ورقة سياسات أمنية

الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

م.د. علي احمد عبد مرزوك
عضو هيأة تحرير/ المجلة العلمية لجهاز
مكافحة الارهاب

ورقة سياسات امنية

الأمن السيبراني

درع التحول الرقمي العراقي

(بين التحديات الراهنة وضرورات المستقبل)

م.د. علي احمد عبد مرزوك
عضو هيأة تحرير/ المجلة العلمية لجهاز
مكافحة الارهاب

تاريخ الاستلام: 2023/7/1 ، تاريخ: الارجاع: 2023/8/10 ، تاريخ الموافقة: 2023/9/15

يعد برنامج الحكومة الالكترونية عنصراً حيوياً لإصلاح وتحديث القطاع العام في العراق، وبذلك اعتمدت الحكومة العراقية على الاخذ بحوكمة التحول الرقمي سعياً للانتقال الى (دولة بلا ورق) في المعاملات الإدارية وتقديم الخدمات الى المواطنين، انسجاماً مع استراتيجية التنمية الوطنية والأهداف الإنمائية العراقية، ويواجه العراق العديد من التحديات في هذا المجال على المستويات البشريّة والتشريعيَّة والفنيَّة.. وغيرها ما أدى الى تموضع العراق في مراكز متأخرة في مؤشرات الحكومة الالكترونية الصادرة عن الأمّم المتحدة، زيادة على ما تقدم فقد واجه العراق تحديات كبيرة في مجال الفضاء السيبراني، فابتداءً من العزلة الدولية التي مر بها قبل عام (2003)، والعزلة المحلية عن العالم الخارجي التي فرضها النظام السابق، ومروراً بالأزمات التي تلت هذا العام من عدم الاستقرار على كافة المستويات، جعلته في حالة ضعيفة وغير قادر على امتلاك القدرات المطلوبة للتكيف مع تلك التحديات التي يفرضها واقع الفضاء السيبراني أو الاستعداد للانتقال من الفضاء الحقيقي إلى الفضاء الافتراضي.

وبالتالي وضع العراق أمام هذا الفضاء الواسع وسريع الحركة دون أن يمر بمراحل انتقالية، فالبنى المادية والبشرية في العراق ماتزال غير قادرة على التفاعل أو حتى المواكبة، مع تلك التحديات العديدة للفضاء السيبراني، وبالرغم من اقدام العراق على تبني

سياسيات ومشاريع رقمية تهدف باتجاه التحول نحو حوكمة التحول الرقمي ضمن مشاريع السياسات العامة العراقية لمجلس الوزراء العراقي؛ إلا ان العراق يواجه تحدٍ استراتيجي وامني بالغ الخطورة يضمن أمن وسلامة البيانات الرقمية العراقية ضمن منظومة أمن سيبراني متكاملة ومحصنة ضد الهجمات السيبرانية، على أساس ما تقدم سنتناول في هذه الورقة اهم التحديات والفرص المستقبلية للأمن السيبراني العراقي، عبر المحاور الآتية:

المحور الأول: الفضاء الالكتروني

تتطلب تهديدات الإنترنت المتزايدة في العالم من الإدارات العامة التركيز على تدابير أمن الحوكمة الإلكترونية، وإدراك التهديدات التي تتعرض لها، وعلى المؤسسة المنسقة وضع قواعد وتدابير أمن المعلومات ذات الصلة ومراقبتها والإشراف عليها، وينبغي إنشاء مؤسسة معينة على شكل فريق استجابة لطوارئ الكمبيوتر/ فريق استجابة للأحداث السيبرانية، وإنشاء عمليات تدقيق مناسبة، ويجب أن تكون جميع الوزارات والسلطات على دراية بالإجراءات الأمنية المناسبة وأن تستخدمها، وينبغي إنشاء إطار لأمن الفضاء الإلكتروني ونظام التدابير الأمنية بموجب قوانين[1].

اولاً: التحديات

تقر المؤسسات الحكومية بالحاجة إلى سياسات أمن إلكتروني جادة وتتخذ التدابير المناسبة بقدر ما تسمح به مواردها المتاحة ولكن في كثير من الحالات لا تسمح مخصصات تمويل تكنولوجيا المعلومات والاتصالات بإجراءات أمنية منسقة، ولذا تترك مسؤولية الاستعداد للتهديدات الالكترونية ومكافحتها للأفراد المعنيين بتكنولوجيا المعلومات والاتصالات أو تسند إلى شركات من القطاع الخاص مسؤولين أيضاً عن البنية التحتية للمؤسسة، وانسجاماً مع حاجة العراق الى الأمن السيبراني تأسس فريق الاستجابة الوطني للحوادث السيبرانية لمواجهة أحداث القضاء الالكتروني في العراق تحت إشراف مستشار الأمن الوطني العراقي، ولكن ليس لهذا الفريق حضور عام نشط، حيث لم يحدث موقعه الالكتروني وقناته على وسائل التواصل الاجتماعي منذ تأسيسه في العام ٢٠١٩.

أدى عدم وجود سياسة متماسكة لأمن المعلومات إلى عدم احتفاظ بعض المنظمات باتصالات خارجية عبر الإنترنت أو تقديم خدمات إلكترونيّة ممكنّة أخرى خوفاً

من عدم القدرة على التعامل مع الحوادث السيبرانيّة المحتملة، فضلاً عن ذلك لا يوجد لدى العراق تشريعات محددة للتعامل مع الجرائم السيبرانيّة، ويستخدم قانون العقوبات رقم (111) لسنة 1969 وقانون مكافحة الإرهاب لمكافحة الجرائم السيبرانية والالكترونية، وفي العام 2010 توصلت جامعة الدول العربية والعراق ضمناً، الى اتفاق بشأن الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات، وكان القصد وضع سياسّة جنائيّة مشتركة بشأن الهجمات الالكترونيّة غير القانونيّة والجرائم المماثلة في الدول العربية[2].

وعلى الرغم من إقرار وثيقة أمن المعلومات ومشاركة البيانات، إلا أنه لم توجد جهة معينة مسؤولة على تطبيق الفقرات الخاصة بأمن المعلومات، وتشكلت وأُلغيت اللجنة الفنية للاتصالات والمعلوماتيّة، ثم أُعيد تشكيلها، كما أن ملف الأمن السيبراني يشهد تقاطعات بين كثير من المؤسسات الحكومية التي هي: (الأمن الوطني، والمخابرات، والاتصالات، ومستشارية الامن القومي)، وقد تم حديثاً تشكيل فريق لوضع المقترحات النهائيّة بشأن تشكيل اداري يعنى بالأمن السيبراني، وبانتظار تحديد المهام وتهيئة المتطلبات الضروريّة لذلك، وهناك في جهاز المخابرات فريق الاستجابة للأحداث السيبرانية، يقدم دعماً في هذا المجال، لكن يتطلب المزيد من الأدوات والتقنيات والاتفاقيات مع جهات دولية لتحقيق امناً سيبرانياً عالي المستوى، فضلاً عن النقص في المعرفة لدى موظفي المؤسسات في موضوع الأمن السيبراني، وعدم ادراكهم لخطورة تسريب البيانات أو قرصنة حساباتهم، فمثلاً الموظف يضع كلمة مرور (1 2 3 4 5 6)، أو يعطي كلمة المرور الخاصة به الى زميله الآخر في العمل، وغيرها من الجوانب التي تُعرض الحسابات للاختراق بسبب الاهمال وعدم المعرفة.

ثانياً: الضرورات المستقبلية

تطرح الورقة جملة من الفرص والتدابير في مجال أمن الحوكمة الالكترونيّة عبر النقاط الآتية:

1. تكليف فريق الاستجابة الوطني بإدارة الحوادث السيبرانية والإبلاغ عليها، إلى جانب تحسين رؤية أنشطتهم من أجل زيادة الوعي العام تحديد الحد الأدنى من متطلبات أمن الفضاء الإلكتروني لسلطات القطاع العام ومقدمي الخدمات الحيويّة،

وتحديد البنية التحتيّة الحيوية بوضوح وتطبيق الحد الأدنى من متطلبات الأمن السيبراني، وأن يلتزم مقدمو الخدمات الرقمية ومشغلو الخدمات الأساسيّة بإخطار السلطات الحكومية المعنية بأي حوادث تمس الأمن السيبراني.

2. اعتماد تحليل موحد وآلية اعتماد موحدة لسياسة الأمن السيبراني وتفعيل استراتيجية الأمن السيبراني العراقية في جميع مؤسسات الدولة، وينبغي تحديد مسؤوليات مؤسسية متخصصة، مثل ضرورة إدارة التهديدات مركزيا وإيجاد تعاون دولي فعال.
3. تزويد المؤسسات العامة بالموارد اللازمة لضمان البنيّة التحتيّة للأمن السيبراني، وأن تشمل الموارد تمويلاً كافياً للموظفين وبرامج تدريب إضافية لجميع الموظفين العموميين ومكونات البنيّة التحتيّة الأساسيّة لضمان المستوى الأساسي للأمن السيبراني.

المحور الثاني: الإمكانات اللوجستية والبنى التحتية

انطلاقاً من مبدأ أن (الأمن السيبراني درع التحول الرقمي العراقي) فان توفير البنى التحتية للأمن السيبراني شرط أساسي للحكومة الالكترونيّة، وتحقيق حد أدنى من قدرة البنى التحتية لتكنولوجيا المعلومات والاتصالات ضروري لتنفيذ مشاريع الحوكمة الإلكترونية وتأمينها، بالإضافة الى ذلك تشكل التحديات التقليدية كالحروب والأزمات وعدم الاستقرار العام وكل ما يمس الأمن الوطني العراقي من تهديدات داخلية أو خارجية، عائقاً أمام مواكبة العالم الحديث المتمثل بالتقدم التكنولوجي والتقني وغيرها من العلوم الحديثة والتي ظهرت تلبية لمتطلبات تثبيت أركان الحكومة الإلكترونية وتعزيز ديمومتها وتحصينها من المخاطر السيبرانية، ويمكن أن تكون مواكبة إستراتيجية وعمليات الأمن السيبراني تحدياً يتمثل في قدرة الدولة على التكيف مع التغيير السريع في المجالات العامة عموماً، لا سيما في شبكات الحكومة والمؤسسات العامة والخاصة، فغالباً ما تستهدف التهديدات السيبرانية الأصول السرية أو السياسية أو العسكرية أو البنية التحتية للدولة.

اولاً: التحديات

إن غياب مكونات البنية التحتية للأمن السيبراني أو عدم كفايتها في المؤسسات الحكومية هو أحد التحديات الرئيسة أمام الأمن السيبراني العراقي وتسهيل الاتصالات في المؤسسات، ويتعلق ذلك بقلة التخصيصات المالية المرصودة، وتقادم الأجهزة بسبب اجراءات التقشف المالي التي تزامنت مع أحداث 2014.

ثانياً: الضرورات المستقبلية

تطرح الورقة جملة من الفرص في هذا المجال إذ من الضروري أن تتعاون الحكومة العراقية مع القطاع الخاص والشركات الدولية لتطوير البنى التحتية للأمن السيبراني العراقي، بالإضافة الى تبني مشاريع مشتركة تنموية على المستوى الإقليمي والدولي، ويشمل ذلك الوصول الى آليات التمويل العام لتعزيز البنى التحتية وديمومتها.

المحور الثالث: إدارة البيانات وتأمينها

تشكل البيانات عنصراً رئيسياً في الأمن السيبراني، حيث أن كل تفاعل في البيئة الرقمية يولد بيانات ويعتمد اعتماداً كبيراً على توفر البيانات في صيغة رقمية، ويتطلب تعزيز حوكمة التحول الرقمي أن تفهم الحكومات بشكل أفضل نوع البيانات المتاحة وسبل تأمينها، وكيف يمكن مواءمة هذه البيانات واستخدامها لخلق قيمة في القطاع العام وفي المجتمع ككل[3].

اولاً: التحديات

ما تزال إدارة البيانات في العراق وتأمينها في حالة تطور، وان المؤسسات الحكومية لا تملك فكرة عن البيانات العامة المتوفرة ولا تطبق أي آليات واضحة لجمع البيانات، ولكل وزارة او مؤسسة حكومية مبادئها الخاصة بشأن صيغ البيانات واستخدامها وطرق تأمينها، ما يجعل التعاون بين المؤسسات واتخاذ القرارات التي تعتمد على البيانات أمراً صعباً، ولا توجد مبادئ واضحة للبيانات المفتوحة العامة أو منافذ جاهزة، اذ يجمع الجزء الأكبر من البيانات ويحفظ على الورق ولكن يتم إنشاء أنظمة إدارة الوثائق داخل المؤسسة بشكل متزايد، ما يسمح بمعالجة صيغ البيانات الإلكترونية، وعادة ما تدار قواعد

البيانات في المؤسسات التي تجمع فيها البيانات الإلكترونية وفق حلول مرخصة أو متاحة دولياً مثل Oracle أو MySQL، ولكنها تستخدم في بعض الحالات الحلول القديمة مثل MS access أو حلول بسيطة .MS Excel

بناءً على المعلومات المتاحة للعموم على الموقع الإلكتروني للجهاز المركزي للإحصاء يبدو أن المعلومات التي جمعت عن التكنولوجيا والحكومة الإلكترونية قد تضمنت مسوحات لسنوات متفرقة هي مسح تكنولوجيا المعلومات للعام (2008) والعام (2011) والعام (2022) ولكن لم تتضمن تلك التقارير أساليب محدثة معنية بأمن المعلومات وتوفر احصائيات عن مدى خطورة هذا القطاع لتنبيه صناع القرار ورفد صناع السياسات بالأرقام والاحصائيات ذات العلاقة بالأمن السيبراني[4].

ثانياً: الضرورات المستقبلية

تطرح الورقة جملة من الفرص والتدابير في مجال إدارة البيانات وتأمينها عبر النقاط الآتية:

1. **جمع البيانات ومعالجتها وتخزينها بصيغ رقمية:** ينبغي إعطاء الأولوية لرقمنه الوثائق والبيانات الورقية الموجودة لأن ذلك يشكل الشرط الأساسي للتنمية المستندة إلى البيانات، ينبغي التركيز على رقمنه وجرد البيانات الأساسية الإلزامية عن السكان (أي السجل المدني) والشركات والأراضي والممتلكات.
2. **وضع لائحة شاملة لإدارة البيانات عابرة للحكومة:** عبر تحديد قواعد استخدام البيانات والوصول إليها وملكيتها كشرط أساسي للتشغيل العملي للحوكمة الإلكترونية وتأمينها في الفضاء السيبراني، وأن يعطي تنظيم إدارة البيانات الأولوية لرقمنه المستندات الحالية والبيانات الورقية كشرط أساسي للتطوير المُستند إلى البيانات، وأن تدار البيانات في مراكز البيانات وفق مبادئ راسخة وخاضعة للإشراف بما في ذلك قواعد أمن الفضاء الإلكتروني وحماية البيانات وإدارة قواعد البيانات الآمنة.
3. **ترتيب جرد لأصول المعلومات:** وأن تملك الحكومة فكرة واضحة عن نوع ومحتوى البيانات التي تجمع في كافة المؤسسات، ونوصي بإجراء جرد للسجلات وجرد

المستندات المراد رقمنتها وتحديد أنظمة المعلومات وقواعد البيانات والخدمات وأصول المعلومات الموجودة، وأن يرتبط مكون البيانات الوصفية بالبيانات المجمعة لتوفير الإمكانيات الأساسية للاستخدام التبادلي وتحديد التوصيف، وهذا يوفر فرصة أساسية لاستخدام البيانات وتبادلها المدروس بين المؤسسات.

المحور الرابع: الدعم والتعاون الدولي

من اجل الاستفادة من المزايا التي يوفرها التعاون الدولي في ميدان العلاقات الدولية للأمن السيبراني، من المهم ان التشارك الدول في التعاون الإقليمي والدولي، فهذا التعاون يساعدها في تبادل الدروس المستفادة وبناء مشاريع مشتركة وحتى الدخول في اتفاقيات دولية او اتحادات دولية لغرض الأمن السيبراني.

اولاً : التحديات

لا يمكن التقليل من قيمة التعاون الدولي سواء من حيث تبادل الممارسات الجيدة أو الموارد المالية التي قد ينطوي عليها الأمن السيبراني، ولكن الحصول على المساعدة الدولية والاستفادة منها بشكل كامل يتطلب امتلاك القدرات الداخلية والاستعداد، وتتولى حالياً لجنة التنمية الدولية المشكلة حديثاً ضمن الأمانة العامة لمجلس الوزراء تنسيق قضايا التنمية الدولية والمشاريع ذات الصلة، وحتى هذه اللحظة لم تفعل آلية التعاون الدولي ببرامج ومذكرات تعاون حقيقية، وحتى لو كان هنالك امثلة لجهات دولية قد تعاونت مع العراق بشأن الامن السيبراني لكن لم تكن مثمرة ولم تحقق المستوى المطلوب.

ومن ابرز امثلة التعاون الدولي توقيع الحكومة العراقية في العام 2021 مذكرة تفاهم مع مصر في مجال تكنولوجيا المعلومات والاتصالات بهدف تبادل الخبرات في عدد من المجالات كالبنية التحتية للاتصالات والتحول الرقعي وبناء القدرات والابتكار، وأمن الفضاء الإلكتروني، والتشريع والإطار التنظيمي... إلخ.

بالإضافة إلى ذلك، أنشأ البلدان شركة مشتركة لتنفيذ مشاريع التحول الرقمي وتطوير الخدمات الإلكترونية، كما وضعت مجموعة البنك الدولي إطاراً للشراكة القطرية لجمهورية العراق للفترة المالية ٢٠٢٢-٢٠٢٦ تم تنظيمه لتحسين الحوكمة الالكترونية وتقديم الخبرات وتعزيز رأس المال البشري ولكن ابتعدت تلك الشراكة عن آليات التعاون

السيبرانية، حيث تضمنت لائحة الشراكة تغطية خمس عمليات رئيسية تشمل إقامة نظام مالي متكامل ونظم للمعلومات الإدارية، والحوكمة، وتبسيط ممرات التجارة والنقل، وتطوير أنظمة الري والموارد المائية، وامدادات المياه والصرف الصحي[5].

ثانياً: الضرورات المستقبلية

تطرح الورقة جملة من الفرص والتدابير في مجال التعاون الدولي عبر النقاط الآتية:

1. ينبغي ان تضع الحكومة استراتيجية واضحة للتعاون الدولي والشراكات في مجال تكنولوجيا المعلومات والاتصالات، وان تصوغ الاحتياجات التفصيلية للمواضيع ذات الأولوية للتعاون الدولي وان تضع اطاراً لمؤسسة معينة تتولى مسؤولية التعاون السيبراني.
2. على الحكومة العراقية أن تضمن تمثيل السياسة الخارجية والعلاقات الدولية بشكل جيد في القنوات السيبرانية، وعرض اهتمامات الامن السيبراني في العراق على الدول الاخرى والمنظمات الدولية وكذلك الشركات التكنولوجية، ويوصى بتوقيع مذكرات تفاهم مع نقاط عمل محددة بشأن المبادرات الرقمية مع الحكومات ذات الأهداف الرقمية المشتركة، والبحث بنشاط عن فرص التعاون الرقمي مع المنظمات الدولية التي تقدم الكفاءات المناسبة والنماذج المرجعية والدعم في المبادرات الرقمية.

نظراً لانعدام الرؤية المستقبلية وضعف القيادة الإدارية التي تمر بها منظومة التخطيط الإستراتيجي للعراق، التي تمثل أحدى السمات الرئيسية للعصر الحديث، بات التخبط واضحاً في مخرجات الإدارة التي انعكست على المسيرة التنموية للفرد والدولة العراقية، لاسيما أن العراق في هذه المرحلة الحساسة يحتاج إلى رؤية تخطيطية واضحة وشاملة لحوكمة التحول الرقمي والامن السيبراني، من خلال وضع برنامج حكومي ثابت الأركان مع أساليب تخطيطية واجب اتباعها لمواجهة تحديات المرحلة القادمة وتحقيق الأهداف الوطنيّة المنشودة، بمعنى التفكير والتخطيط قبل الأداء بوضع حلول لمشكلات

الدولة العراقية لتحسين أداء المنظومة الإستراتيجية الخاصة بالتحول الرقمي والامن السيبراني في ضوء الإمكانات المتاحة.

فضلاً عن ذلك إن منظومة الأمن الوطني للعراق، تواجه جملة من التحديات التي يمكن تصنيفها بالتحديات المرئية (التقليدية) وغير المرئية (السيبرانية)، وتتجلى أخطرها بتلك التي تتمظهر بالصورة غير المرئية، فلا يمكن التماسها بصورة مباشرة إلا عن طريق البحث والاستقراء التحليلي والتقني، وتشكل هذه التحديات تهديداً إستراتيجياً من شأنها أن تؤثر على الأمن الإستراتيجي (للفرد والدولة) فضلاً عن مسيرة التحول الرقمي الذي تسعى الى تحقيق الحكومة.

وبالتالي ان هذه التحديات في التحول الرقمي ستشمل معظم القطاعات والمؤسسات الحكومية وغير الحكومية، التي تتمحور حول البنية التحتية الارتكازية للدولة لتصل إلى الأمن الإدراكي للمواطن، وتتراوح هذه التحديات ما بين التهديدات السيبرانية للمنظومة الرقمية للدولة، وزيادة عدد السكان من دون أن يصيب هذه الزيادة تخطيط إستراتيجي يواكب التطورات والتحديات المحدقة بمؤسسات الدولة الرسمية وغير الرسمية، فتشكل تحدياً كبيراً لمنظومة الأمن الإستراتيجي للعراق، وبالتالي باتت الضرورة الملحة في تركيز الجهود البحثية والاستشرافية وتسلطها في هذا المجال، لاسيما في ظل الزيادة الملحوظة للتحديات المحدقة بمنظومة الأمن الوطني العراقية بشقها السيبراني لارتباطه وتماسه المباشر مع باقي قطاعات الأمن للدولة.

المصادر والمراجع

(1) علي احمد الخوري، الحكومة الرقمية: مفاهيم وممارسات، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، 2018، ص203.

(2) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، القاهرة، 2010، ص17.

(3) منتدى القمة العالمية لمجتمع المعلومات 2021، تقرير خطوات عمل القمة العالمية لمجتمع المعلومات، شبكة المعلومات الدولية (الانترنت)، على الرابط:
https://www.itu.int/net4/wsis/forum/2021/ar/Home/Outcomes.

(4) مسح استخدام تكنولوجيا المعلومات والاتصالات للاسر والافراد لسنة 2022، مديرية اصحاء النقل والاتصالات، وزارة التخطيط والتعاون الإنمائي، الجهاز المركزي للإحصاء، 2023، ص7-10.

(5) وثيقة مجموعة البنك الدولي، استراتيجية الشراكة مع جمهروية العراق للسنوات المالية 2022-2026، البنك الدولي، 2022، ص9.