د/ رحاب حسنى الرحماوى
مهندسة كهرباء اتصالات بالهيئة الوطنية للإعلام

إدارة المخاطر السيبرانية
فى المجـــال الاقتصـــادى

مقدمـة :

يشهد الاقتصاد العالمى عدة تحولات وتغيرات جَرَّاء الدخول إلى العالم الرقمى، فعلى مدى السنوات الثلاثين الماضية، ازداد اعتماد الحكومات والشركات والمواطنين على الإنترنت وعلى تقنيات المعلومات والاتصالات بشكل كبير، فكونت فضاءً سيبرانيًا يعكس ما تحتويه الدول من بيانات ومدخرات، ولكن على شكل معلومات رقمية عالية الحساسية، تُحاكى الواقع الاقتصادى لها، خاصةً تلك الدول التى انغمست بشكل كبير فى العمل المُحوسب، وانهمكت فى الحداثة المعلوماتية، الأمر الذى جعل منها ساحةً للصراعات السيبرانية وانعكس هذا الصراع على المجال الاقتصادى مع إمكان السيطرة عليه، والعبث بمحتوياته كما باتت الدول التى أنتجت هذه التكنولوجيا هى الأكثر تعرضًا للمخاطر السيبرانية، فضلًا عن صعوبة التزامها بمتطلبات الحفاظ على أمنها القومى.

تواجه كثير من الدول وما بها من مؤسسات وشركات مخاطر سيبرانية تؤثر على المجال الاقتصادى للدولة، مما جعلها تتشاطر مستوى من المسئولية فى إدارة هذه المخاطر، ولذلك أصبح على الدول والشركات أن تدرك أولاً أن إستراتيجيتها وأجندتها الرقمية ينبغى أن تكون قائمة على منهج منضبط لمواجهة وكيفية إدارة المخاطر السيبرانية بها. فالتراخى وعدم اتخاذ الإجراءات المناسبة له يُعرضهم لمخاطر جَمَّة. كما أنَّ الخطر السيبرانى آخذ بالازدياد بسبب توافر سوق للبرامج والأدوات الخبيثة والخدمات غير المشروعة والبيانات الحسَّاسة غير المُتاحة للعامة (وبأسعار ميسورة). لذلك أصبح تأمين البيانات يُشكل تحديًا كبيرًا أمام المجال الاقتصادى، وعلى الرغم من ذلك، فإن معظم المؤسسات لم تتخذ خطوات لتعزيز مهارات الأمن السيبرانى لديها.

كما أنَّ التحول السريع نحو اقتصاد رقمى عالمى، يؤدى إلى زيادة الهجمات السيبرانية يومًا بعد يوم وتصبح أكثر تعقيدًا وتأثيرًا، وهو ما يفرض علينا مواجهة وإدارة هذه المخاطر السيبرانية حتى نستطيع صياغة واقع اقتصادى رقمى جديد آمن، مما يُعزز أهمية تأمين الدول منظوماتها وكياناتها بشكل جيد والعمل على إدارة المخاطر السيبرانية فى المجال الاقتصادى لتحقيق الأمن القومى من خلال أسلوب إدارى لمواجهة هذه المخاطر السيبرانية حيث تعانى كثير من المؤسسات والمنظمات عدم القدرة الإدارية لمواجهة المخاطر السيبرانية، ومن هنا جاءت هذه الدراسة لإلقاء الضوء على كيفية إدارة المخاطر السيبرانية فى المجال الاقتصادى.

مشكلة الدراسة :

تكمُن مشكلة الدراسة فى تحديد المخاطر السيبرانية وآثارها السلبية على المجال الاقتصادى للدول وللمؤسسات

والمنظمات بها، خاصة أنَّ كثيرًا من الدول حاليًا تسعى إلى التحول الرقمى مما شكَّل مجالًا للاختراقات السيبرانية وتعرضها للهجمات السيبرانية التى تستلزم إدارة هذه المخاطر السيبرانية حتى لا تؤدى إلى خسائر فى المجال الاقتصادى للدول ولمؤسساتها ومنظماتها الاقتصادية ولتحقيق الأمن القومى.

أهمية الدراسة :

تأتى أهمية الدراسة من منطلق ما تُشكِّله المخاطر السيبرانية على المجال الاقتصادى للدول ومؤسساتها ومنظماتها من خطر يهدد أمنها القومى، خاصة مع تحول الحكومات للاقتصاد الرقمى، برزت المخاطر السيبرانية لتهدد تلك الإنجازات، ومن ثَمَّ وجب إلقاء الضوء على هذه المخاطر السيبرانية، وتأثيرها على المجال الاقتصادى للدول، وكيفية إدارة مخاطرها السيبرانية للدول، وداخل المنظمات والمؤسسات، لتحقيق الأمن القومى للدول.

هدف الدراسة :

الوصول إلى إستراتيجية مقترحة لإدارة المخاطر السيبرانية فى المجال الاقتصادى للدول.

منهج الدراسة :

تم اتباع المنهج الوصفي التحليلي فى تحليل كيفية إدارة المخاطر السيبرانية للمجال الاقتصادي، وتحديد تأثير المخاطر السيبرانية على المجال الاقتصادى للدول والمؤسسات والمنظمات بها، وذلك فى محاولة للإجابة عن التساؤل الرئيسي فى هذه الدراسة، ألا وهو:

كيف تستطيع الدول إدارة المخاطر السيبرانية فى المجال الاقتصادى لها ولمنظماتها ومؤسساتها لتحقيق الأمن القومى؟

ترتيبًا على ما تقدم تأتى هذه الدراسة حول إدارة المخاطر السيبرانية فى المجال الاقتصادى من خلال خمسة محاور على النحو التالى:

المحور الأول: الإطار النظرى والمفاهيمى للدراسة.

المحور الثانى: تأثير المخاطر السيبرانية على المجال الاقتصادى.

المحور الثالث: إجراءات إدارة المخاطر السيبرانية فى المجال الاقتصادى.

المحور الرابع: الملامح الرئيسية لإستراتيجية مقترحة لإدارة المخاطر السيبرانية فى المجال الاقتصادى.

المحور الأول :
الإطار النظرى والمفاهيمى للدراسة

أولًا: مفهوم المخاطر السيبرانية :

يُقصَد بالمخاطر السيبرانية أنها مخاطر تشغيلية على أصول المعلومات والتكنولوجيا التى لها عواقب تؤثر على سرِّية أو توافر أو سلامة المعلومات أو نظم المعلومات. مقارنة بفئات المخاطر التى يُغطيها التأمين. فإن المخاطر السيبرانية تتفق من حيث الخصائص والمسئولية، مع مخاطر كل من الممتلكات والخصوم، وكذلك المخاطر الكارثية والتشغيلية[١].

ثانيًا: تصنيف المخاطر السيبرانية :

تُصنَّف المخاطر السيبرانية فى المجال الاقتصادى إلى نوعين: مخاطر إجرائية ومخاطر تقنية كالآتى:

١- المخاطر الإجرائية :

أ- **المسئولية:** عدم وجود جهة مسئولة عن الفضاء السيبرانى وعن حماية المعلومات.

ب- **التصنيف:** غياب تصنيف المعلومات، الذى على أساسه تُصنَّف المعلومات على حسب أهميتها.

جـ- **السياسات الإستراتيجية:** عدم توافر سياسات وإستراتيجيات الفضاء السيبرانى، أو عدم العمل بها بشكل كامل إن كانت متوافرة.

د- **الكوادر البشرية:** عدم توافر الكفاءات والكوادر الوطنية المُدرَّبة وغياب الوعى بالأمن السيبرانى بين أطياف المجتمع[٢].

٢- المخاطر التقنية :

أ- **الفقدان:** وهو فقدان وضياع المعلومات نتيجة مسحها أو تلفها.

ب- **التدمير والتخريب:** هو تدمير المعلومات وتخريبها بأى وسيلة بسبب جهات داخلية أو خارجية والغرض منها منع الحصول على المعلومات نهائيًا.

جـ- **التسريب:** وهو تسرب المعلومات من مصدر الحفظ الرئيسى.

د- **التغيير:** وهو تعديل البيانات بغرض تزييفها أو إعطاء معلومات مغلوطة من شأنها تخريب المعلومات.

هـ- **التشويش:** وهو منع الوصول للمعلومات بشكل مؤقت.

و- **التقادم:** وهو عدم تحديث المعلومة لمدة من الزمن مما يؤدى إلى تقليل قيمة المعلومة وإعطاء نتائج غير دقيقة[٣].

ثالثًا: العلاقة بين الأمن السيبرانى والاقتصاد:

أصبحت العلاقة بين الاقتصاد والأمن السيبرانى علاقة متشابكة فى ظل عملية التحول الرقمى التى تتجه إليها العديد من الحكومات للاستحواذ على مقدرات الثورة الصناعية الرابعة، وأصبحت قضية مواجهة المخاطر السيبرانية خاصة فى المجال الاقتصادى فى ظل العصر الرقمى من القضايا الصاعدة، التى فرضت المزيد من المتغيرات الجديدة أمام الحكومات فى العديد من دول العالم، وظهرت مصالح جديدة وأخطار ذات طبيعة سيبرانية فى ظل الاعتماد المتزايد على الفضاء السيبرانى وتقديم الخدمات وتراكم الثروة، والأثر السلبى لانعدام أو ضعف الأمن السيبرانى على الاقتصاد خاصة الاقتصاد الرقمى.

وذلك فى إطار العلاقة الطردية التى تجمع بين كلا البُعدين، وتأثير ذلك فى معدلات الثقة فى البيئة الرقمية والعرض الرقمى والطلب الرقمى والبنية التحتية المعلوماتية، وبخاصة مع تزايد المخاطر السيبرانية فى البيئة الرقمية، وفى الوقت نفسه زيادة دور الاقتصاد الرقمى فى النمو الاقتصادى، مما دفع الدول إلى زيادة الإنفاق فى مجال الدفاع السيبرانى وتخصيص موارد فى الميزانية العامة للدولة أو فى ميزانيتها المعنية بالأمن والدفاع، وذلك فى ظل التحديات المتجددة التى تفرضها عمليات التحول الرقمى وتطبيقاته الاقتصادية، التى أدَّت إلى إحداث تغيير كمى ونوعى فى عناصر الثروة والموارد الاقتصادية ومرتكزات العرض والطلب.

ويؤكد المنظور الاقتصادى للأمن السيبرانى أن الفاعلين من حكومات أو شركات أو مستخدمين لديهم مطالب ومصالح أمنية مختلفة وفق طبيعة الاستخدام، وهذا التعارض فى الاهتمامات والمصالح يحتاج إلى أن يخضع إلى معايير للضبط الذاتى سواء عبر مراقبة البعض أو اتخاذ ردود الأفعال على أساس الحوافز التى تحرك دوافع كل طرف[٤].

رابعًا: إدارة المخاطر السيبرانية:

عادة ما يتم تقديم إدارة المخاطر السيبرانية كعملية، وتتكون المراحل مما يلى:

تحديد المخاطر، وتحليل المخاطر، وتقييم المخاطر، والمراقبة ومراجعة المخاطر.

فتتضمن إدارة المخاطر تطبيق طريقة منطقية ومنهجية لتحديد المخاطر، وتحليلها وتقييمها ومعالجتها ومراقبتها بطريقة تُمَكِّن المنظمات من تقليل الخسائر وتعظيم المكاسب، ويمكن تطبيق إدارة المخاطر على العديد من المستويات فى المنظمة؛ فيمكن تطبيقها فى المستوى الإستراتيجى والمستويات التشغيلية [٥].

ويُعَد إنشاء مسار لإدارة المخاطر الناشئة والاستجابة بسرعة وفعالية أمرًا بالغ الأهمية لضمان استجابة مبسطة وضمان التخفيف من أى خطر مُحتمل قدر الإمكان، وتنفيذ إستراتيجيات الاستجابة وعمليات الإدارة بشكل استباقى[٦] وتسير عمليات إدارة المخاطر وفقًا للخطوات التالية:

١- تحديد المخاطر السيبرانية:

تُحدد المؤسسة المخاطر السيبرانية المحتَملة التى قد تؤثر سلبيًا على عملية ما أو مشروع معين تقوم به، كما يجب تحديد بيئة الأعمال والعوامل المساهمة التى يمكن أن تسبب حدوث المخاطر السيبرانية والأسباب الجذرية للمخاطر السيبرانية، ووصف المخاطر وفهم الهدف من المخاطر والتهديدات التى تواجه المؤسسة. وجدير بالذكر أنه يتم دعم التقييم الاستباقى من خلال البيانات ذات الصلة والاتجاهات والأحداث الجارية[٧]، ويمكن تحديد المخاطر من مجموعة من المصادر كالآتى:

أ- تبادل الأفكار باستخدام أفراد عمليات ذوى خبرة.
ب- تطوير سيناريوهات المخاطر.
جـ- برامج تحليل البيانات.
د- استقصاءات السلامة ومراجعات السلامة فى مراقبة العمليات.
هـ- بيان التحقيقات فى الحوادث.
و- العوامل التنظيمية، مثل سياسات المؤسسة أو المنظمة أو الشركة للتوظيف والتدريب، المكافآت وتخصيص الموارد.
ز- عوامل البيئة التشغيلية، مثل الضوضاء والاهتزازات المحيطة، درجة الحرارة والإضاءة ومعدات الحماية، العوامل البشرية مثل الحالات الطبية، وقيود الأداء البشرى، وواجهة الإنسان والآلة.
ح- عوامل الامتثال التنظيمى مثل انطباق اللوائح واعتماد المعدات والأفراد والإجراءات.

- أدوات تحديد المخاطر السيبرانية المحتَملة:

قوائم المراجعة، والدراسات الاستقصائية، وعمليات التفتيش الشخصية، وآراء الخبراء التى تعتمد على وعى الخبير وإدراكه مدى حجم الخطر، وطريقة تداول الأفكار؛

بمعنى عمل توليفة مما سبق للوصول إلى أفضل النتائج، ومن وسائل تحديد المخاطر أيضًا العصف الذهنى- *SWOT*-استبيانات المخاطر- ورش العمل - تحليل المخاطر - تقييم المخاطر- سياسات علاج المخاطر- مراقبة ومتابعة الخطر[٨] .

٢- تحليل المخاطر السيبرانية :

يُعَد تحليل المخاطر الخطوة التالية فى عملية إدارة المخاطر، ولكن يمكن أن يكون أيضًا الخطوة الأولى إذا كانت هناك مخاطر تم تحديدها بوسائل أخرى غير تقييم المخاطر، أما الغرض الأساسى من تحليل المخاطر فهو التقييم، فبمجرد تحديد أنواع محددة من المخاطر، تحدد المؤسسة تصنيفها وأولوياتها وضوابطها ومستويات الخطر، وبعد ذلك احتمالات حدوثها وكذلك عواقبها، والهدف من تحليل تلك المخاطر زيادة فهم كل حالة محددة من المخاطر، وكيف يمكن أن تؤثر على الأهداف الاستراتيجية للمؤسسة.

يمكن توضيح الخطوات الخمس[٩] لعملية تحليل المخاطر فيما يلي:

أ- وصف واضح للمخاطر:

يجب أن يكون هناك بيان موجز يصف ماهية المخاطر السيبرانية، وكيف يمكن أن تؤثر على تحقيق الأهداف، ويجب أن يتفق فريق مراجعة المخاطر على نطاق المخاطر ثم وصف سيناريو المخاطرة، مما يوضح ما يبدو عليه حدث الخطر المحتمل.

ب- أسباب المخاطر:

وتعنى «لماذا يحدث هذا الخطر؟» بصرف النظر عن الأسباب المباشرة للمخاطر، نحتاج أيضًا إلى فهم جيد للأسباب الأساسية الجذرية والمحركات الرئيسة؛ من أجل تقليل احتمالية المخاطر بشكل فعال.

جـ- الضوابط الوقائية :

بمجرد أن نفهم الأسباب الجذرية، نحتاج إلى الاتفاق على الضوابط الموجودة بالفعل التى تساعد فى تقليل احتمالية حدوث هذه الأسباب أو الدوافع، وتحديد الضوابط الإضافية التى يمكننا وضعها لتقليل الاحتمالية بشكل أكبر؛ فالمنظمات التى تتبع إستراتيجية استباقية لإدارة مخاطر السلامة تعتقد أنه يمكنها التقليل من المخاطر السيبرانية من خلال تحديد نقاط الضعف، واتخاذ الإجراءات اللازمة للحد من العواقب السلبية للمخاطر الناشئة.

د- عواقب المخاطر:

وتعنى ماذا سيكون الأثر إذا تحققت هذه المخاطر؟ فإن تحديد هذه العواقب المحتملة مقدمًا يساعد فى وضع خُطط للطوارئ فى حالة حدوث خطر.

هـ- الضوابط المخففة :

- ما الضوابط التى يجب تطبيقها، والتى من شأنها أن تساعد فى تقليل تأثير العواقب؟
- ما الضوابط الإضافية التى يمكن وضعها لتقليل التأثير بشكل أكبر؟

٣- تقييم المخاطر السيبرانية :

يجب على الإدارة المعنية تنفيذ إجراءات تقييم المخاطر السيبرانية بحد أدنى فى الحالات الآتية:

أ- فى المراحل الأولى من المشاريع التقنية.
ب- قبل إجراء تغيير جوهرى فى البنية التقنية.
جـ- عند التخطيط للحصول على خدمات طرف خارجى.
د- عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

ويتضمن تقييم المخاطر الآتى:

التهديد والضعف، كما يحلل ويأخذ فى الاعتبار عوامل التخفيف المعمول بها[١٠] ، والغرض من عنصر تقييم المخاطر هو تحديد الآتى:

أ- التهديدات الموجَّهة للمنظمات أى العمليات أو الأصول أو الأفراد أو التهديدات الموجَّهة من خلال منظمات ضد منظمات أخرى.
ب- نقاط الضعف داخل وخارج المنظمات.
جـ- الضرر (أى التأثير المعاكس) الذى قد يحدث فى ضوء احتمالية حدوث التهديدات.
د- احتمال وقوع الضرر.

يقوم الممارس بتحليل المخاطر السيبرانية لتحديد احتمالية أن تؤدى أحداث التهديد والظروف المعرضة للخطر إلى تأثيرات ضارة على أصل النظام، وبالمثل يقوم الممارس بتحليل قيمة التأثير وحساب مخاطر التعرض باستخدام المنهجية المحددة فى إستراتيجية مخاطر المؤسسة مثل (احتمالية المخاطرة X تأثير المخاطر) لذا، فإن تحليل السبب الجذرى (التفكير فى الأحداث السابقة التى أدَّت بالفعل إلى حدث ما) يساعد فى النظر إلى العواقب المحتملة للأحداث المستقبلية، كما يساعد فى توثيق تسلسل النتائج التى يمكن أن تنشأ بعد بدء حدث تهديد، وبينما يُعَدُّ حكم الخبراء ذا قيمة فى تقدير عوامل

الخطـر، إلا أن هنـاك طريقـة واحـدة لتقليـل الذاتيـة هى استكمال هذا الحكم باستخدام نماذج المحاكاة.[١١]

يجب إعادة تقييم المخاطر السيبرانية وتحديثها على النحو التالى:

أ- دوريًا لجميع الأصول المعلوماتية والتقنية، وسنويًا على الأقل للأنظمة الحسّاسة.

ب- بعـد وقـوع حـادث متعلق بالأمـن السـيبرانى ينتهك سلامة الأصول المعلوماتية والتقنية وتوافرها وسرّيتها.

جـ- بعد الحصـول على نتائـج تدقيق مهّمـة أو معلومات استباقية.

د- فى حال التغيير على الأصول المعلوماتية والتقنية.

ويجب أن تغطى عملية تقييم المخاطر السيبرانية ما يلى:

أ- **تحليـل المخاطر السـيبرانية:** يجب أن تُقيّم (الإدارة المعنيـة بالأمن السـيبرانى) احتماليـة وقوع المخاطر والتهديـدات والآثار الناتجة عنها، وأن تسـتخدم نتائج هـذا التقييم لتحديد المسـتوى العام لهـذه المخاطر، ويجـب أن تعتمد (الإدارة المعنية بالأمن السـيبرانى) منهجية كميّة أو نوعيّة لإجراء تحليل المخاطر.

ب- **تقدير المخاطر السيبرانية:** يجب أن تُقَدِّر (الإدارة المعنية بالأمن السيبرانى) حجم المخاطر السيبرانية بالتوافق مع معايير تقدير المخاطر المؤسسية المعتمدة فى «اسـم الجهة» وتحديد أساليب التعامل معها حسب الأولوية[١٢].

٤- المعالجة أو الاستجابة للمخاطر السيبرانية:

تتضمن الاسـتجابة للمخاطر السيبرانية تحديد مجموعة الخيـارات لمعالجة المخاطر وتقييمها وإعداد خُطط معالجة المخاطر وتنفيذها، وتشـمل تلك الخيارات تجنُّب المخاطر، وتقليـل احتمالية الحدوث، وتقليل العواقـب، ونقل المخاطر، والاحتفاظ بالمخاطر[١٣].

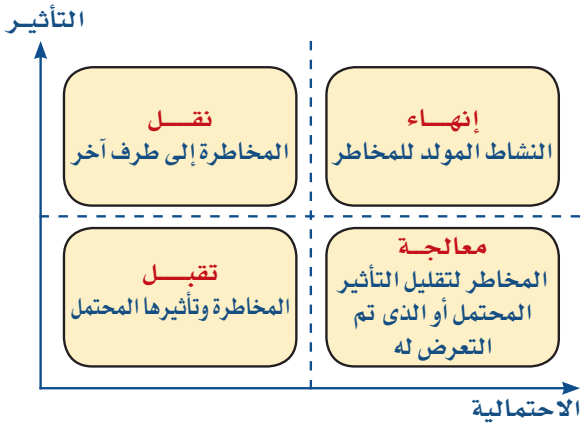
ويجـب أن تحـدد (الإدارة المعنيـة بالأمن السـيبرانى) خيارات معالجة المخاطر السيبرانية حسب الخطوات التالية:

أ- **معالجـة المخاطـر أو تقليلهـا:** معالجـة أو تقليـل درجـة الخطـر من خلال تطبيق الضـوابط الأمنية اللازمة لتقليل احتمـال الحـدوث أو التأثيـر أو كليهمـا، التـى تسـاعد فى احتواء المخاطر والمحافظة عليها ضمن مستويات مقبولة.

ب- **تجنُّب المخاطـر:** التخلص مـن الخطـر بتجنـب الاستمرار بمصدر الخطر عن طريق عمل الآتى:

- **مشـاركة المخاطر أو تحويلها:** مشاركة المخاطر مـع طـرف ثالث لديـه الإمكانـات فـى التعامل مع المخاطـر بشـكل أكثـر فاعليـة، أو التأميـن علـى الأصـول المعلوماتيـة والتقنيـة فى حال تعرضـها لمخاطر سيبرانية.
- **تقبُّـل المخاطـر وتحمُّلها:** مسـتوى الخطـر مقبول ولكن يجب المراقبة باستمرار فى حال حدوث تغيير.

وتشـمل خيارات الاستجابة للمخاطر السيبرانية كلاً من: التسـامح وهى مناسـبة فقط عندما يكون من الممكن قبولها حين تكون الخسارة أو الضرر قد حدث / الاحتفاظ، والمعالجة / التقليل، والنقل (وتسـتند إلى إعطاء توجيهات للناس حول كيفيـة التأكـد مـن عدم حـدوث خسـائر، لكنهـا تعتمد على الأشـخاص الذين يتبعون أنظمة عمل آمنة راسخة)، والإنهاء والتجنـب (من خلال تنفيذ الضـوابط الوقائية المناسـبة)، وتنتقد الاسـتجابة للمخاطر على أنها قيادة تصـحيحية حتى الآن أكثر من كونها وقائية كما فى الشكل التالى.



شكل يوضح خيارات الاستجابة للمخاطر[١٤]

خلال هذه الخطـوة تقوم المؤسسـة بتقييم المخاطر السـيبرانية الأعلـى تصـنيفًا، والتعامـل معهـا بإيجابية، ووضـع خطـة لتخفيفهـا باسـتخدام ضـوابط محـددة للمخاطر، وتشـمل هذه الخطط عمليات تخفيف المخاطر وتكتيكات الوقاية من المخاطر، وخطط الطوارئ فى حالة ظهور المخاطر[١٥].

٥- متابعة المخاطر السيبرانية:

هى جزء من خطة التخفيف تقوم على متابعة كل المخاطر السـيبرانية من رصـد، وتتبع الجديدة منها والحالية بشـكل مستمر، بالإضافة إلى مراجعة عملية إدارة المخاطر الشاملة وتحديثهـا وفقًـا للمواقف المختلفة والمتغيـرة، وتتم مراجعة المخاطر على أسـاس ربع سـنوى وتحديد المخاطر الجديدة والتغييـرات القائمـة، وتحديـث سـجل المخاطـر، وتقييـم

الإجراءات التى يتخذها أصحاب المخاطر لإدارة المخاطر وتصحيح الأداء غير اللائق[١٦].

ولمتابعة المخاطر السيبرانية يجب أن تُعد «الإدارة المعنية بالأمن السيبرانى» سجلاً للمخاطر، وأن تحافظ عليه لتوثيق مخرجات عملية إدارة المخاطر السيبرانية، على أن يشتمل بحد أدنى على المعلومات التالية:

أ- عملية تحديد المخاطر.
ب- نطاق المخاطر.
جـ- المسئول أو صاحب المخاطر.
د- وصف للمخاطر بما فى ذلك أسبابها وآثارها.
هـ- تحليل للمخاطر يُوضح التأثيرات الناتجة عن المخاطر ونطاقها الزمنى.
و- تقييم وتصنيف للمخاطر يشتمل على احتمالية المخاطر وحجمها وتصنيفها الإجمالى فى حال حدوثها.
ز- خُطة التعامل مع المخاطر تتضَمَّن إجراء التعامل معها والشخص المسئول عنها وجدولها الزمنى.
ح- وصف الخطر المتبقى.
ط- يجب على «الإدارة المعنية بالأمن السيبرانى» جمع الأدلة المتعلقة بحالة المخاطر السيبرانية ومراجعتها بشكل دورى.

٦- مستوى المخاطر السيبرانية المقبول:

وتتم كالآتى:

أ- يجب تحديد معايير تقبّل المخاطر السيبرانية وتوثيقها، وفقًا لمستوى المخاطر، وتكلفة معالجة الخطر مقابل تأثيره، من خلال تحديد مدى تأثير الخطر، حيث يتم تصنيف كل خطر[١٧] بإحدى الحالات الآتية:

- مخاطر ذات تأثير جسيم، ويجب وضع الإجراءات والخطط لمواجهتها.
- مخاطر ذات تأثير كبير، وتحتاج إلى دراسة ووضع خطط.
- مخاطر ذات تأثير متوسط، والتى يمكن أخذه بعين الاعتبار.
- مخاطر ذات تأثير منخفض، ولا تتطلب خططًا محددة لها.
- مخاطر ذات تأثير منخفض جدًا، ولا تتطلب وضع خطط محددة لها.

ب- يجب تطبيق ضوابط إضافية من أجل تقليل المخاطر إلى مستوى مقبول فى حال عدم استيفاء الخطر المتبقى لمعايير تقبّل المخاطر.

جـ- فى حال تجاوز معايير تقبّل المخاطر، يتم التصعيد لصاحب الصلاحية لاتخاذ الإجراءات أو القرارات اللازمة.

د- يجب تحديث إجراءات إدارة مخاطر الأمن السيبرانى على فترات زمنية مخطط لها (أو فى حال حدوث تغييرات فى المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة).

هـ- يجب المراجعة السنوية لسياسة إدارة مخاطر الأمن السيبرانى.

٧- مراقبة المخاطر السيبرانية:

تقوم على رصد المخاطر الجديدة وما تم إنجازه بشكل مستمر لإضافته لعملية إدارة المخاطر السيبرانية بشكل دائم[١٨].

الغرض من مكون مراقبة المخاطر هو كالآتى:

أ- تحديد الفاعلية المستمرة للاستجابات للمخاطر (بما يتفق مع إطار المخاطر التنظيمية).

ب- تحديد التغييرات التى تؤثر على المخاطر والبيئات التى تعمل فيها الأنظمة.

جـ- التحقق من تنفيذ استجابات المخاطر المخطط لها، واستيفاء التشريعات والتوجيهات واللوائح والسياسات والمعايير والمبادئ التوجيهية[١٩].

المحور الثانى
تأثير المخاطر السيبرانية على المجال الاقتصادى

زادت العلاقة بين الأمن والتكنولوجيا، ومعها تزايد إمكان تعرُّض المصالح الاستراتيجية للدولة للمخاطر السيبرانية، بل وهددت بتحول الفضاء السيبرانى لوسيط، ومصدر لأدوات جديدة للصراع الدولى[٢٠].

وتمثل أبرز المخاطر السيبرانية على المجال الاقتصادى منها الآتى:

١- التلاعب بالمعلومات الموجودة فى نظام معين، وتشويهها أو إتلافها، سواء عبر الاختراق أو نشر الفيروسات.

٢- الجرائم العادية التى تستخدم الإنترنت، للسرقة والغش وسرقة الهويات، والاعتداء على الملكية الفكرية وغيرها.

٣- الجرائم التى تندرج فى إطار الجريمة المنظمة، التى تهدد أمن الأفراد والدول، كتبييض الأموال والإرهاب...إلخ، كالتهديدات الأمنية الخاصة بنظام

الفدية، وهى أداة إجرامية انتشرت عبر الإنترنت لعدة سنوات، مستمرة فى التطور وتشمل كلًا من الأفراد والاقتصادات على المستوى الفردى.

٤- مخاطر التقنيات الذكية مثل العملات الرقمية التى قد تؤدى لانهيار الاقتصاد، وتسهيل ارتكاب الجرائم حيث يصعُب تتبعها لأنها مُشفَّرة وتسهل عملية غسيل الأموال، وكذلك استخدام الهندسة الاجتماعية وهى إحدى وسائل النصب فى معرفة الحسابات البنكية من الفرد المستهدَف نفسه.(٢١)

٥- قد تستهدف الهجمات السيبرانية توقف الإنترنت كليًا فى الدولة المُستهدَفة، مما يؤدى لتوقف المعاملات البنكية، ومعاملات الحكومة الإلكترونية وسرقة أرقام وتفاصيل بطاقات الائتمان التى يتم التسوق بها عبر الإنترنت، مما ينتج عن ذلك تعطل تدفق الأموال فى الدولة، وبالتالى توقف أهم القطاعات فى الدولة مثل الصناعة وغيرها من قطاعات الدولة، ومن الممكن أن تفشل المعاملات نظرًا لحبس السيولة، وأن تفقد الأسر والشركات قدرتها على النفاذ إلى الودائع والمدفوعات، وفى مثل هذا السيناريو الحاد، قد يطالب المستثمرون والمودعون بأموالهم أو يحاولون إلغاء حساباتهم أو غير ذلك من الخدمات والمنتجات التى يستخدمونها فى العادة.

٦- أصبحت أدوات القرصنة الآن أقل تكلفة وأكثر سهولة وأشد قوة، مما يتيح للقراصنة ذوى المهارات المحدودة إلحاق ضرر أكبر مقابل نسبة ضئيلة من التكلفة السابقة، ويؤدى التوسع فى الخدمات القائمة على الأجهزة المحمولة (وهى المنصة التكنولوجية الوحيدة المتاحة للكثيرين) إلى زيادة فرص القرصنة، ويستهدف المهاجمون المؤسسات الكبيرة والصغيرة والدول الغنية والفقيرة، ويعملون عبر الحدود، ولذلك يجب أن تكون محاربة الجريمة السيبرانية والحد من مخاطرها مسئولية مشتركة عبر البلدان وفى داخلها(٢٢).

٧- من الممكن أن تشن جهات فاعلة منفردة هجمات سيبرانية لسرقة الأموال من حسابات بنكية فردية، وكذلك يمكن للدول المتنافسة والمعارضين الأيديولوجيين أن يهدفوا إلى الحصول على بيانات سرية، والتسبب فى اضطرابات فى النظم المالية وإثارة الذعر بين المواطنين.

نظرًا لتعرُّض المنظومة الاقتصادية فى الدول لمثل هذه المخاطر كان لابد من وجود الأمن القومى الاقتصادى، حيث إنه أكثر القطاعات الأمنية عُرضةً للهجمات السيبرانية، نظرًا لتحول الاقتصاد العالمى لاقتصاد رقمى معتمد على تكنولوجيا المعلومات، وبالتالى تعرض تلك المنظومة لمثل هذه المخاطر قد يتسبب فى خسائر اقتصادية وقومية هائلة مما يؤثر على تحقيق الأمن القومى للدولة مما يستلزم العمل على إدارة المخاطر السيبرانية فى المجال الاقتصادى(٢٣).

المحور الثالث

إجراءات إدارة المخاطر السيبرانية فى المجال الاقتصادى

أولاً: الإجراءات الفنية:

يمكن حماية مصادر المعلومات الحساسة من الأخطار السيبرانية عن طريق إبقائها بعيدة عن الأنظار، أو بعيدة عن أعين المعتدين، وذلك باتباع الإجراءات الآتية:

١- **الحماية المادية:** وتشمل ما يلى:

أ- الرقابة السيبرانية التى لا تتيح فرصة لنفاذ (الهاكرز).

ب- كاميرات الرصد والمراقبة التى يتم وضعها فى أماكن مختلفة من البناء.

جـ- الحراسة المشددة التى لا تتيح أى فرصة للوصول للمعلومات.

٢- **التشفير:** تتم عن طريق خلط المعلومات الرقمية، بحيث لا يمكن إعادة ترتيبها إلا باستخدام مفتاح معين، وتكون المعلومات المخلوطة غير مفهومة بتاتًا للشخص الذى لا يملك هذا المفتاح، وتُعرَف عملية الخلط هذه بالتشفير، أما عملية إعادة الرسالة المشفرة على وضعها الأصلى فتُعرف بفَك الشفرة وإرجاعها.

٣- **الحماية عن طريق المكونات:** توفر هذه الطريقة حماية شبه كاملة ضد الفيروس، وذلك باستخدام أجهزة دون الذاكرة المستخدمة، كما يمكن استخدام الأقراص الضوئية فى تخزين البرامج تخزينًا دائمًا، وهذه الأقراص تكون للقراءة فقط، ولا يمكن الكتابة عليها، وكذلك تخزين نظم التشغيل على هذه الأقراص، حيث إنَّ ذلك يوفر لها الحماية ضد الفيروسات.

٤- **الترشيح:** من الطرق التى تلجأ إليها كثير من الجهات للتستر من وراءها ما يُعرف بالترشيح وهى طريقة للحصول على معلومات منتقاة من معلومات سرية دون الكشف عن المعلومات السرية نفسها.

٥- **مراقبة التخلص من النفايات المعلوماتية:** يجب تطبيق هذا الإجراء بدقة وحذر لتفادى المخاطر السيبرانية لأنَّ هناك برامج وأساليب وطرقًا يمكن بها استرجاع البيانات من وسائط التخزين بعد مسحها[٢٤].

ثانيًا: الإجراءات الإدارية:

تشدد كل الدول فى الحفاظ على معلوماتها وحمايتها من التعرض للسرقة والتخريب، وقد حَتَّم عليها هذا الحرص أن تتخذ بالإضافة للإجراءات الفنية، بعض الإجراءات الإدارية فى مراكزها، وأجهزتها، وعلى أفراد العاملين، وتتمثل بعض هذه الإجراءات فى الآتى:

١- **تحديد المسئوليات:** تقع مسئولية توفير الحماية للمعلومات وتلافى الأخطار السيبرانية على ثلاث جهات مهمة تتمثل فى: رئيس المعلومات، مدير الأمن السيبرانى، وضابط الأمن السيبرانى، وذلك على النحو التالى:

أ- **رئيس المعلومات:** يطبق إجراءات الأمن بدقة لضمان سرية معلومات المنشأة، وله القدرة على مسح ما يشاء من معلومات، ووضع تعليمات الاستخدام وإعطاء الصلاحية.

ب- **مدير الأمن السيبرانى:** مهمته التحكم فى محتويات المركز وأيضًا مسئول عن أجهزة التشفير.

جـ- **ضابط الأمن السيبرانى:** مسئول عن اختيار البرامج وفحصها، والتأكد من خلوها من الفيروسات، أو التشفيرات التى يمكن أن يستفيد منها العدو أو العابثون.

٢- **تحديد الصلاحيات:** من الصعوبات التى تواجه حماية المعلومات وصول أشخاص من داخل المنشأة أو خارجها إلى مراكز المعلومات، لذا يجب تحديد الصلاحيات للأشخاص المُصرَّح لهم بالوصول واستخدام المعلومات وقواعد البيانات، وكذلك وضع قواعد تحدد الأشخاص أو المجموعات التى لها حق الوصول إلى نوع معين من المعلومات، وهذا يتطلب تقسيم الملفات داخل شبكة الكمبيوتر إلى أقسام معينة، بحيث لا يمكن لأى شخص الوصول إلى قسم غير مصرح له، وهذا يساعد كثيرًا فى حماية المعلومات من وصول المخربين.

٣- **حماية الأفراد:** يتعرض العاملون فى مراكز المعلومات لهجمات مدبَّرة من العدو بغرض شَلّ قدرتهم على حماية معلوماتهم، وعليه لابد من حماية هؤلاء الأفراد وتحصينهم ضد أفكار وإجراءات الحرب النفسية التى يشنها العدو، وترسيخ تمسكهم بمبادئهم.

٤- **صيانة الأجهزة:** يجب مراقبة عمال الصيانة التابعين للشركة المُصنِّعة، أو التى تقوم بتركيب النظام بصورة مستمرة عند السماح لهم بالوصول إلى مراكز المعلومات فى أثناء الصيانة، ويتم التغلب على هذه المشكلة باستبدال عمال صيانة الشركة بأفراد من المنشأة يتم تدريبهم للقيام بأعمال الصيانة[٢٥].

المحور الرابع
الملامح الرئيسية لإستراتيجية مقترحة لإدارة المخاطر السيبرانية فى المجال الاقتصادى:

هدف الاستراتيجية المقترحة:

تحقيق نمو اقتصادى آمن بمصر وتأمينه من أى مخاطر سيبرانية.

مرتكزات الاستراتيجية المقترحة:

تقوم الاستراتيجية المقترحة على عدة مرتكزات من أهمها:

١- السماح لشركات عالمية فى هذا المجال بالدخول فى السوق المصرية وتقديمها العديد من الخدمات المتطورة.

٢- تحتل مصر المركز الرابع بين دول الشرق الأوسط وشمال إفريقيا والـ ٢٣ عالميًا فى الأمن السيبرانى من بين ١٨٢ دولة بدرجة ٩٥,٤٥ من ١٠٠.

٣- تأسيس المجلس الأعلى للأمن السيبرانى ومركز إيجى سيرت للاستجابة لطوارئ الإنترنت والحاسب.

٤- عضوية مصر فى بعض الاتحادات الدولية والهيئات المختصة بالأمن السيبرانى.

٥- تماسك وجاهزية القوات المسلحة وإنتهاجها نهج الجيوش الإلكترونية الحديثة وذلك لتصديها لتهديد الأمن المصرى المستحدث والمعتمد على الفضاء السيبرانى.

٦- تنظيم البنك المركزى المصرى لاستخدام العملات الرقمية ومنع تداولها.

٧- إحداث تغيير فى طبيعة بيئة الأعمال لكل القطاعات الاقتصادية حيث تضاعف الطلب على تكنولوجيا التأمين للأمن السيبرانى ضد المخاطر السيبرانية.

محددات الاستراتيجية المقترحة:

تقوم الاستراتيجية المقترحة على عدة محددات من أهمها:

١-التحول للاقتصاد الرقمى أصبح وسيلة تساعد أكثر فى الاختراق والهجوم السيبرانى.

٢-الارتفاع النسبى فى تكلفة تطبيق تقنيات أمن نظم المعلومات والفضاء السيبرانى بصورة ملحوظة.

٣- صعوبة تطبيق ضوابط أمن نظم المعلومات والفضاء السيبرانى نظرًا لضعف ثقافة الأمن السيبرانى لدى بعض العاملين فى بعض القطاعات خاصة المالى والمصرفى.

٤-الحاجة إلى وجود آلية رقابة واضحة على جميع القطاعات خاصة البنوك والشركات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبرانى وإدارة مخاطره.

٥-التخلف والجهل والأمية، وضغوطات النمو التى تقع على كاهل المجتمع بالفقر والأمية والجريمة كل ذلك يُحد من فرص الانتقال إلى المجتمع المعلوماتى والسيبرانى فلابد من تطور البنى الاقتصادية حتى تتمكن المجتمعات من دخول المجتمع المعلوماتى والسيبرانى بيُسر.

٦-نقص الكفاءات على مستوى بعض القيادات الإدارية بسبب عدم التأهيل وهجرة العقول شَكَّل تحديًا كبيرًا.

أهم السياسات التنفيذية للإستراتيجية المقترحة:

أولا: على المستوى الإقليمى والدولى:

١- صياغة استراتيجية دولية وأخرى عربية مشتركة لمواجهة تصاعد الأخطار السيبرانية، وتعزيز أمن الفضاء السيبرانى والتعاون فى مجالات مكافحة المخاطر السيبرانية، بحيث تتم صياغتها بتعاون وتنسيق من قبل مراكز الدراسات والمؤسسات الرسمية المعنية.

٢-تفعيل تقنية التوقيع الرقمى لحماية أموال البنوك والمؤسسات.

٣-استخدام الذكاء الاصطناعى فى مواجهة المخاطر السيبرانية حيث أصبح هناك ذكاء اصطناعى يواجه ذكاء اصطناعيًا.

٤-تطوير برامج حماية إلكترونية لمواجهة الهجمات السيبرانية، وفى سبيل ذلك عقدت شراكات بين الدول والقطاع الخاص فى كل دولة لتطوير البنية التحتية.

٥- إعداد برامج توعوية حول الأمن السيبرانى يتم تقديمها وبثها بطريقة واضحة ومبسطة لعامة الناس.

٦- إعادة النظر فى القواعد القانونية الدولية التى تنظم هذا النوع من الحروب، وضرورة بلورة توافق دولى بهذا الخصوص.

٧- ضرورة أن تعمل الدول على تأمين منظوماتها، وكياناتها بشكل جيد، والإبلاغ عن الحوادث السيبرانية، والمشاركة الفعالة للمعلومات، وذلك لتعزيز قدرة السلطات فى جميع أنحاء العالم على إدارة الحوادث بفاعلية، حيث يُعَد نموذج الإبلاغ عن الحوادث، ومشاركة المعرفة الذى يتم العمل عليه من قبل مجلس الاستقرار المالى (***The Financial Stability Board***) خطوة مهمة لتعزيز الأمن السيبرانى.

٨- تطوير القدرات الوقائية: ينبغى مساعدة الاقتصادات النامية والبلدان المنخفضة الدخل فى تعزيز الاستقرار المالى ودعم الشمول المالى، وذلك عبر ضمان الاستفادة من التكنولوجيا بشكل يحفظ الأمن والسلامة ضد المخاطر السيبرانية.

ثانيًا: على المستوى المحلى:

١- إنشاء مركز أمن اقتصادى سيبرانى للتعامل السريع مع أى مشكلة اقتصادية، وهذا يختلف عن إدارة للأمن السيبرانى، ولكن هذه الإدارة تكون على ربط مع هذا المركز، وهذا يرجع لأهمية المجال الاقتصادى حيث هو مجال حساس يمكن أن يؤثر على باقى مجالات الدولة.

٢- التوعية الاقتصادية والثقافة الأمنية لرجال الأعمال والمستثمرين لمواجهة أى مخاطر سيبرانية متمثلة فى عمليات ابتزاز واختراقات، وكيفية التعامل مع هذه الأوضاع.

٣- تفعيل الإنترنت الفائق السرعة حيث له دور كبير فى التنمية الاقتصادية.

٤- الشراكة بين القطاع العام والخاص فيما يخص تبادل المعلومات حول المخاطر السيبرانية المختلفة.

٥- محو أمية التقنية المالية، ونشر الوعى الرقمى فى المجتمع.

٦- تخصيص هياكل للردع السيبرانى، وهو ما نَصَّت عليه المادة ١٤ من اتفاقية بودابست للإجرام المعلوماتى حيث يسمح ذلك بالمواجهة السريعة لأى هجوم سيبرانى.

٧- تطوير استراتيجيات الاستجابة حيث يجب أن يكون النظام المالى قادرًا على استئناف عملياته بسرعة.
٨- تفعيل استراتيجية الردع السيبرانى حيث يجب خفض تكلفة الهجمات السيبرانية والحد من خطرها عبر إجراءات ردعية فعالة.
٩- استخدام وسائل الإعلام مثل التليفزيون والراديو للتوعية عن حماية البيانات الشخصية.
١٠- استحداث هيئة، وهى جهة تنظيمية مستقلة وطنية للإنترنت، تتضمن منصة أمان عبر الإنترنت بكمية هائلة من المحاكاة للمعلومات والموارد؛ لمساعدة المجتمع ولتعزيز المسئولية عبر الإنترنت، والمرونة لبناء ثقافة إيجابية، وتتمثل مهمتها فى الترويج للسلامة الرقمية من خلال تعزيز الثقافة الإيجابية حول المواطنة الرقمية، ومن مهامها أيضًا احتواؤها نظام شكاوى مكثفًا لمساعدة المجتمع؛ فإذا لم يلتزم موقع التواصل الاجتماعى بامتثال المعايير الواردة فى مدونة قواعد الممارسة، فيمكن للفرد أن يلجأ إلى مفوض السلامة الرقمية، الذى يمكنه توجيه موقع التواصل الاجتماعى للامتثال للمعايير الواردة فى المدونة. مع رفع مستوى الوعى العام حول الأمن السيبرانى باعتماد جهود الوقاية الاستباقية.

الخلاصة :

تناولت الدراسة مشكلة المخاطر السيبرانية فى المجال الاقتصادى خاصة للمؤسسات والمنظمات بالدول، وأجابت عن تساؤل مهم وهو كيف تستطيع الدول إدارة المخاطر السيبرانية لها ولمنظماتها ومؤسساتها فى المجال الاقتصادى؟، وأشارت الدراسة إلى الإجراءات والسياسات المطلوبة لإدارة المخاطر السيبرانية فى المجال الاقتصادى، وقد خَلُصَت الدراسة إلى النتائج الآتية :

١- التطور السريع فى التكنولوجيا أسهم فى زيادة حجم المخاطر السيبرانية أمام الدول، حيث يكشف عن نقاط ضعف أكبر، وأدوات أرخص وأسهل للمهاجمين، وفى حين أصبحت بعض الشركات المالية والهيئات التنظيمية أكثر وعيًا واستعدادًا للهجمات السيبرانية، فإن الثغرات السيبرانية لا تزال كبيرة وما زالت تمثل تحديًا أمام المؤسسات والدول.
٢- تزايد عدد الهجمات السيبرانية خلال العقدين الأخيرين، حتى باتت إحدى أهم الوسائل والتكتيكات المعتمدة بين الأطراف المتصارعة حول العالم، وذلك نظرا لتدنى كلفتها والخسائر التى قد تنجم عنها للطرف المهاجم مقارنة مع حجم ما يمكن تحقيقه وإلحاقه من أضرار بالخصم عبر توظيفها.
٣- هناك العديد من الإجراءات الفنية والإدارية المتاحة لمجابهة وإدارة المخاطر والهجمات السيبرانية فى الفضاء السيبرانى والتصدى لها، وأن الالتزام بتطبيق وتفعيل أكبر قدر منها يمكن أن يكون معينًا إلى حد بعيد فى التصدى لهذه الهجمات بل والعمل على إدارة مخاطرها السيبرانية قبل حدوثها.
٤- نجد أنَّ أمن الدول لم يَعُد متعلقًا فقط من خلال حمايتها من المخاطر والهجمات العسكرية، وإنما امتد واتسع ليشمل الحاجة لحماية مجتمعاتها ومنشآتها الحيوية وبنيتها التحتية وخاصة الاقتصادية من التعرض للمخاطر السيبرانية.
٥- ضرورة الالتزام التنظيمى للمؤسسات بإدارة المخاطر السيبرانية؛ حيث إن مجرد وجود الرغبة دون سياسات وإجراءات مدروسة لا يكفى لإيجاد ثقافة مناهضة للمخاطر السيبرانية.
٦- أصبح من الضرورى العمل على الحد من هذه المخاطر السيبرانية عن طريق وضع إجراءات وسياسات تحمى البيانات الاقتصادية بالدول، وعليه يبقى اتباع نظام إدارى لإدارة المخاطر السيبرانية داخل المنظمات والمؤسسات بالدولة هو الحل لحماية القطاعات الاقتصادية، والمالية من القرصنة، واختراق البيانات، ولذا أصبح من الضرورى العمل على إدارة المخاطر السيبرانية فى المجال الاقتصادى لحماية وتحقيق الأمن القومى للدول.

الهوامـش :

(1) Cebula, J.J. and L.R. Young, A taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, 2020, Pennsylvania, P 75.

(٢) صـلاح حيدر عبد الواحد، حروب الفضـاء الإلكتروني: دراسة فى مفهومها وخصائصـها وسبل مواجهتها، ٢٠٢١، جامعة الشرق الأوسط، عمان، ص ٥٨.

(٣) المرجع السابق، ص٦٠.

(4) ISOC, Unleashing the potential of the internet for ASEAN economies. https://www.internetsociety.org/sites/default/files/ASEAN_ISOC_Digital_Economy_Report_Full_0.pdf, (5 mars 2023).

(5) Authority, C. A. S., Safety management systems, Canberra, ACT, Australia, 2002, P 45.

(6) Sityata, I., Botha, L., & Dubihlela, J., Risk Management Practices, Version 5, South African Universities, 2021, South African, p 195.

(7) Pest Management Regulatory Agency Health Canada, A Framework for Risk Assessment and Risk Management of Pest Control Products, PMRA Guidance Document, Canada, 2021, p 112.

(٨) عمر النجار، أثر إدارة المخاطر على التميز المؤسسـى لجامعة الأقصـى بقطاع غزة، رسالة ماجستير، كلية الاقتصاد والعلوم الإدارية، الجامعة الإسلامية، ٢٠٢٠، غزة، ص ٦٨.

(٩) أحمـد الخيـاط، تصـور مقترح لتطويـر إدارة الأعمال فى ضـوء مدخـل إدارة المخاطر بمؤسسـات الأعمال الكويتيـة، المجلة العلمية للاقتصاد والتجارة، كلية التجارة، جامعة عين شمس، ٢٠٢٠، القاهرة، ص ٢٨.

(١٠) المرجع السابق، ص ٢٩.

(11) Quinn, S., Ivy, N., Barrett, M., Feldman, L., Witte, G., & Gardner, R., Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management, National Institute of Standards and Technology, 2021, p.p 52-53.
Enterprise Risk Management, National Institute of Standards and Technology, 2021, p.p 52-53.

(12) Hopkin, PFundamentals of risk management: understanding, evaluating and implementing effective risk management, Kogan Publishers, 2020, London, p135.

(13) Cybersecurity Risk Management: Why it is needed and How to proceed. https://www.azeusconvene.com, (10 Mars 2023).

(14) Maphorisa, Leadership and the risk management Conundrum in Batswana Country, 24 (1) Mosennodi Journal, 2021, Botswana, p. 17

(15) Buganová, K., & Šimíčková, J., Risk management in traditional and agile project management, Transportation Research Procedia, Version 40, 2021, p.p 986-993.

(١٦)سارة محمد حسين، إجراءات مقترحة لإدارة المخاطر السيبرانية، العدد الرابع والثلاثون، مجلة الإدارة التربوية، ٢٠٢٢، القاهرة، ص ٣٥.

(17) Aven, T., Risk assessment and risk management: Review of recent advances on their foundation, European Journal of Operational Research, 2016, p.p 1-13.

(18) Centers for Medicare & Medicaid Services Information Security and Privacy Group, Version 3, Risk Management Handbook, 2021, Chapter 14, p195.

(19) Ibid, p. 195.

(٢٠) سارة محمد حسين، مرجع سابق، ص ٦٥.

(٢١) مروة فتحى السيد بغدادى، اقتصاديات الأمن السيبرانى، مجلة البحوث القانونية والاقتصادية، العدد ٧٦، يونيو ٢٠٢١، القاهرة، ص١٦.

(٢٢) المرجع السابق، ص١٧.

(٢٣) صـليحة محمدى، الارهـاب الإلكترونى والأمن القومـى للدول: نمط جديد وتهديـدات مختلفة، المجلة الجزائريـة للأمن والتنمية، ٢٠٢٠، الجزائر، ص٦٧.

(٢٤) نبيل حشاد، إدارة المخاطر السيبرانية بالمصارف، العدد ٢٨٨ ، مجلة اتحاد المصارف العربية ، ٢٠٠٤، ص ٣٥.

(25) Khan, M. A., & Malaika, M., Risk Management Fintech and Cybersecurity, International Monetary Fund, 2021, p.p 87 - 90.

إدارة المخاطر السيبرانية فى المجال الاقتصادى

■ د/ رحاب حسنى الرحماوى
مهندسة كهرباء اتصالات بالهيئة الوطنية للإعلام

المستخلص :

يرتبط الجانب السيبرانى ارتباطًا وثيقًا بالاقتصاد، خاصة بعد التوسع فى استخدام تقنيات المعلومات والاتصالات، ولذلك يأخذ الأولوية فى الاهتمام لما له التأثير الأكبر على تعزيز باقى قدرات قوى الدولة الشاملة ويؤثر فى مقدرات الأفراد والوطن على جميع المستويات.

فقد هدفت الدراسة إلى معالجة موضوع يُعد من الموضوعات الحديثة والبالغة الأهمية حيث تمثل المظهر الجديد لحروب المستقبل من خلال استخدام الفضاء السيبرانى كوسيلة للهجوم السيبرانى للسيطرة على اقتصاد الدول باستخدام مجموعة من البرمجيات، والفيروسات المدمرة كأسلحة استراتيجية سيبرانية ناتجة عن توجهاتهم الاستراتيجية، وكوسيلة لتدمير البنية التحتية الاقتصادية للدولة، ومن ثم التأثير على الأمن القومى للدولة المستهدفة، مما جعل هناك ضرورة للعمل على إدارة هذه المخاطر السيبرانية فى المجال الاقتصادى للدولة، ولذلك تظهر مشكلة الدراسة فى تحديد المخاطر السيبرانية وآثارها السلبية على المجال الاقتصادى للدول وللمؤسسات والمنظمات بها. تأتى أهمية الدراسة فى توضيح تأثير المخاطر السيبرانية على المجال الاقتصادى للدول وكيفية إدارة مخاطرها السيبرانية داخل المنظمات والمؤسسات لها، لتحقيق الأمن القومى.

وقد خلُصت الدراسة إلى عدة نتائج منها أنَّ هناك العديد من الإجراءات الفنية والإدارية المتاحة لمجابهة وإدارة المخاطر والهجمات السيبرانية فى الفضاء السيبرانى والتصدى لها، وأن الالتزام بتطبيق أكبر قدر منها يمكن أن يكون معينًا إلى حد بعيد فى التصدى لهذه الهجمات بل والعمل على إدارة مخاطرها السيبرانية قبل حدوثها.

الكلمات المفتاحية : الفضاء السيبرانى، المخاطر السيبرانية، المجال الاقتصادى

Cyber Risks Management in the Economic Field

■ *Dr / Rehab Hosny El Rahmawy*
Communications Electrical Engineer at the National Media Authority

Abstract:

This study explores the critical relationship between the cyber domain and the economy, heightened by the widespread adoption of information technology. The cyber realm's significance lies in its capacity to bolster a nation's comprehensive state capabilities and affect individuals and the nation across all levels.

The research investigates the emerging trend of cyber warfare, wherein cyber attacks employing strategic cyber weapons, including destructive programs and viruses, are used to manipulate a nation's economy in alignment with the aggressor's strategic objectives. These attacks aim to disrupt the economic infrastructure of the target state, jeopardizing its national security. Therefore, the study emphasizes the need to proactively manage cyber risks within a nation's economic sphere.

The study's central challenge is identifying and mitigating cyber risks' adverse impact on a nation's economic entities and institutions. Its significance lies in understanding how these risks affect a nation's economic landscape and proposing strategies for proactive risk management to ensure national security.

The study concludes that various technical and administrative measures are available to counter and manage cyber risks and attacks. Adherence to these measures can effectively thwart cyber attacks and proactively manage cyber risks before they materialize, safeguarding a nation's economic security.

Keywords: Cyber space,, Cyber Risks, Economic field