقيق الغاية المرجوة منه نص المشرع على أن المركز هو الجهة المختصة لتلقي لشكاوى والإخبارات المتعلقة بالأمن السيبراني وحوادث الأمن السيبراني وله متابعتها وإتخاذ الإجراء المناسب لمعالجتها ومنع حدوثها أو إستمرارها وفق الصلاحيات الممنوحة له، ولتحقيق التكاملية في الإبلاغ عن حوادث الأمن السيبراني ألزم الوزارات والدوائر الحكومية والمؤسسات الرسمية العامة والخاصة بتزويد المركز بكل المعلومات اللازمة عن أي تهديد أو خطر سيبراني.

وقد نص قانون الأمن السيبراني في المملكة على إنشاء مركز يسمى (المركز الوطني للأمن السيبراني) يرتبط برئيس الوزراء ويتمتع بشخصية إعتبارية ذات إستقلال مالي وإداري وله بهذه الصفة تملك الاموال المنقولة وغير المنقولة والقيام بجميع التصرفات القانونية اللازمة لتحقيق أهدافه بما في ذلك إبرام العقود وله حق التقاضي وينوب عنه في الإجراءات القضائية وكيل إدارة قضايا الدولة.

يهدف المركز إلى بناء منظومة فعالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها للحماية من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفعالية بما يضمن إستدامة العمل والحفاظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات.

يتولى المركز في سبيل تحقيق أهدافه المهام والصلاحيات حددها القانون:

1. إعداد إستراتيجيات وسياسات ومعايير الأمن السيبراني ومراقبة تطبيقها ووضع الخطط والبرامج اللازمة لتنفيذها ورفعها للمجلس لإقرارها.
2. تطوير عمليات الأمن السيبراني وتنفيذها وتقديم الدعم والإستشارة اللازمين لبناء فرق عمليات الأمن السيبراني في القطاعين العام والخاص وتنسيق جهود الإستجابة لها والتدخل عند الحاجة.

3. تحديد معايير الأمن السيبراني وضوابطه وتصنيف حوادث الأمن السيبراني بموجب تعليمات يصدرها لهذه الغاية.
4. منح الترخيص لمقدمي خدمات الأمن السيبراني وفقا للمتطلبات والشروط والرسوم المحددة بموجب نظام يصدر لهذه الغاية.
5. تبادل المعلومات وتفعيل التعاون والشراكات وإبرام الإتفاقيات ومذكرات التفاهم مع الجهات الوطنية والإقليمية والدولية ذات العلاقة بالأمن السيبراني.
6. تطوير البرامج اللازمة لبناء القدرات والخبرات الوطنية في مجال الأمن السيبراني وتعزيز الوعي به على المستوى الوطني.
7. التعاون والتنسيق مع الجهات ذات العلاقة لتعزيز أمن الفضاء السيبراني.
8. إعداد مشروعات التشريعات ذات العلاقة بالأمن السيبراني بالتعاون مع الجهات المعنية ورفعها للمجلس.
9. التقييم المستمر لوضع الأمن السيبراني في المملكة بالتعاون مع الجهات المعنية في القطاعين العام والخاص.
10. تحديد شبكات البنى التحتية الحرجة ومتطلبات استدامتها.
11. إنشاء قاعدة بيانات بالتهديدات السيبرانية.
12. تقييم النواحي الأمنية لخدمات الحكومة الإلكترونية.
13. تقييم وتطوير فرق الإستجابة لحوادث الأمن السيبراني.
14. إعداد سياسة تتضمن معايير أمن وحماية المعلومات.
15. دعم البحث العلمي في مجالات الأمن السيبراني بالتعاون مع الجامعات.
16. إجراء تمارين ومسابقات للأمن السيبراني.
17. إعداد مشروع الموازنة السنوية للمركز والتقرير السنوي عن أعماله والبيانات المالية الختامية.
18. إعداد التقارير ربع السنوية عن الوضع الأمني السيبراني للمملكة ورفعها للمجلس.
19. أي مهام أو صلاحيات أخرى تنص عليها الأنظمة والتعليمات الصادرة إستنادا إلى أحكام هذا القانون.

ثانياً: نظام المركز الوطني السيبراني رقم 1 لسنة 2020

نـص الدسـتور الأردنـي علـى أن الملـك يصـدق علـى القـوانين ويصـدرها ويـأمر بوضـع الأنظمة اللازمة لتنفيذها بشرط أن لا تتضمن ما يخالف أحكام القانون.( )

ووفقاً لما سبق نص النظام على أن رئيس مركز الأمن السيبراني يكون مسؤولا أمام المجلس الوطني للأمن السيبراني عن إدارة المركز، وفي سبيل تحقيق ذلك يجب عليه القيام بالمهام التالية :-( )

1. التنسيق بين المركز والجهات المختصة بالتحقيق في الجرائم أو الحوادث المتعلقة بالأمن السيبراني.
2. بناء منصة مركزية لتبادل المعلومات بين مختلف فرق الإستجابة لحوادث الأمن السيبراني المحلية والدولية وإدارة قنوات الاتصال بينها وبناء منظومات قادرة على التحليل وتوزيع المعلومات المتعلقة بالتهديدات السيبرانية.
3. الإشراف على قيام المركز بتقديم خدماته بما فيها فحص قابلية إختراق نظم وشبكات المعلومات والإتصالات وتقييم ومسح المخاطر والدعم الفني والاستشاري ووفقا للتعليمات الصادرة لهذه الغاية.
4. إعلام مجلس الوزراء وبعد موافقة المجلس بالوزارات والدوائر الحكومية والمؤسسات الرسمية والعامة التي تخالف أحكام القانون.
5. التنسيق مع الأجهزة الأمنية والعسكرية لإتخاذ ما يلزم من إجراءات لمعالجة أي أخطار أو تهديدات تتعلق بالأمن السيبراني.

إذن يتضح أن المشرع عمل على تنظيم قطاع الأمن السيبراني من خلال القوانين والأنظمة السابقة، إضافة إلى ذلك نص على العقوبات والجزاءات على من يخالف القوانين والأنظمة والتعليمات المعنية بالأمن السيبراني حيث يتم إتخاذ إجراء أو أكثر من هذه الإجراءات وفق ما يتناسب مع طبيعة المخالفة والجهة التي ارتكابتها:

1. التنبيه الخطي لتصويب المخالفة خلال المدة التي يحددها.
2. تصويب المخالفة والرجوع على المخالف بالنفقات التي تكبدها المركز نتيجة لذلك.
3. حجب أو الغاء أو مصادرة أو تعطيل شبكة الإتصالات ونظام المعلومات والشبكة المعلوماتية واجهزة الإتصالات والرسائل الإلكترونية الخاصة مع الجهات ذات العلاقة عن كل من يشتبه في إرتكابه أو إشتراكه في أي عمل يشكل حادث أمن سيبراني.
4. إلزام الجهة المخالفة بإتخاذ الإجراءات القانونية بحق من يثبت تسببه بالمخالفة من العاملين لديها.
5. الغاء أو إيقاف ترخيص المرخص له بتقديم أي من خدمات الأمن السيبراني للمدة التي يراها المركز مناسبة.
6. فرض غرامة لا تقل عن (500) دينار ولا تزيد على (100,000) دينار وتضاعف الغرامة في حال تكرار المخالفة.

تأسيساً على ما تقدم وبعد إستعراض نصوص قانون الأمن السيبراني والنظام المعني به يعتبر قانون الأمن السيبراني الأول من نوعه في المملكة، حيث تم سن القانون في العام 2019 وجاء ذلك بسبب الحاجة إلى تنظيم الفضاء الأمني الإلكتروني وبناء القدرات المتخصصة في الأمن السيبراني لمواجهة جميع التحديات والتهديدات التي قد تتعرض لها المملكة.

ففي العام 2015 سن المشرع نصوص قانونية تعنى بتنظيم الجريمة الإلكترونية وعقوبتها من خلال قانون الجرائم الإلكترونية، لأن القاعدة العامة تنص على أنه لا جريمة ولا عقوبة إلا بنص، ولكن عندما تم تشريع قانون الأمن السيبراني لسنة 2019 ضمن وجود مرجعية موحدة تنظم الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني، حيث عمل القانون على حصر الجهات المختصة بإقرار الإستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني،

والـذي بـدوره يجـب أن يـؤدي إلـى الإنسـجام فـي القـرارات الصـادرة والمتعلقـة بـالأمن السـيبراني ، كـون هـذا القـانون أصبح ضـرورة وطنيـة فـي ظـل التحـول الرقمـي العالمي، وهـو قانون حديث العهد في المملكة وهذا ما يجعله عرضة للتعديل والتطوير بما يتـواءم مع التغذية الراجعة من المعنيين، حيث أن التعاون ما بين الفنيين والقانونيين سيؤدي إلى معالجة التحديات التي تنشأ نتيجة لتسارع التطورات التقنية محلياً ودولياً.

وعلى الرغم من أن القانونين منفصلين عن بعضهما إلا أنهما يهدفان إلى ذات الغاية وهـي إيجـاد فضـاء إلكترونـي أكثـر أمانـاً بعيـداً عـن الجـرائم والأخطـار الإلكترونيـة، ولكـن الرابطة ما بينهما هو العمل على وجود مرجعية موحدة في القضايا والحوادث السيبرانية التي تهدد الوطن بجميع مكوناته في أنظمته وشبكاته وبناه التحتية، بالإضافة إلى رفع مستوى الأمن الوطني العام والشامل للمؤسسات و الأفراد، من خلال تطوير قدرات ردع ومراقبـة وإنـذار وإسـتجابة لحـوادث الأمـن السـيبراني، أي بوجـود هـذه المرجعيـة الموحـدة ستسـتطيع الحكومـة تنفيـذ الإسـتراتيجية الوطنيـة للأمـن السـيبراني بالإعتمـاد على الشـرعية القانونية دون وجود عوائق أو صعوبات عند التنفيذ. وما يؤكد ذلك هو نـص المـادة 8 مـن قـانون الأمـن السـيبراني والتـي تؤكـد بـأن المركـز هـو مـن يتقلـى الشـكاوي و الإخبـارات المتعلقـة بـالأمن السـيبراني وعلـى الـوزارات والـدوائر الحكوميـة والمؤسسات الرسمية العامة والخاصة الإلتزام بذلك، كما نص القانون في المادة 19 على أن رئيس الوزراء والوزراء مكلفون بتنفيذ أحكام هذا القانون.

المحور الثالث: التحديات التي تواجه المنظومة الأمنية السيبرانية في المملكة الأردنية الهاشمية

مع إستمرار العديد من الدول في تحديث وتنويع إقتصادها مع الإعتماد على الخدمات الرقمية في المعاملات الإلكترونية الحكومية والتجارة والتعليم تتزايد فرص التهديدات الرقمية على حد سواء،

ففي ظل الإعتماد على وسائل الإتصال الإلكترونية لابد من وضع خطط لتعزيز البنية التحتية الإلكترونية تهدف إلى خلق فضاء سيبراني أكثر أماناً يساعد على تمكين الأفراد من تحقيق طموحاتهم، ويمكن الشركات من التطور والنمو في بيئة مزدهرة.

وقد ذكرنا سابقاً أن الأمن السيبراني حديث العهد، لذلك فمن الطبيعي أن تواجة عدد من التحديات والعوائق في سبيل تحقيق الأهداف لبناء إستراتيجية سيبرانية متكاملة على المستوى العالمي.

سوف أقوم بذكر أهم التحديات على النحو التالي:

أولا: الثقافة الوطنية للأمن السيبراني

يتعين على جميع الجهات المعنية في كل من القطاعين العام والخاص فهم المخاطر الإلكترونية المحتملة التي تهدد أمنها، ومدى تأثير تلك المخاطر عليها وعلى الأخرين في النظام البيئي الخاص بالبنية التحتية الإلكترونية.( )

ويقع على عاتق الجهات المعنية المسؤولة عن مكافحة جميع المخاطر الناشئة عن الأمن السيبراني، وقد حدد قانون الأمن السيبراني هذه المسؤولية وحصرها بالمركز الوطني للأمن السيبراني حيث نص على انه يتولى العديد من المهام ومن ضمنها إعداد إستراتيجيات وسياسات ومعايير الأمن السيبراني ومراقبة تطبيقها ووضع الخطط والبرامج اللازمة لتنفيذها، إضافة إلى تقديم الدعم والإستشارة اللازمين لبناء فرق عمليات الأمن السيبراني في القطاعين العام والخاص وتنسيق جهود الإستجابة لها والتدخل عند الحاجة، وتبادل المعلومات وتفعيل التعاون والشراكات وإبرام الإتفاقيات ومذكرات التفاهم مع الجهات الوطنية والاقليمية والدولية ذات العلاقة بالأمن السيبراني، كما يجب على المركز إنشاء قاعدة بيانات بالتهديدات السيبرانية ويأتي ذلك في سبيل تشكيل قاعدة بيانات محتملة بالأخطار التي قد تتعرض لها المملكة في المستقبل.( )

ثانياً: الثقافة المجتمعية للأمن السيبراني

تعتمد المجتمعات بشكل كبير على الإنترنت والخدمات الإلكترونية، وفي ظل التزايد في إستخدام الوسائل الإلكترونية لابد من العمل على نشر ثقافة الأمن السيبراني بين الأفراد المستخدمين لهذه الوسائل بإستخدام الأدوات المناسبة لذلك، ويجب التنوية إلى أن ثقافة الأمن السيبراني أكبر من مجرد وضع سياسات وإستراتيجيات فلا من وجود آلية فعالة للتوعية بمفهوم وماهية الأمن السيبراني، حيث يعتبر التحدي الأكبر هو عدم الإدراك الحقيقي لمفهوم الأمن السيبراني.( )

وفي سبيل تحقيق هدف نشر الثقافة يكون الدور الأكبر للمدارس والجامعات والجهات المعنية، حيث يجب على القطاعات المعنية إدماج مفاهيم الأمن السيبراني ضمن المناهج التعليمية، حيث يبدأ النهج التوعوي منذ الصفوف الأولى.

ثالثاً: الكوادر الوطنية

تماشيا مع التطورات السريعة والإستخدام المتزايد للوسائل والخدمات الإلكترونية، قامت المملكة في سبيل إخراج جيل واعي ومدرك لمجالات الأمن السيبراني وإنشاء كوادر مؤهلة بإستحداث التخصصات الجامعية المعنية بالأمن السيبراني، فالتحول الرقمي أجبر الدول على تعزيز هذا القطاع. حيث أن الكوادر البشرية المؤهلة والمختصة في مجالات الأمن السيبراني من أكبر العوائق التي تواجهه الجهات المعنية في تحقيق أهداف المركز الوطني للأمن السيبراني. كما تعتبر تكلفة التأهيل المرتفعة في مجالات الأمن السيبراني احد اهم العوائق أمام المهتمين في المجال السيبراني سواء على مستوى الطلبة أو العاملين في مجال أمن وحماية المعلومات.

المحور الرابع: الخدمات الأمنية السيبرانية في المملكة الأردنية الهاشمية

تتنوع الخدمات السيبرانية المقدمة من قبل مزودي تلك الخدمات كما تتفاوت جودة تقديم هذه الخدمات حيث تعتمد على العديد من العوامل مثل القدرات والخبرات والمنهجيات المتبعه في إدارة هذه الخدمات.

عـرف المشـرع الأردنـي خـدمات الأمـن السـيبراني بأنهـا الأنشـطة الفنيـة والإداريـة والإستشـارية فـي مجال الأمـن السـيبراني بما فيها خـدمات التقييم الأمني والمراقبة والتدقيق والخدمات الإستشارية.( )

وقـد نـص قـانون الأمـن السـيبراني علـى أن المركـز الـوطني للأمـن السـيبراني يمتلـك صلاحيات لـ "منح الترخيص لمقدمي خدمات الأمن السيبراني وفقا للمتطلبات والشروط والرسـوم المحـددة بموجـب نظـام يصـدر لهـذه الغايـة"، وفـي حـال تقـديم الخـدمات دون الحصول ترخيص فأن الجهة تعرض نفسها للمسؤولية وفق العقوبات السالفة الذكر.( )
ولكـن علـى الـرغم مـن ذلـك يجـب العمـل علـى ضـمان وضـبط جـودة الخـدمات السـيبرانية المقدمة من قبل مزوديها وإيجاد آلية للمتابعة وتقييم الأداء لتحقيق الغايات المرجوه منها حيث يسهم ذلك في تحسين كفاءة المنظومة السيبرانية.

المقابلات

عمل المعهد السياسي لإعداد القيادات الشبابية على تنسيق وتسهيل إجراء المقابلات الشخصية مع المعنيين في مجال الأمن السيبراني على المستوى الوطني للبحث والتقصي حول بيان مستوى القدرات الدفاعية الإلكترونية والوعي الأمني الإلكتروني في مجالات الأمن السيبراني في المملكة، إضافة إلى معرفة مدى الإلمام والإختصاص في مجال الأمن السيبراني ضمن الهيئات المعنية.

ووفقاً لذلك قد تم إجراء المقابلات مع الجهات التآلية:
أولا: المركز الوطني للأمن السيبراني
ثانياً: وحدة مكافحة الجرائم الإلكترونية
تم توجيه عدة أسئلة إلى الجهات المذكورة أعلاه وتم التعاون من قبل المختصين بشكل كبير وقد تم الحصول على إجابات مفيدة لغايات البحث الإجرائي للدراسة.

نتائج الدراسة:

أولا: أدت الثورة الإلكترونية إلى زيادة ملحوظة في التهديدات والمخاطر من خلال الهجمات الرقمية، مما أدى إلى الاعتداء على حقوق الآخرين ومخالفة القانون، ولهذا السبب تم ضبط قواعد السلوك للإستخدام الأمثل لوسائل الإتصال الإلكتروني، بناء عليه عمل المشرّع الأردني على تنظيم النصوص القانونية المعنية بالأمن السيبراني وفق لقانون الأمن السيبراني رقم 16 لسنة 2019، وقانون الجرائم الإلكترونية رقم 27 لسنة 2015.

ثانياً: قلة الوعي الأمني الإلكتروني لدى مكونات المجتمع الأردني، حيث ساهمت جائحة كوفيد19 بزيادة نسبة الحاجة إلى إستخدام الوسائل الإلكترونية المختلفة في شتى القطاعات، وهذا بدوره أدى إلى تعرض شريحة واسعة إلى خطر التهديدات الإلكترونية الشائعة والمحتملة خصوصاً بعد الإعتماد على التجارة الإلكترونية والتعليم عن بعد من خلال وسائل الإتصال الرقمي مما يزيد من فرص تعرض شريحة أكبر من المجتمع وخاصة الأطفال لخطر الجرائم الإلكترونية. حيث أن الجهات المختصة في مجالات الأمن السيبراني تقوم على إعداد وتنفيذ برامج توعوية في التهديدات الأمنية السيبرانية ولكنها لاتزال تفتقر إلى المنهجية المتسلسلة في طرح المخاطر والتهديدات الإلكترونية وإلى أدوات قياس المخرجات من هذه البرامج وهذا يؤدي إلى عدم الوصول إلى الهدف المرجو من البرامج التوعوية.

ثالثاً: نقص حاد في الكوادر الوطنية في مجالات الأمن السيبراني، خصوصاً مع زيادة الطلب والحاجة الملحة على هذه التخصصات في ظل تزايد التهديدات والمخاطر السيبرانية، وعلى الرغم من أن المملكة بدأت بالعمل على طرح مجالات الأمن السيبراني في التخصصات الجامعية إلا أن النقص ما زال عائق أمام الجهات المعنية خصوصاً في ظل إرتفاع الرسوم الدراسية لتخصصات الأمن السيبراني وإفتقار وسائل التحفيز للإختصاص في هذه المجالات.

رابعاً: عدم القدرة على المحافظة على الكفاءات الوطنية الحالية والحد من هجرة الكفاءات، بسبب إرتفاع رواتب أصحاب الخبرة في سوق العمل مما يحد من قدرة المؤسسات الحكومية والوطنية على إستقطاب هذه الخبرات والذي يؤدي إلى تمركز وإحتكار الإختصاص في يد القطاع الخاص والجهات الخارجية، حيث أن الفروقات في قيمة الرواتب بين القطاع العام والخاص تعتبر مجزية للأفراد المختصين في هذه المجالات، وهذا العائق يشكل عقبة أمام تطوير المجال السيبراني ويعود ذلك سلبا على النظام الأمني الإلكتروني خصوصاً في ظل توجه معظم القطاعات الحكومية إلى الفضاء الإلكتروني.

خامساً: إرتفاع كلف التدريب والتأهيل في مجالات الأمن السيبراني سواء للجهات الحكومية والخاصة والأفراد، وهذا العائق يدل على أن إستراتيجيات تطوير مجال الأمن السيبراني قد لا تلبي الهدف المطلوب طالما يوجد صعوبة في تنفيذها على أرض الواقع وخصوصاً في ظل الأو ضاع الإقتصادية الحالية وهذا بدوره يؤدي إلى عدم الإقبال على الإختصاص من قبل المهتمين في هذا المجالات، وحيث أن العديد من الدول بدأت بتدارك هذا العائق من خلال العديد من الحلول كتدرب مدربين مختصين في مجالات الأمن السيبراني للعمل على تدريب كافة الفئات من ابتداءاً من الموظفين في مختلف الجهات والقطاعات ووصولا إلى الطلبة الجامعيين مثل مبادرة (سايبرهبَ) في المملكة العربية السعودية المعنية بالطلبة الجامعيين التي تسعى إلى بناء الكفاءات الوطنية بما يتوافق مع رؤية 2030 لسد الإحتياج في هذا المجال

تحليل وخيارات السياسة

التوصيات العامة

أولا: العمل على نشر ثقافة التوعية الأمنية الإلكترونية لدى الجهات الحكومية والجهات الخاصة وكافة فئات المجتمع وخاصة مستخدمي وسائل الإتصال الرقمي، ويتم ذلك من خلال تطوير منظومة توعوية عن طريق القنوات والوسائل الرقمية والوجاهية المختلفة بشكل دوري ومستدام تعتمد على مدخلات ومخرجات واضحة يتم متابعتها من خلال أدوات التقييم والقياس للتأكد من فعالية المخرجات المطلوبة، إضافة إلى ذلك يجب العمل على تحديث البرامج التوعوية بما يتواءم مع تطور المخاطر والتهديدات الإلكترونية.

ثانياً: إدماج ثقافة الوعي بالمخاطر والتهديدات الإلكترونية في جميع المراحل التعليمية بشكل متدرج لتوعية الطلبة بالمخاطر الإلكترونية بمختلف أنواعها وإنشاء جيل واعٍ في أمن المعلومات والأمن السيبراني منذ الصفوف الأولى.

ثالثاً: تحفيز الطلبة للتوجه إلى إختصاصات وتفرعات أمن وحماية المعلومات والأمن السيبراني من خلال إبراز أهمية هذه التخصصات وتوفير الدعم لها عن طريق توفير الموارد والمتطلبات اللازمة لهذه التخصصات في الجامعات والكليات التعليمية وتخفيض الرسوم الدراسية وزيادة فرص الإبتعاث في هذه التخصصات مما يؤدي إلى زيادة إعداد المؤهلين في هذه المجالات.

رابعاً: تأسيس مراكز وطنية تدريبية متخصصة في مجالات الأمن السيبراني في كافة أنحاء المملكة تقوم على إعداد وتأهيل كوادر وطنية على قدر عالٍ من الكفاءة في مجالات الأمن السيبراني بما يمكنها من إدارة ومتابعة البنى التحتية للأمن السيبراني في المملكة الأردنية الهاشمية، بحيث تستطيع العمل على منع وتحديد المخاطر الإلكترونية والتخفيف منها وإزالتها بالسرعة الممكنة.

خامساً: توفير الدعم الحكومي لتعزيز الأمن السيبراني في مختلف القطاعات من خلال زيادة الميزانيات المخصصة للقطاعات، إضافة إلى العمل على استثناء الكوادر الوطنية ذات الكفاءات من موظفي قطاع الأمن السيبراني من هيكلة الرواتب بما يتواءم مع سوق العمل لضمان عدم هجرة الكفاءات والقدرة على إستقطاب خبرات جديدة في القطاعات الحكومية.

سادساً: تشجيع الإستثمار في مجالات الأمن السيبراني من خلال الحصول على إمتيازات تفضيلية لإنشاء الإستثمارات المحلية وإستقطاب الشركات الإقليمية والعالمية للإستثمار في المملكة مما يساهم في توفر فرص عمل وتأهيل خبرات على مستويات متقدمة في مجالات الأمن السيبراني.

سابعاً: التوجه لوضع معايير وضوابط وأطر عمل على مقدمي خدمات الأمن السيبراني في المملكة الأردنية الهاشمية لضمان جودة تقديم هذه الخدمات والحصول على الحد الأدنى المرجو من قيمة هذه الخدمات وإجراء آليات تقييم وتدقيق لاحق لضمان إلتزام مزودي الخدمات.

ثأمناً: سد الفراغ التشريعي في مجال مكافحة الجريمة السيبرانية، من خلال العمل على تغليظ العقوبات المقررة لمثل هذه الجرائم للحد والتقليل منها للوصول إلى فضاء سيبراني أكثر أماناً، إضافة إلى تطوير البنية التشريعية الجنائية الوطنية بما يتماشى مع الجهود الدولية في مكافحة الجرائم السيبرانية. والذي بدوره ينعكس على إبراز صورة مشرقة للمملكة إقليمياً ودولياً.

الخاتمة

مع تحول الدول و الإقتصاديات في جميع أنحاء العالم إلى التحول الرقمي لم يعد تبني هذا التطور والتحول أمراً إختيارياً، وكون المملكة الأردنية الهاشمية جزء من هذا العالم ما زالت تسعى نحو مواكبة التطورات التكنولوجية والإستفادة من الممارسات العالمية من خلال الفرص المتاحة بما يمكنها من التحول إلى الحكومة الرقمية الشاملة بإمتياز، حيث حرصت المملكة على إشراك جميع المواطنين وتمكينهم من الوصول للخدمات الرقمية الأساسية.

كما أن الرؤية الحالية للمملكة هي العمل على تنفيذ أو لويات الحكومة للأعوام (2021-2023) بشأن التحول الرقمي ودعم قطاع الإتصالات وتكنولوجيا المعلومات بهدف رقمنة الخدمات الحكومية المهمة، وبموجب هذه الخطة سيتم رقمنة 250 خدمة تساهم في خدمة 80 % من المواطنين، إضافة إلى أن التحول الرقمي له أثر إيجابي في ريادة الأعمال الرقمية و الإبتكار حيث يعمل على خفض نسبة البطالة من خلال دورها في إيجاد الوظائف المتعلقة بالأمن السيبراني.

وغير ذلك فأن تبني التحول الرقمي و التكنولوجي أصبح ضرورة عالمية وإقليمية لتعزيز الإقتصاد الرقمي والإستثمار به، فعلى الرغم من وجود بعض التحديات والعوائق في عملية التحول الرقمي إلا أن الحكومة تسعى إلى تهيئة البيئة التحتية الملائمة من خلال وضع الخطط و الإستراتيجيات لإدامة وتشجيع التحول الرقمي وإيصالها إلى كافة مكونات المجتمع، وفي ذات الوقت يعتمد نجاح هذا التحول على وجود تعاون كبير بين القطاعين العام والخاص، إضافة إلى وجود الرؤية والخبرة والدعم،

قائمة المراجع

أولا: التشريعات:

- الدستور الأردني،1952
- قانون الأمن السيبراني - رقم (16) لسنة 2019
- قانون الجرائم الإلكترونية لسنة 2015
- نظام المركز الوطني للأمن السيبراني لسنة 2020

ثانياً: الكتب والدراسات والأبحاث:

- الأمم المتحدة،الإسكوا،اللجنة الإقتصادية والإجتماعية 2015،الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية
- بانقا،علم الدين،2019،مخاطر الهجمات الإلكترونية السيبرانية وآثارها الإقتصادية:دراسة حالة مجلس التعاون الخليجي،المعهد العربي للتخطيط،ع63
- بوينس،آيرس،2017،المؤتمر العالمي لتنمية الاتصالات،الأرجنتين
- تقرير أعمال الحكومة الأردنية لسنة 2019
- جمعية الأنترنت،2020،المبادئ التوجيهية المتعلقة بأمن البيئة التحتية للإنترنت في الدول العربية
- حسين،حنين،2021،الإطار القانوني لخدمات الأمن السيبراني،رسالة ماجستير،جامعة الشرق الاوسط
- حمدان،سماح،20121،وعي أفراد الأسرة بمفهوم الأمن السيبراني خلال جائحة كورونا،المجلة العربية للعلوم الاجتماعية،ع124،مصر
- السدخان،ضحى،2021،مجلة العلوم الانسانية،مج5،ع1
- العابد،سكينة،2020،أمن المعلومات عبر شبكات التواصل الأجتماعي،المجلة العربية للمعلوماتية و أمن المعلومات،ع1

قائمة المراجع

- فيلالي،أسماء2018،تهديدات أمن المعلومات،مجلة البشائر الاقتصادية،مج4،ع3
- المشاقبة محمد،2020،أثر تطبيق سياسة الامن السيبراني على جودة المعلومات المحاسبية في البنوك الأردنية،رسالة ماجستير جامعة ال البيت
- مصطفى،صلاح،2020،ثقافة الأمن السيبراني،مجلة التنمية الأدارية،معهد الأدارة ،ع182،السعودية

ثالثاً: المقابلات:

- وحدة الجرائم الإلكترونية
- المركز الوطني للأمن السيبراني