دور استراتيجيات الأمن السيبراني في تعزيز كفاءة التحاسب الضريبي بالبيئة المصرية

إعداد

أ / عبدالستار محروس مصطفى حسين زايد

٢٠٢٥م – ١٤٤٦هـ

قسم المحاسبة والمراجعة ... كلية التجارة ... جامعة مدينة السادات

الملخص:
تناقش الورقة البحثية دور استراتيجيات الأمن السيبراني في تعزيز كفاءة التحاسب الضريبي، خاصة في ظل التطور الرقمي المتزايد والاعتماد الكبير على الأنظمة الإلكترونية في مختلف القطاعات، كما تسلط الورقة البحثية الضوء على التحديات التي تواجه السلطات الضريبية في حماية البيانات والمعلومات من الهجمات السيبرانية، وانعكاسات ذلك على كفاءة التحصيل الضريبي وشفافيته ، ويمكن الاشارة إلى أن تطبيق استراتيجيات الأمن السيبراني الفعالة يمكن أن يساهم في حماية الأنظمة الضريبية من الهجمات السيبرانية، وتحسين دقة الحسابات الضريبية، وتعزيز الامتثال الضريبي، وزيادة ثقة دافعي الضرائب في النظام الضريبي.

وأخيرا يمكن تقديم مجموعة من التوصيات للجهات المسؤولة حول كيفية تطبيق استراتيجيات الأمن السيبراني بشكل فعال في عمليات التحصيل الضريبي، مثل: تطبيق أنظمة تشفير قوية، وتطوير الجدران النارية المتقدمة، وتفعيل مراقبة مستمرة للأنظمة، وتدريب الموظفين على كيفية التعامل مع التهديدات السيبرانية، واستخدام تكنولوجيا التعرف على الهوية، ووضع استراتيجيات استجابة للطوارئ، والامتثال للمعايير الدولية للأمن السيبراني

أولاً : الإطار العام للورقة البحثية

١ ـ فكرة الورقة البحثية :

يعد النظام الإداري الضريبي من الركائز الأساسية للتنمية الاقتصادية ، وتساهم زيادة كفاءة النظام الضريبي ووضوحه في زيادة قدرة الحكومة على تحصيل الإيرادات الضريبية بأقل تكلفة والحد من التهرب الضريبي . إضافة إلى ذلك ، تساهم كفاءة النظام الضريبي في تحسين بيئة الأعمال ، الأمر الذي يساهم في جذب الاستثمار المحلي والاستثمار الأجنبي المباشر . ومع زيادة التطور الرقمي المستمر، وقد أصبحت جرائم الأمن السيبراني تشكل تهديد للمؤسسات، كما يعد حدوث اختراقات للأمن السيبراني من المخاطر الرئيسية التي تواجهها الشركات في العالم الرقمي، ولقد أدى الارتفاع في اختراقات الأمن السيبراني إلى جعل الأمن السيبراني مجالا بالغ الأهمية للشركات والأسواق والجهات التنظيمية العالمية ، كما تشير التقديرات إلى أن تكاليف الأضرار الناجمة عن الجرائم السيبرانية قد تصل إلى ١٠.٥ تريليون دولار سنويًا بحلول عام ٢٠٢٥، وذلك وفقًا لتقرير صادر عن "سايبر سيكيوريتي فنتشرز(Cybersecurity Ventures) " ، وبناء على تقرير المنتدى الاقتصادي العالمي " مستقبل الأمن السيبراني ، ٢٠٢٥ " أن التسارع التقني الهائل، والاضطرابات السياسية العالمية، وتطور أساليب الاختراق، والتشابك المعقد في سلاسل التوريد، والنقص الحاد في الكفاءات الرقمية، كلها عوامل تسهم في تعميق الفجوة الرقمية بين الدول المتقدمة والنامية، وبين المؤسسات الكبرى والصغرى (شرف ، ٢٠٢٤) .

وتعتبر الايرادات الضريبية الركيزة الاساسية لعمليات التنمية المستدامة، كما تعد الايرادات الضريبية الدافع والداعم الرئيسي والأكبر لعمليات التنمية المستدامة لخطة الدولة في ضوء استراتيجية ورؤية مصر ٢٠٣٠م، حيث تمثل الايرادات الضريبية نسبة ٧٦% من من ايرادات الموازنة العامة للدولة المصرية ، وفي ظل قصور منظومة الضرائب التقليدية وارتفاع حالات التهرب الضريبي وانخفاض الحصيلة الضريبية من الايرادات خلال الفترات السابقة، أصبح من الضروريات الملحة إعادة النظر في منظومة الضرائب التقليدية ومحاولة تطبيق آليات التحول الرقمي لمعالجة جوانب القصور والضعف بتلك المنظومة ، وتعتبر حصيلة الإيرادات الضريبية الركيزة الأساسية والداعم الرئيسي لبرامج التنمية المستدامة في البيئة المصرية ، وفي ظل ضعف منظومة التحاسب الضريبي التقليدية في الحد من ممارسات التهرب الضريبي وتحقيق العدالة الضريبية ، مما ينعكس بالسلب على حصيلة الإيرادات الضريبية (خليفة ، ٢٠٢٢) .

وفي ظل التطور السريع للتكنولوجيا الرقمية وزيادة الاعتماد على الأنظمة الإلكترونية في مختلف القطاعات، أصبحت السلطات الضريبية تواجه تحديات كبيرة تتعلق بأمن المعلومات وحماية البيانات، وتعتبر الهجمات السيبرانية والاختراقات الإلكترونية من أكبر المخاطر التي تهدد كفاءة التحصيل الضريبي. حيث يمكن أن تؤدي إلى فقدان المعلومات أو التلاعب بها، مما يؤثر سلباً على دقة التحصيل والشفافية، ونقص ثقة الممولين في المنظومة الضريبية وبالتالي زيادة التهرب ، حيث تعتبر مشكلة التهرب الضريبي واحدة من التحديات الرئيسية التي تواجه الحكومات في جميع أنحاء العالم، فقد تؤدي إلى خسارة الإيرادات العامة وتعرقل التنمية الاقتصادية، ومع التطور التكنولوجي وانتشار التعاملات الرقمية ظهرت فرص جديدة لمرتكبي التهرب الضريبي لاستخدام تقنيات متقدمة للإفلات من الرقابة، ولذا يتطلب الأمر تطوير استراتيجيات أمنية سيبرانية فعالة لمواجهة هذه التحديات (شرف ، ٢٠٢٤) .

ويعتبر الأمن السيبراني هو عملية حماية الأنظمة البنكية والشبكات والبرامج ضد الهجمات الرقمية تهدف هذه الهجمات السيبرانية عادة إلى الوصول إلى المعلومات الحساسة واستغلالها في أفعال قد تهدد أمن الدول والأشخاص كانوا الاعتباريين أو الذاتيين ، حيث ان الأمن السيبراني لم يبدأ إلا في سبعينيات القرن الماضي، إذ لم يكن هناك الكثير من المعلومات عما بات يعرف ببرامج التجسس والاختراق والفيروسات ، وغيرها من المصطلحات التي أصبحت فيما بعد معروفة ومتداولة على نطاق واسع، وذلك بعد حدوث ارتفاع هائل في جرائم الإنترنت خاصة الجرائم المتعلقة بالأنظمة البنكية، حيث أصبح مفهوم الأمن السيبراني معروفا وشائعا ومهما ، وذلك بسبب الاعتماد المتزايد على مختلف أنواع الأجهزة الإلكترونية المتصلة بالإنترنت وبشبكات الاتصال اللاسلكية فبدأ مفهوم الأمن السيبراني يظهر شيء فشيء مع ظهور أنواع جديدة من تقنيات وتضاعف اخطارها وظهور أنماط جديدة من التهديدات المرتبطة بالأنترنت مرورا من الثمانينات والتسعينيات ، ووصولاً إلى فترة القرن الحادي والعشرين بحلول العقد الأول من القرن الحادي والعشرين تنوعت وتضاعفت

التهديدات والاختراقات وكذلك الهجمات الإلكترونية المتعلقة بالأنظمة البنكية التي بدأت كثير من الكيانات الإجرامية القيام بها وبشكل محترف باستخدام تقنيات عالية، الأمر الذي دفع الكثير من الدول والحكومات إلى اتخاذ العديد من القرارات من أجل تضييق الخناق على هذه الجهات. وكان ذلك من خلال العديد من الخطوات مثل من التشريعات الخاصة بهذا النوع من الجرائم، وإصدار الأحكام الجنائية ومع مرور الوقت، تقدم أمن وحماية المعلومات والبيانات على شبكة الإنترنت ذلك ما تزال العديد من الجهات تنتج مختلف أنواع الفيروسات لخرق هذا الإنترنت، ومع الأمن (الحيمودي ، ٢٠٢٣) .

ولقد اهتمت الحكومة المصرية بتطبيق آليات التحول الرقمي في كافة الأعمال وخاصة فيما يتعلق بمنظومة الضرائب المصرية ، حيث لم يعد تطبيق منظومة التحول الرقمي خياراً نحو التنمية المستدامة ، بل ضرورة قطعت فيها معظم دول العالم خطوات كبيرة ، وأصبح التحول الرقمي لمنظومة الضرائب المصرية من الضروريات الملحة ، وخاصة في ظل التطور المتسارع في استخدام وسائل تكنولوجيا المعلومات في كافة نواحي الحياة سواء كانت متعلقة بالمعاملات مع القطاع الحكومي أو الخاص أو كانت تخص الأفراد، لذلك هناك ضغط واضح من كافة شرائح المجتمع على المؤسسات والهيئات والشركات لتحسين خدماتها ، وفي ضوء تبني الحكومة المصرية لخطط التنمية المستدامة وتحقيق استراتيجية ورؤية مصر ٢٠٣٠ أصبحت من الأولويات الهامة والملحة ضرورة التوجه نحو تطوير منظومة التحاسب الضريبي ومحاولة معالجة جوانب الضعف والقصور بتلك المنظومة وذلك من خلال التوجه نحو التحول الرقمي لكافة أركان المنظومة الضريبية (خليفة ، ٢٠٢٢) .

وتعد مخاطر الأمن السيبراني أحد أشكال مخاطر الخسارة المالية أو التعطل أو الإضرار بسمعة الشركة نتيجة لفشل في أنظمة تكنولوجيا المعلومات الخاصة بها بسبب هجمات خارجية. تتضمن أمثلة مخاطر الأمن السيبراني مخاطر فقدان البيانات الحساسة والتعطل في شبكة الشركة وأنظمتها وخدماتها والأضرار الإلكترونية المادية. يعتبر المسؤولون التنفيذيون في الشركات والمشاركون في السوق في الاقتصادات المتقدمة حاليًا مخاطر الأمن السيبراني واحدة من أهم المخاوف العالمية ، وهو أمر غير مفاجئ نظرًا للزيادة السريعة في الهجمات الإلكترونية الكبرى في السنوات الأخيرة. وعلى الرغم من الاستثمارات الكبيرة في أنظمة أمن المعلومات، لا تزال معظم الشركات معرضة بشدة لمخاطر الأمن السيبراني (Florackis, 2022) .

٢ ـ أهداف الورقة البحثية :

يتجسد الهدف الرئيس للورقة البحثية في بيان دور استراتيجيات الأمن السيبراني في زيادة كفاءة التحاسب الضريبي من خلال الحد من الهجمات السيبرانية ، وبناء جسور من الثقة بين مصلحة الضرائب والمجتمع الضريبي ، وذلك سعياً نحو تحقيق الأهداف الفرعية التالية :

١/٢- بيان أهم التهديدات والمخاطر الأمنية التي تؤثر على أنظمة التحصيل الضريبي واقتراح حلول لتقليل تلك المخاطر.

٢/٢- تقديم آليات تطبيق استراتيجيات الأمن السيبراني بشكل فعال لتحسين كفاءة التحاسب الضريبي.

٣/٢- تحديد طبيعة العلاقة بين استراتيجيات الأمن السيبراني المستخدمة ومستوى كفاءة التحصيل الضريبي.

٣ ـ أهمية ودوافع الورقة البحثية ، تبرز أهمية دراسة دور استراتيجيات الأمن السيبراني في زيادة كفاءة التحاسب الضريبي من خلال النقاط التالية:

١/٣- تسليط الضوء على أهمية استخدام التقنيات والنظم المستحدثة في حماية البيانات الضريبية من الهجمات السيبرانية.

٢/٣- تعزيز كفاءة وشفافية التحصيل الضريبي من خلال الاستفادة من استراتيجيات الأمن السيبراني ، مما يسهم في بناء ثقة المواطنين في النظام الضريبي ويؤدي إلى تقليل ممارسات التهرب الضريبي.

٣/٣- توجه مصلحة الضرائب المصرية نحو التحول الرقمي لمنظومة الضرائب كوسيلة الحصر كافة الممولين والحد من ممارسات التهرب الضريبي، ودمج قطاعات الاقتصاد غير الرسمي مع الاقتصاد الرسمي.

٤ ـ تنظيم الورقة البحثية ، سعياً نحو تحقيق أهداف الورقة البحثية يمكن تنظيمها على النحو التالي:

أولاً : الإطار العام للورقة البحثية.

ثانياً : أهمية استراتيجيات الأمن السيبراني في زيادة كفاءة التحاسب الضريبي

ثالثاً : أهم الدلالات والتوصيات البحثية.

ثانياً : أهمية استراتيجيات الأمن السيبراني في زيادة كفاءة التحاسب الضريبي

يمكن عرض وتحليل بعض المفاهيم الرئيسية التي تتعلق بمتغيرات الورقة البحثية علي النحو التالي

١ ـ الأمن السيبراني : عبارة عن عملية تستهدف حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات، وما تحتويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ، ويعرف بأنه عبارة عن مجموعة من التقنيات والعمليات والممارسات التي تحمى وتضمن حماية أصول المنشأة . كما يعرف الأمن السيبراني بأنه تنظيم وجمع الموارد والعمليات والهياكل التي يتم استخدامها لحماية الفضاء الإلكتروني والأنظمة الأخرى التي تدعم الفضاء الإلكتروني من الهجمات والحوادث الإلكترونية (شرف ، ٢٠٢٤) .

ويمكن تعريف الأمن السيبراني أيضًا بأنه النشاط أو العملية أو القدرة أو الحالة التي تُحمى من خلالها أنظمة المعلومات والاتصالات والمعلومات الواردة فيها من التلف أو الاستخدام أو التعديل أو الاستغلال غير المصرح به. لا شك أن الإنترنت يزيد من معرفة الفرد. على سبيل المثال، تتطلب ألعاب الكمبيوتر عبر الإنترنت مستخدمين ذوي مهارات عالية في اللغة الإنجليزية لفهم إعدادات اللعبة وإجراءاتها. وهذا يُشجع بشكل غير مباشر على تطوير مهارات القراءة والكتابة والتحدث باللغة الإنجليزية. ومع ذلك، عادةً ما تكون ألعاب الكمبيوتر ممتعة، وتستغرق وقتًا طويلاً لإكمالها. قد يُسبب هذا كسل المراهقين أو تركيزهم على اللعب والأجهزة. كما قد يُصبح المراهقون مدمنين، ويُتجاهلون الأنشطة الإنتاجية، مثل مراجعة دروسهم (Rahman , 2020) .

٢ ـ **القوة السيبرانية :** هي القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني ، وهي القدرة على استخدام الفضاء الإلكتروني لخلق مزايا، والتأثير على الأحداث المتعلقة بالبيئة الواقعية عبر أدوات إلكترونية (شرف ، ٢٠٢٤) .

٣ ـ **الدفاع السيبراني :** ويقصد به مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثير الهجمات السيبرانية، والتخفيف من حدتها والتعافي منها بسرعة، وقد عرفت العقيدة الفرنسية الدفاع الإلكتروني على أنها مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع في الفضاء الإلكتروني عن نظم المعلومات الحرجة، ويعرفه البرلمان الأوروبي بأنه عمليات تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات السيبرانية والتعامل معها (أمير ، ٢٠٢٣) .

٤ ـ **الردع السيبراني :** نتيجة للطبيعة الخاصة للفضاء السيبراني، فإنه من الصعوبة منع الهجمات السيبرانية بصورة كلية، فضلاً عن صعوبة تعقب مصدر الهجمة، ومعرفة الفاعل من الناحية الفنية، لذا فإن تحقيق الردع بالطرق التقليدية لا يتحقق في أفضل الأحوال في الفضاء الإلكتروني كما في حالات الردع التقليدي، لذلك فإن الردع في الفضاء الإلكتروني يتحقق من خلال تبني خطط واستراتيجيات للتعامل مع الهجمات السيبرانية في حالة حدوثها تشمل (أمير ، ٢٠٢٣) :

١/٤ـ **التخفيف من حدتها :** والتي تشير إلى تقليل الأضرار والآثار الناجمة عن الهجوم السيبراني بعد وقوعه، والعمل على استعادة الأنظمة والخدمات المتأثرة بأسرع وقت ممكن.

٢/٤ـ **عدم التأثير على البنى التحتية الحرجة :** وذلك من خلال تحديد البنى التحتية الحيوية التي يجب حمايتها بشكل خاص، وتطبيق إجراءات أمنية متقدمة عليها لضمان استمرار عملها في حال وقوع هجوم سيبراني، بالإضافة إلى وجود خطط طوارئ بديلة لضمان استمرار الخدمات الأساسية في أسوأ السيناريوهات.

٣/٤ـ **الخدمات الرئيسية والمعلومات المهمة التي تشكل :** وذلك من خلال تحديد هذه الخدمات والمعلومات وتصنيفها حسب أهميتها وحساسيتها، وتطبيق تدابير أمنية وقائية واستباقية لحمايتها من الاختراق أو التعطيل، بالإضافة إلى وضع خطط استجابة سريعة للتعامل مع أي محاولات اختراق أو هجمات ناجحة لضمان استعادة الخدمات والمعلومات بأسرع وقت ممكن وتقليل الأضرار.

٤/٤ـ **ركيزة للأمن القومي للدولة :** وذلك من حيث ضمان سلامة واستقرار الفضاء السيبراني للدولة وحماية مصالحها الحيوية وأمنها القومي من التهديدات السيبرانية المختلفة، بما في ذلك حماية البنية التحتية الحيوية، وضمان استمرار الخدمات الحكومية الأساسية، وحماية المعلومات الحساسة، ومكافحة الجرائم السيبرانية، وتعزيز القدرات الدفاعية والهجومية السيبرانية للدولة.

٥ ـ الإفصاح عن المخاطر السيبرانية : هو مجموعة من الإجراءات والضوابط المنطقية التي تمارسها المنظمات للإفصاح عن المعلومات المحيطة بالخرق الأمني، من خلال التأثيرات المختلفة لأصحاب المصلحة، والعوامل الداخلية والخارجية، وغالباً ما تؤدي العملية إلى درجات متفاوتة من الاكتمال والدقة وحسن التوقيت والشفافية ومشاركة الإدارة في المعلومات التي يتم إرسالها إلى أصحاب المصلحة المعنيين لاتخاذ القرارات، واعطاء الفرصة لاستكشاف وفهم الظاهرة والتحقيق في القضايا ذات الصلة وتكمن أهمية الإفصاح عن المخاطر السيبرانية في إظهار جميع المعلومات الضرورية وتلبية احتياجات مستخدمي القوائم المالية عبر موقع الشركة أو إفصاحتها في البورصة وغيرها من التقارير، لمساعدتهم في اتخاذ القرارات، وتخفيض حالة عدم التأكد (عبدالفتاح ، ٢٠٢٤) .

٦ ـ التحاسب الضريبي الإلكتروني : من المعلوم انه تعود فكرة الضريبة إلى فترة طويلة في تاريخ الحضارات والمجتمعات، وعلى الرغم من أنها لم تكن معروفة لدى العرب والمسلمين في البداية، إلا أنها تطورت عبر العصور لتصبح مصدرا اقتصاديًا يجب على الدولة الحصول عليه لأنها تساهم في حل العديد من المشاكل المالية والاقتصادية والاجتماعية التي تواجهها الدول، وهناك تحديات تواجهها الإدارة الضريبة في التحاسب الضريبي على الأنشطة الرقمية وإيضاح دور المنظمات المهنية والمحاسبية في إيجاد حلول ومعالجات لهذه التحديات ، وقد استفادت التجارة الإلكترونية وصناعة المحتوى بشكل كبير من الميزات التي توفرها شبكات التواصل الاجتماعي لصانعي المحتوى والمؤثرين، حيث أتاحت لهم هذه المنصات إمكانية نشر محتواهم وتوزيعه والوصول إلى جماهير واسعة من المتابعين حول العالم ، وطلبت مصلحة الضرائب المصرية من البلوجرز واليوتيوبرز والإنفلونسر، التوجه إلى مكاتبها لفتحملفات ضريبية لهم وإصدار بطاقة ضريبية والذين تبلغ إيراداتهم ٥٠٠ ألف جنيه خلال أثنى عشر شهراً من تاريخ مزاولة النشاط بالتسجيل في مأمورية القيمة المضافة المختصة ، وقد أثار هذا الكثير من الجدل والتساؤلات، لا سيما مع عدم تحديد الرسوم المستحقة، وعدم إطلاق تعريفات دقيقة للفئات المستهدفة من تحصيل الضرائب بحسب المتابعين (قامش ، ٢٠٢٤) .

وتعتبر الفاتورة الإلكترونية هي وثيقة رقمية الكترونية موحدة معترف بها من مصلحة الضرائب المصرية تستخدم لأثبات عملية بيع السلع والخدمات المختلفة وتشمل كل وثيقة على توقيع الكتروني خاص بها يوضح فيها هوية الموقع، وذلك لمنع التزوير والتزييف، وذلك لضمان الأمان والخصوصية، وكذلك منظومة الفاتورة الإلكترونية الحديثة في مصر تعتبر بمثابة إجراء جديد يقوم بتحويل العملية التقليدية لإصدار فواتير الشراء من عملية يدوية بحته إلى عملية الكترونية كاملة (ابوالعينين ، ٢٠٢٤) .

٧ ـ الأهداف الاستراتيجية للأمن السيبراني : مع التوسع في التحول الرقمي أصبحت حماية الأنظمة والبيانات من التهديدات السيبرانية ضرورة ملحة تهدف الاستراتيجية الوطنية للأمن السيبراني إلى تحقيق أربعة أهداف رئيسية (شرف ، ٢٠٢٤) :

أ) **الحماية (Protect):** تهدف إلى بناء حصن دفاعي قوي ضد الهجمات السيبرانية ، لتعزيز ثقة ومرونة المؤسسات الحكومية والخاصة ، وتشمل الإجراءات:

١ - وضع سياسات وإجراءات وطنية موحدة للأمن السيبراني.

٢ - تطبيق حوكمة فعالة لضمان الأمن السيبراني.

٣ - تطوير بنية تحتية تقنية متقدمة للأمن السيبراني.

٤ - طلاق برامج توعية وتدريب لبناء قدرات بشرية مؤهلة.

ب) **الكشف والتحري (Detect):** يركز على القدرة على اكتشاف التهديدات السيبرانية في وقت مبكر، وفهم طبيعتها وأساليبها ، وتشمل الإجراءات:

١ - تطوير قدرات استخباراتية متقدمة لرصد التهديدات.

٢ - تحليل سلوك المهاجمين وتحديد الأهداف الأكثر عرضة للخطر.

٣ - اختبار وتقييم فعالية الدفاعات الأمنية بشكل دوري.

٤ - استخدام أدوات وتقنيات متطورة للكشف عن الحوادث السيبرانية.

ج) **الاستجابة (Respond):** يهدف إلى تطوير قدرات فعالة للتعامل مع الهجمات السيبرانية، والحد من آثارها السلبية ، وتشمل الإجراءات:

١ - وضع خطط استجابة للحوادث السيبرانية، وتحديد الأدوار والمسؤوليات.

٢ - توفير أدوات وتقنيات لاستعادة الخدمات الأساسية بعد الهجوم.

٣ - إجراء تحقيقات جنائية رقمية لتحديد الأسباب والمسؤولين عن الهجوم.

٤ - تحسين الإجراءات الوقائية لمنع تكرار الهجمات.

د) **التطور (Evolve):** يركز على بناء قدرات وطنية مستدامة في مجال الأمن السيبراني، ومواكبة التطورات التكنولوجية ، وتشمل الإجراءات:

١ - تعزيز التعاون وتبادل المعرفة مع المنظمات المتخصصة.

٢ - تأهيل الكوادر الوطنية في مجال الأمن السيبراني.

٣ - تطوير التشريعات والقوانين اللازمة لحماية الفضاء السيبراني.

٤ - توفير الأدوات والموارد اللازمة لتطوير القدرات السيادية المستدامة.

٥ - إنشاء قنوات اتصال وطنية ودولية لتبادل المعلومات والخبرات.

٨ ـ **تعزيز الأمن السيبراني بالبيئة المصرية:** تبذل الحكومة المصرية جهوداً كبيرة لتعزيز الأمن السيبراني في البلاد، وتشمل هذه الجهود:

١/٨- **إصدار القوانين والتشريعات:** أصدرت مصر العديد من القوانين والتشريعات التي تهدف إلى حماية البيانات والمعلومات من التهديدات السيبرانية، مثل قانون مكافحة جرائم تقنية المعلومات.

٢/٨- **إنشاء الهيئات والمؤسسات:** أنشأت مصر العديد من الهيئات والمؤسسات المعنية بالأمن السيبراني، مثل المجلس الأعلى للأمن السيبراني والجهاز القومي لتنظيم الاتصالات.

٣/٨- **تنفيذ الاستراتيجيات والسياسات:** وضعت مصر استراتيجية وطنية للأمن السيبراني تهدف إلى بناء منظومة رقمية آمنة ومستدامة.

٤/٨- **التعاون الدولي:** تتعاون مصر مع العديد من الدول والمنظمات الدولية في مجال الأمن السيبراني لتبادل الخبرات والمعلومات.

٥/٨- **مبادرة سايبر مصر ٣٦٠ :** وهي مبادرة تهدف إلى تعزيز أمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات.

وتتزايد اهمية الأمن السيبراني في مصر مع التقدم التكنولوجي السريع وكثرة استخدام التقنيات الرقمية في مختلف القطاعات، وهو يشمل جميع الإجراءات والتدابير التي تتخذها الحكومة والشركات لحماية الأنظمة الرقمية والمعلومات من التهديدات السيبرانية، وتعتبر التحديات في مجال الأمن السيبراني في مصر ذات أهمية كبيرة، فمع التطور التكنولوجي، تتزايد أيضًا وسائل التهديد السيبراني، مما يتطلب إجراءات أمان أكثر تقدما، وتعاني الكثير من الكوادر البشرية في مصر من نقص في التحضير والوعي السيبراني، الأمر الذي يزيد من تعرضهم، وقد يكون هناك تحدي في تحديث وتحسين البنية التحتية لتكنولوجيا المعلومات والاتصالات وحاجة إلى تحسين التشريعات والسياسات المتعلقة بالأمن السيبراني لضمان فعالية الإجراءات الوقائية والتصدي ، ومع ذلك يتسع أيضًا الفضاء للفرص في مجال الامن السيبراني في مصر، اذ يمكن للتعاون مع دول وهيئات دولية تقديم فرص لتبادل الخبرات والدعم في مجال الأمن السيبراني ، وتطوير وتحسين المهارات والوعي السيبراني للكوادر العاملة مما يوفر فرصة لتعزيز التحضير والتصدي للتهديدات ويمكن أن يوفر الاستثمار في تكنولوجيا الأمن السيبراني فرصة لتعزيز القدرة على مواجهة التحديات ، ويظهر الأمن السيبراني في العراق كمجال مهم يتطلب اهتماماً وجهوداً مستدامة لتعزيز الحماية الرقمية وضمان استمرار التنمية التكنولوجية (صليبي ، ٢٠٢٤)

٩ ـ دور الأمن السيبراني في الحد من التهرب الضريبي:

يسهم نظام الإقرارات الضريبية الالكترونية في ضم القطاع غير الرسمي وبناء قاعدة بيانات تسمح بالتنبؤ بضريبة الدخل كناتج لتتبع الممول بدقة طوال العام بالإضافة إلى فحص صحة أرقام التسجيل الضريبية في الفواتير والتأكد من صحة الرقم القومي حيث يتم الفحص الأوتوماتيكي لملفات فواتير المشتريات والمبيعات وذلك لمراجعة الملف قبل رفعه علي

المنظومة وتحديد الأخطاء الموجودة بالفاتورة وإظهارها للممول ليقوم بإصلاحها قبل إرسالها للمصلحة، ويتضمن نظام الإقرارات عددا من المعلومات المهمة مثل رقم التسجيل الضريبي والرقم القومي والاسم وعنوان البائع في فاتورة مشتريات الممول وهى معلومات إجبارية لزيادة الإحكام على الفواتير والحد من تقديم الفاتورة المجمعة (شحاتة ، ٢٠٢٠) .

وفيما يلي أهم المزايا التي تقدمها الإقرارات الضريبية إلكترونياً:

١/٩- تحسين ترتيب مصر في التقارير الدولية الخاصة بالتنافسية وجذب الاستثمارات وتحسين مناخ ممارسة الأعمال وهو ما كان له صدى إيجابي، وإشادة من المؤسسات الدولية وعلى رأسها صندوق النقد الدولي .

٢/٩- إنهاء حالات التكدس من خلال تخفيض عدد مرات تردد الممولين والمسجلين على مأموريات الضرائب إلى أقل من المتوسط العالمي مما يتيح للممولين والمسجلين وقتا أطول للتركيز على أعمالهم بدلا من ضياع جزء منها في إنهاء التعاملات الحكومية.

٣/٩- تمكين مأموري الضرائب من القيام بمهامهم الأساسية في فحص الملفات الضريبية خاصة ذات القيم الكبيرة للحد من التهرب الضريبي، وتدعيم الاقتصاد القومي.

٤/٩- التوسع في خدمات التوقيع الالكتروني للإقرارات الضريبية والربط المعلوماتي للبيانات المالية.

يمكن للسياسات الضريبية أن تؤثر على هيكل تكلفة شركات التجارة الإلكترونية الإدارة المسائل المتعلقة بالضرائب بشكل فعال، غالبا ما يقوم تجار التجزئة عبر الإنترنت بجمع وتخزين بيانات واسعة النطاق للعملاء، وفي سياق الأمن السيبراني يسلط هذا الضوء على ضرورة حماية معلومات العملاء، إن اختراق البيانات بسبب عدم كفاية تدابير الأمن السيبراني لا يهدد خصوصية العملاء فحسب، بل يمكن أن يؤدي أيضا إلى خسائر مالية، ولذلك يجب على الشركات الاستثمار في الأمن السيبراني القوي لحماية بيانات العملاء للحفاظ على الثقة (عبد الكريم ، ٢٠٢١) .

تمتلك التجارة الإلكترونية القدرة على دفع التجارة الدولية وتحفيز النمو الاقتصادي، وأخيرا يمكن للحكومات والشركات التي تتعاون لوضع لوائح ضريبية واضحة في الاقتصاد الرقمي أن تعمل معا أيضا لتنفيذ تدابير قوية للأمن السيبراني. تعتبر هذه التدابير ضرورية لحماية البيانات المالية والضريبية الحساسة من الهجمات السيبرانية. بما أن معاملات التجارة الإلكترونية تنطوي على تبادل المعلومات المالية، فإن ممارسات الأمن السيبراني القوية ضرورية للحماية من اختراقات البيانات والأنشطة الاحتيالية (منصور ، ٢٠٢٠) .

في مجال الجريمة السيبرانية يمكن تطبيق مجالات مختلفة على التجارة الإلكترونية. حيث يمثل الاحتيال في الدفع أشكالاً مختلفة من الأنشطة الاحتيالية مثل الاحتيال على بطاقات

الائتمان وسرقة الهوية والاستيلاء على الحساب، ومن المناسب دراسة كيف يمكن لشركات التجارة الإلكترونية اكتشاف مثل هذه المعاملات ومنعها مجال آخر للتركيز هو التصيد الاحتيالي. حيث يقوم الباحثون بتحليل الأساليب الخادعة التي يستخدمها مجرمو الإنترنت للكشف عن المعلومات مع ،على استراتيجيات تثقيف المستهلك وحمايته، وغالبا ما تعمل شركات التجارة الإلكترونية عبر ولايات قضائية متعددة، مما يزيد من تعقيد عملية إنفاذ الضرائب (عبد الكريم ، ٢٠٢١) .

١٠ ـ حماية منظومة الضرائب المصرية ضد الهجمات السيبرانية:

منظومة الضرائب المصرية تعتبر من البنى التحتية الهامة التي يجب أن تكون محمية ضد الهجمات السيبرانية، خاصة في ظل التحول الرقمي الكبير الذي تشهده الحكومة المصرية، والذي يهدف إلى تحسين الكفاءة وتبسيط الإجراءات الضريبية. على الرغم من التقدم في هذا المجال، إلا أن الأنظمة الإلكترونية الضريبية تبقى عرضة لعدة تهديدات سيبرانية قد تؤثر على نزاهة البيانات وحمايتها، وهو ما يجعل الحاجة إلى استراتيجيات قوية للأمن السيبراني أمرًا بالغ الأهمية ، ويمكن عرض استراتيجيات حماية المنظومة الضريبية ضد الهجمات السيبرانية في ما يلي :

١/١٠- تطبيق أنظمة تشفير قوية: يجب تشفير جميع البيانات الضريبية المخزنة أو المنقولة عبر الشبكات لضمان سرية المعلومات وحمايتها من التسريب أو التلاعب. يمكن استخدام تقنيات مثل التشفير باستخدام خوارزميات AES- 256 لحماية البيانات.

٢/١٠- تطوير جدران نارية قوية: ينبغي تحديث وتطوير الجدران النارية (Firewalls) بشكل مستمر للحماية ضد الهجمات الخارجية مثل الهجمات بالفيروسات أو البرمجيات الخبيثة. يجب أن تكون هذه الجدران النارية قادرة على كشف أي محاولات للوصول غير المصرح به إلى الأنظمة الضريبية.

٣/١٠- تفعيل مراقبة مستمرة للأنظمة: يجب إنشاء فرق متخصصة في مراقبة الأنظمة بشكل مستمر للكشف المبكر عن الهجمات المحتملة أو الأنشطة المشبوهة. هذه المراقبة تساعد في اتخاذ التدابير الوقائية الفعّالة وتوجيه الاستجابة السريعة عند حدوث أي اختراق.

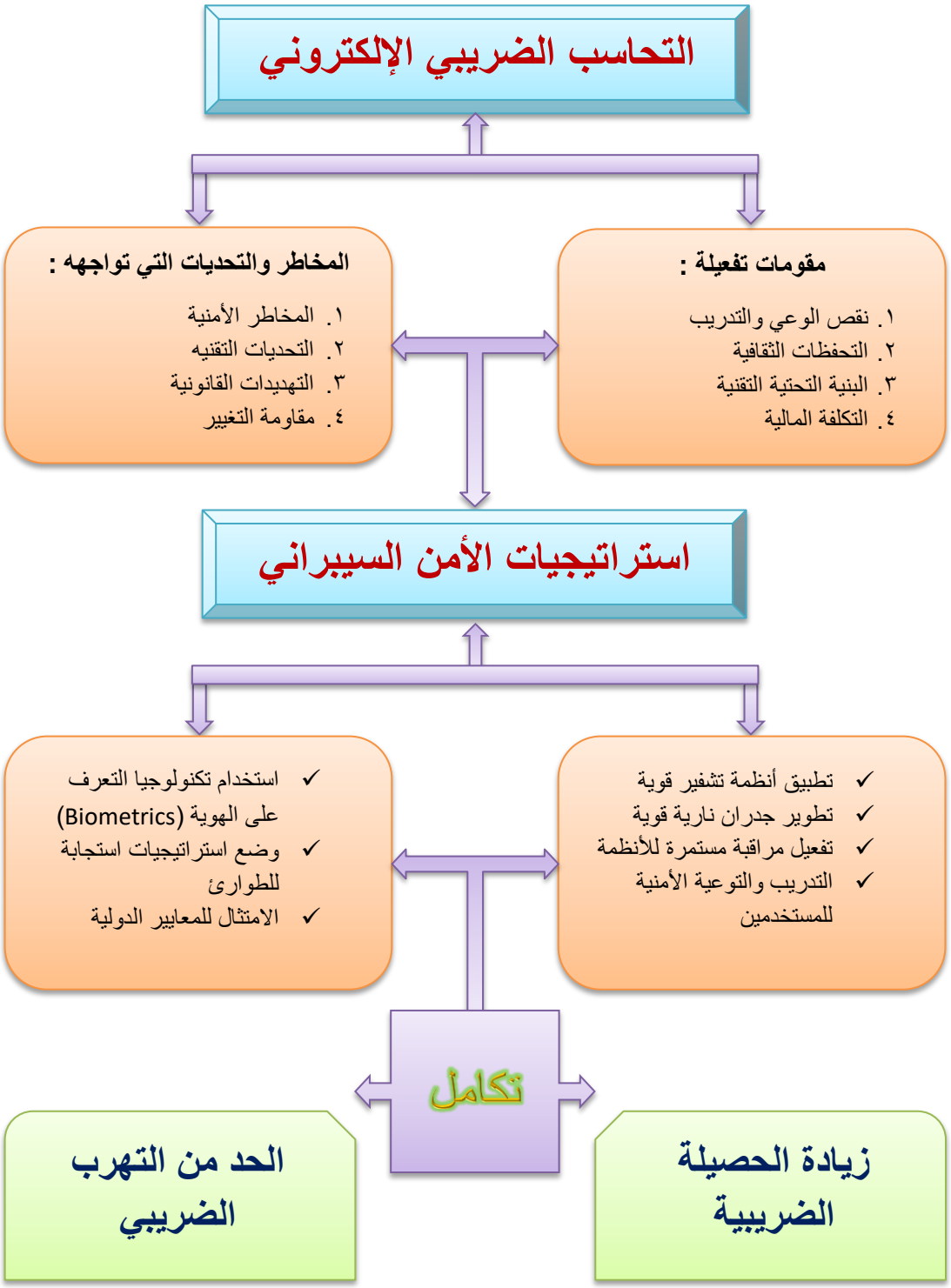
٤/١٠- التدريب والتوعية الأمنية للمستخدمين: يعتبر التدريب المستمر للعاملين في القطاع الضريبي حول التهديدات السيبرانية وكيفية التعامل مع البيانات بشكل آمن خطوة أساسية في تقليل مخاطر الهجمات السيبرانية. يشمل ذلك تعليم الموظفين كيفية التعرف على الرسائل الاحتيالية (Phishing) وأهمية استخدام كلمات مرور قوية.

١٠/٥- استخدام تكنولوجيا التعرف على الهوية (Biometrics) : يمكن تحسين الأمان من خلال تطبيق تقنيات التعرف على الهوية مثل بصمات الأصابع أو التعرف على الوجه عند الوصول إلى الأنظمة الضريبية.

١٠/٦- وضع استراتيجيات استجابة للطوارئ: ينبغي أن يتم تجهيز خطة استجابة للطوارئ تتضمن آليات لاستعادة البيانات في حال حدوث هجوم سيبراني ناجح. ويجب أن تشمل هذه الخطة إجراءات للتعامل مع المهاجمين وإعادة النظام إلى العمل بأسرع وقت ممكن.

١٠/٧- الامتثال للمعايير الدولية: يتعين على منظومة الضرائب المصرية الالتزام بالمعايير الدولية للأمن السيبراني، مثل المعايير التي تحددها منظمة "المنظمة الدولية للمعايير" (ISO) أو "المعهد الوطني للمعايير والتقنية" (NIST). هذه المعايير توفر إرشادات واضحة حول كيفية تأمين الأنظمة وحمايتها.

ويمكن الإشارة إلى الدور الفعال ليبين استراتيجيات الأمن السيبراني في تقدير كفاءة عمليات التحاسب الضريبي، ومن ثم زيادة الحصيلة الضريبية من خلال الشكل التالي:



المصدر : من إعداد الباحث .

ثالثاً : أهم الدلالات والتوصيات البحثية

يمكن استخدام مجموعة من البدلات التي تتعلق بدور استراتيجيات الأمن السيبراني في تقدير كفاءة عمليات التحاسب الضريبي علي النحو التالي :

١ ـ تقديم نموذج وصفي يعتمد على استراتيجيات الأمن السيبراني لتحسين كفاءة التحصيل الضريبي وتقديم حلول واقعية للسلطات الضريبية.

٢ ـ زيادة الوعي بين المسؤولين والممارسين في القطاع الضريبي حول أهمية الأمن السيبراني وكيفية تطبيقه لتعزيز كفاءة التحصيل وضمان حماية البيانات.

٣ ـ إن تنفيذ النموذج المقترح يؤدي إلى زيادة فعالية وكفاءة تحصيل الضرائب من خلال تعزيز الحماية ضد الهجمات السيبرانية.

٤ ـ يعزز تطبيق استراتيجيات الأمن السيبراني من أمان الأنظمة الضريبية ويقلل من المخاطر المرتبطة بالاختراقات والتهديدات السيبرانية.

٥ ـ أهم عوامل تحسين كفاءة التحاسب الضريبي :

١/٥ـ تبسيط وتوضيح التشريعات الضريبية : قلل من فرص التفسيرات الخاطئة والتلاعب، مما يسهل عملية التحاسب ويقلل من النزاعات التي قد تستغل الثغرات القانونية .

٢/٥ـ تطوير الإدارة الضريبية : يشمل تبني أنظمة تكنولوجية آمنة وفعالة لإدارة البيانات الضريبية وعمليات التحصيل، مع التركيز على تدريب الموظفين على أفضل ممارسات الأمن السيبراني.

٣/٥ـ تعزيز التوعية والالتزام الضريبي لدى الممولين : يتضمن توضيح أهمية الأمن السيبراني في حماية بياناتهم الضريبية وتشجيعهم على تبني ممارسات آمنة عند التعامل مع الأنظمة الضريبية الرقمية.

٤/٥ـ استخدام التكنولوجيا والتحول الرقمي : يستلزم تطبيق حلول أمن سيبراني متقدمة لحماية الأنظمة والبيانات من التهديدات والاختراقات، وضمان سلامة وسرية المعلومات المتبادلة.

٥/٥ـ بناء نظام ضريبي متكامل ومحكم : يتطلب دمج إجراءات الأمن السيبراني في جميع جوانب النظام الضريبي، بدءًا من تصميم الأنظمة وصولًا إلى عمليات التدقيق والمتابعة، لضمان سلامة وفعالية النظام ككل.

مراجع الورقة البحثية

أ) المراجع باللغة العربية

شحاتة ، محمد موسى . (٢٠٢٠) . دور تفعيل آليات التحول الرقمي في تحسين كفاءة النظام الضريبي المصري كمرتكز للحد من التهرب الضريبي في ضوء رؤية مصر ٢٠٣٠ م . المجلة العلمية للدراسات والبحوث المالية والادارية ، ٦ (١) ، ص ١ ـ ٦٢ .

عبدالفتاح ، عمرو عادل . (٢٠٢٤) . قياس أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك . المجلة العلمية للدراسات والبحوث المالية والادارية ، ١٦ (٤) ، ص ٤١٧ ـ ٤٦٥ .

شرف ، الشيماء فؤاد . (٢٠٢٤) . نموذج مقترح لتعزيز كفاءة التحصيل الضريبي باستخدام استراتيجيات الأمن السيبراني . المجلة العلمية للبحوث و الدراسات التجارية ، ٣٨ (٤) ، ص ٤٢١ : ٤٨٠ .

الحيمودي ، بدر . (٢٠٢٣) . الأمن السيبراني وحماية الأنظمة المعلوماتية . مجلة شمال إفريقيا للنشر العلمي ، ص ١٧٤ : ١٨٩ .

خليفة ، محمد يوسف عبدالرحيم . (٢٠٢٢) . أثر التحول الرقمي لمنظومة التحاسب الضريبي المصرية في دعم حصيلة الايرادات الضريبية . المجلة العلمية للدراسات التجارية والبيئية ، ١٣ (٣) ، ص ٣٢٥ ـ ٣٦٦ .

أمير ، نهى علي . (٢٠٢٣) . الأمن السيبراني في استراتيجية الامن القومي الروسي . افاق اسيوية ، ٧ (١١) ، ص ١٦٨ : ١٩٦ .

قامش ، محمد ابراهيم . (٢٠٢٤) . أثر استخدام أسلوب التكليف العكسي للمحاسبة عن أنشطة صانعي المحتوى الرقمي بهدف ترشيد التحاسب الضريبي . مجلة البحوث المالية والتجارية ، ٢٥ (٤) ، ص ٣٠٧ : ٣٢٨ .

ابوالعينين ، احمد سعد محمد . (٢٠٢٤) . أثر تطبيق منظومة الفاتورة الإلكترونية على جودة معلومات التحاسب الضريبي والحد من الآثار السلبية للتهرب الضريبي في مصر . المجلة العلمية للدراسات والبحوث المالية والادارية ، ٥ (١) ، ص ٣٢٢ : ٣٨٤ .

صليبي ، رعد خضير . (٢٠٢٤) . تعزيز الامن السيبراني في العراق . مركز الدراسات الاستراتيجية والدولية ، ٩٩ ، ص ٥٠٥ : ٥٢٨ .

عبد الكريم ، أحمد . (٢٠٢١) . تحليل دور الأمن السيبراني في حماية المنظومات الحكومية حالة النظام الضريبي المصري . مجلة الأمن السيبراني ، ١٥ (٢) ، ص ٦٠ ـ ٧٢ .

منصور ، محمد . (٢٠٢٠) . التحول الرقمي في النظام الضريبي المصري التحديات والأمن السيبراني . المجلة العربية للدراسات الاقتصادية ، ٢٢ (٤) ، ص ٩٥ – ١١٠ .

ب) المراجع باللغة الإنجليزية

Florackis, Chris. (2022). Cybersecurity risk. National Bureau of Economic Research, 36 (1), 2-40.

Alharkan, I. (2020). Cybersecurity and Taxation: A Comprehensive Overview. Journal of Taxation Technology, 35 (2), 75-88.

Benkhelifa, E., & O'Rourke, M. (2019). The Role of Cybersecurity in Protecting Digital Tax Systems. International Journal of Cybersecurity, 10 (4), 215-230.

Saleh, A. (2021). Securing Tax Data: The Importance of Cybersecurity Strategies in Modern Tax Systems. Journal of Digital Taxation, 12 (1), 45-58.

Ibrahim, M. (2022). Tax Compliance and Cybersecurity: Integrating Technology for Effective Taxation. Taxation & Technology Review, 8 (3), 113-127.

Rahman N. A. A, Sairi 1. H., Zizi N. A. M., and Khalid F. (2020). The Importance of Cybersecurity Education in School. International Journal of Information and Education Technology, 10 (5), 378-382.