مجلس الوزراء
مركز المعلومات ودعم اتخاذ القرار



عـــالـم التكنولوجيا

السنة (1) – العدد (1) – مارس 2020

عالم التكنولوجيا



في ظل ما يشهده العالم اليوم من ثورة علمية وتكنولوجية هائلة كأحد مظاهر العولمة التكنولوجية، أصبحنا نجد العالم في سباق محموم من أجل مواكبة هذه الثورة التي تعد أهم معالم اللحظة الحضارية الراهنة، والتي تمثل تحديا حقيقيا يواجه الدول النامية، تلك الثورة لم تكن لتتحقق لولا العلم الذي أصبح اليوم الحقيقة الأساسية في الحياة، والمحور الذي تدور حوله كل الحقائق الحياتية الأخرى.

ولقد بدّلت الثورة العلمية والتكنولوجية كثيرا من الأفكار والمفاهيم والمسلمات القديمة في مختلف مجالات الحياة؛ لذا يجب على تلك الدول أن تستفيد من الميزات الجديدة التي يقدمها ذلك التطور التكنولوجي؛ لتتمكن من استيعاب المعرفة الجديدة وفهمها والتفاعل معها، والعمل على توظيف هذه الثورة المعلوماتية لخدمة أهدافها وتوفير احتياجات شعوبها بأساليب متقدمة، ولتتمكن– كذلك– من اللحاق بركب الدول المتقدمة.

لذا، تأتى نشرة عالم التكنولوجيا كمبادرة من مركز المعلومات ودعم اتخاذ القرار برئاسة مجلس الوزراء المصري؛ لإلقاء الضوء على التطورات في مجال تكنولوجيا المعلومات، والتحول الرقمي وتأثيره في مختلف القطاعات.

هذا، وتستعرض النشرة تأثير التقدم التكنولوجي على فكر الحكومات في دول العالم، ومردوده على المجتمعات وتنمية البشر، كما تستعرض النشرة أيضاً تجارب دولية وعربية عن تطبيقات تكنولوجيا المعلومات، وأهم المفاهيم الحديثة في مجال التكنولوجيا.

عـــــالـم التكنولوجيا

نشرة شهرية تصدر عن مركز المعلومات ودعم اتخاذ القرار – مجلس الوزراء

السنة (1) – العدد (1) – مارس 2020

فريق العمل

رئيس التحرير
م/ أسامة الفيومى

إخراج فنى
م/ وليد جادو

إعداد ومراجعة المحتوى الفنى
د/ فتحى شمس الدين

المراجعة اللغوية
د/ محمود حنفى

إعداد ملف العدد
م/ إيمان محمود ـ م/ محمد السيد

التصميم الجرافيكي
م/ آيات مكي

كُتَّاب عالم التكنولوجيا



د/ فتحي شمس الدين
خبير الإعلام الشبكي

الدولة الذكية ومستقبل شبكات التواصل الاجتماعي



م/ وليد حجاج
خبير أمن المعلومات

مفهوم الحوكمة وأثرها الإيجابي



د/ شريف درويش اللبان
خبير الإعلام الرقمي

وزارة جديدة للقوة الناعمة للدولة المصرية



د/ حسن عماد مكاوي
أستاذ الإعلام وخبير تكنولوجيا المعلومات

الاتصال عبر الفضاء



حامد حسن
خبير تكنولوجيا المعلومات

**ما التحول الرقمي ؟
اكتشاف الحقيقة وراء هذه الكلمة الطنانة**



م/ إسلام غانم
استشاري تكنولوجيا المعلومات

عصر التفوق الكمي



م/ محمد مصباح محمد
باحث واستشارى أمن المعلومات

تأمين البنية التحتية للدول (المخاطر والتحديات)



محمد منير غازي
باحث معلوماتي في مجال المناهج وطرق التدريس

كيف نُعد أبناءنا لمواجهة سيطرة الروبوتات على وظائف المستقبل؟

المحتويات



موضوع العدد

الأمن السيبراني
Cyber Security

22

مصطلحات تكنولوجية

26



28

إصدارات تكنولوجية حديثة



د/ فتحي شمس الدين
خبير الإعلام الشبكي

الدولة الذكية
ومستقبل شبكات التواصل الاجتماعي



أصبحت شبكات التواصل الاجتماعي جزءا أساسيا من أسلوب حياة الأفراد في كل مكان في العالم؛ حيث إن شبكات التواصل الاجتماعي والهواتف الذكية لا يمكن لأحد أن يتخيل يومه دون استخدامهما في التواصل أو القيام بالمهام اليومية بشكل عام، ومع ذلك الانتشار الكبير لشبكات التواصل الشبكي ظهر تغير هائل في سلوك الأفراد، الأمر الذي أربك العلماء – خاصة علماء الاجتماع– وذلك لظهور مفردات جديدة وأنماط سلوكية لم تكن موجودة، بالإضافة إلى ظهور شخصيات تمزج بين السلوك الإنساني والسلوك الإلكتروني الذكي، الأمر الذي أثار مخاوف كبيرة حول طبيعة مستقبل شبكات التواصل الاجتماعي، وتأثيراتها على الهوية الإنسانية، وانعكاساتها على مستقبل الحياة الاجتماعية بشكل كبير.

وتتمثل أهم خطورة في الفجوة المعلوماتية الكبيرة بين الدول، والتي ستمثل أكبر فجوة عرفها العالم في تاريخية ،حيث إن الاعتماد على شبكات التواصل الاجتماعي بشكل خاص وشبكة الإنترنت بشكل عام سيؤدي إلى تسارع دول وثقافات كثيرة نحو المستقبل، بينما تقبع دول أخرى في التأخر، وسيتم التعامل معها على أنها كائنات قديمة لا تنتمي للمستقبل؛ حيث إنه في المستقبل القريب ستتحول شبكات التواصل الاجتماعي لأكبر منصات إعلامية يعتمد عليها الفرد، وسيكون من خلالها العمل عن بُعد أحد الأنماط الوظيفية السائدة، وسيكون كسب المال في الفضاء الرقمي من أعلى الوظائف لدى الأفراد، الأمر الذي من شأنه دفع الدول والحكومات أن تعيد النظر إلى طبيعة تلك الشبكات وكيفية توظيفها في النهضة المجتمعية من خلال مفاهيم مثل «الحكومة الذكية»، حيث تستطيع الدول أن توفر منصات عبر شبكات التواصل الاجتماعي للتدريب والتأهيل، ومن ثم الدعم الإداري والفني والقانوني، والذى من شأنه أن يدفع الأفراد للاستثمار عبر تلك الشبكات؛ حيث إن توفير الوظائف لكل أفراد المجتمع أصبح شيئاً في غاية الصعوبة، لكن توفير تلك الفرص عبر البيئة الرقمية الحديثة سيكون أمرا في غاية السهولة، ويمكن من خلاله استيعاب الأعداد الكبيرة من الأفراد.

وعلى الرغم من أهمية شبكات التواصل الاجتماعي والبيئة الرقمية بشكل عام خاصة في النواحي الاقتصادية والمعرفية، إلا أنك تجد كثيراً من الدول والحكومات لا تدرك أهمية تلك الوسائط الجديدة، وتتعامل معها بعقلية إدارة الأعمال التي عفا عليها الزمن، دون النظر إليها من خلال المفاهيم الحديثة والنظريات الجديدة، ودون معرفة حجم النمو العالمي في التجارة الإلكترونية، ومن الحقائق التي لا جدال فيها أن الدول التي لن تستطيع الاعتماد على البيئة الرقمية الحديثة ستكون متأخرة بصورة كبيرة، ولن يكون لها مكان في عصر المعلومات، وستكون أيضا أكبر عرضة للتفكك والاختراق.

إن استخدام وسائل التواصل الاجتماعي يعد قوة تمكين في يد القطاعين العام والخاص، حيث سيتم استخدام ذلك وربطه بالتنمية المجتمعية؛ لأنها ستكون من أهم أدوات صناعة مستقبل أفضل من خلال نشر الوعي الصحي العام، ونشر الوعي والاستقرار الأمني والروحي والقيمي والمجتمعي، والتمكين الاقتصادي وتعزيز الهوية الوطنية الافتراضية؛ حيث إن الإنسان مقبل على ثورة حقيقية بفضل وسائل التواصل الاجتماعي وتقنيات وتطبيقات الهاتف المحمول الذكي، وعليه فإن على الدولة والحكومة النظر بشكل مختلف لأهمية شبكات التواصل الاجتماعي، والعمل على توظيفها واستغلال إمكاناتها بالشكل الأمثل؛ حتى لا نجد أنفسنا بمثابة إنسان الكهف أمام التقدم التكنولوجي والمعلوماتي الكبير، فالدولة التي لن تكون ذكية معلوماتيا لن يتم النظر إليها ولا الاهتمام بها، وستكون عرضة للتفكك والاختراق.





م / وليد حجاج
خبير أمن المعلومات

الجدار الناري البشرى



انتشرت ظاهرة استخدام مواقع التواصل الاجتماعي من قِبل العاملين في مؤسسات الدولة المختلفة سواء على مستوى العمل، أو على المستوى الشخصي، أو من خلال أجهزة المؤسسة نفسها، حتى إن بعضهم يستخدمها لإرسال صور وأوراق مهمة قد تؤثر بالسلب على المؤسسة بل وعلى الدولة ذاتها ؛ وذلك نظرا لسهولة استخدام برامج ومواقع التواصل الاجتماعي؛ معتقدا أنه يضمن ـ بذلك ـ وصول الرسالة للشخص المطلوب بشكل سريع ومؤكد، وهنا تكمن المشكلة؛ لأن المرسل والمستقبل لهذه النوعية من الرسائل لا يملك من ثقافة الأمن المعلوماتي ما يؤهله لذلك، بل ولا يملك الضمانة بأن هذه المعلومات لن تصل إلى يد ثالثة قد تسيء استخدام هذه المعلومات سواء في حالة سرقة حسابه على مواقع التواصل أو حتى أثناء إجراء صيانة لهاتفه.

فهناك البعضُ ممن يعملون في مؤسسات البنية التحتية مثل الكهرباء أو المياه أو الغاز يقومون بتبادل المعلومات والصور أو المستندات المهمة التي قد تصل في بعض الأحيان إلى خطوط الشبكة أثناء قيام العامل بعمله؛ اعتقادا منه أنها أسهل وأسرع وسيلة للتواصل مع زملائه في المؤسسة، والتي قد تصل في بعض الأحوال لإرسال مستندات شخصية مهمة من خلال برنامج مثل الواتساب أو الفيسبوك ماسنجر؛ مما يجعل منهم هدفا سهلا لاستغلالهم وتسريب المعلومات والبيانات المهمة للمؤسسة،بل وأصبح كل من لديه حساب على الفيسبوك وبعض الخبرة القليلة في التعامل مع الإنترنت القيام بإنشاء صفحة أو جروب على مواقع

التواصل الاجتماعي التي يأتي على رأسها الفيسبوك، وذلك تحت مسمى العاملين بمؤسسة كذا أو نقابة كذا أو حتى للعاملين في إدارته، و يتم تبادل أطراف الحديث عن أسرار و تفاصيل المؤسسة من خلالها، فكيف يتم ذلك دون وضع ضوابط وقوانين من شأنها أن تحد من هذه الظاهرة التي أصبحت تُستغل في بعض الأحيان في نشر أخبار وأكاذيب وإشاعات قد تؤثر بالسلب على المؤسسات والقطاعات الحيوية بالدولة ؟!!!

فقد أصبح من ضروريات ما نشهده الآن من تحول رقمي لمؤسسات الدولة وربط قواعد بياناتها هو بناء ثقافة المواطن والعامل؛ لأن أضعف حلقة في أمن المعلومات هي الإنسان، وخط واحد كاف لاختراق المؤسسة، وحسب آخر تقارير وإحصائيات صدرت في يناير ٢٠٢٠ عن عام ٢٠١٩ فقد تم رصد أن معظم حالات الاختراق كانت من خلال استخدامات خطأ، واختراق لعقول الأشخاص معتمدين فيها على علم الهندسة الاجتماعية، وهو علم يعتمد على جمع المعلومات لاستهداف الدول والمؤسسات والأشخاص.

الحروب الآن بين الـدول أصبحت تعتمد على سياسة ذكية تستخدم فيها الهندسة الاجتماعية لدراسة سلوك الشعوب وعاداتهم من خلال جمع المعلومات وتصنيفها واستخدامها في هجوم لاحق، وبث معلومات مغلوطة أو خطأ من خلال محتوى أصبح مقبولا بعد أن كان غير مقبول في الأسـاس؛ لذلك فإن الجدار الناري البشري [Human firewall] ورفع الوعى لدى المواطنين من أهم خطوط الدفاع لأى دولة تعتمد على التكنولوجيا، ونظرا لأن الدولة المصرية تعمل جاهدة للتحول الرقمي، فقد حان الوقت لوجود منبر لنشر ثقافة التعامل السليم والآمن مع التكنولوجيا، وذلك من خلال عدة محاور وآليات، منها: عقد دورات وورش عمل تدريبية بشكل دوري للعاملين بكل القطاعات الحيوية بالدولة، والتي من شأنها رفع مستوى ثقافة الأمن المعلوماتي والتعرف على أحدث طرق الاستهداف التكنولوجي، وآليات التعامل السليم معها.

ومن أفضل الآليات في هذا الشأن التدريب على كشف خدع الاختراق، وذلك من خلال إنشاء خدع اختراق وهمية يتم إرسالها بشكل عشوائي للعاملين لاختبار ردود أفعالهم وتقييم أدائهم في التعامل معها، مع وضع ضوابط و ميثاق شرف مهني يحد من تداول المعلومات أو البيانات المؤسسية من خلال وسائل التواصل على أن تكون من خلال نظام داخلي خاص بكل مؤسسة، بل واستحداث لوائح وقوانين للحد من ظاهرة « جروبات الشركات » على مواقع التواصل، واستخدام برامج بديلة للتواصل بين العاملين في المؤسسة الواحدة، والتي من خصائصها ـ أيضا ـ الربط بين الشركات المتعددة، وتتيح نفس خصائص التواصل الموجودة في تطبيقات التواصل المتعارف عليها، و لكن من خلال خوادم مصرية داخل حدود الدولة المصرية.

في النهاية يجب خلق جيل واع ومستخدم جديد للتكنولوجيا؛ حتى نستطيع مواجهة الأجيال الجديدة من الحروب التي تعتمد على الإنترنت و تكنولوجيا المعلومات.



د/ شريف درويش اللبان
خبير الإعلام الرقمي

وزارة جديدة للقوة الناعمة للدولة المصرية

استخدمت الولايات المتحدة الأمريكية الثورة الرقمية كإحدى وسائل القوة الناعمة لتدمير القوى السياسية لعددٍ من الدول؛ للسيطرة على شعوب العالم، ولتدمير الحياة السياسية في هذه الدول، وهذا ما اتضح من خلال وسائل الإعلام الأمريكية التي لا تتناول أي أخبار متعلقة بقارة إفريقيا سوى الأخبار السلبية المتعلقة بالمجاعات والحروب والصراعات.

لقد طورت الولايات المتحدة بعد الثورة الرقمية من أساليبها للسيطرة على العالم، من خلال تأسيس شبكة الإنترنت وتضمينها لمفاهيم الليبرالية والديمقراطية بالمفهوم الأمريكي، لإحداث تغيير في أنظمة الحكم في دول العالم الثالث بالطريقة التي تريدها الولايات المتحدة، دون تدخل للقوة الصُلبة أو العسكرية لإحداث هذا التغيير، وهو ما يندرج تحت مفهوم حروب الجيل الرابع.

وليس سرًا أنه توجد خطة أمريكية متكاملة تسعى من خلالها واشنطن لـ «عولمة» خِدمات الإنترنت، وذلك من خلال توفير تلك الخدمة لأية دولة في العالم من خارج حدودها باستخدام شبكة من الأقمار الصناعية لتوصيل خدمة الإنترنت إلى كل دول العالم متخطيةً أنظمة الاتصالات المحلية في كل دولة على حدة، وقدرة الدولة على التحكم في الاتصالات داخل حدودها، بما في ذلك تلاشي قدرة الدول على حجب المواقع التي تهدد كيانها.

إن ثورة ٢٥ يناير لم تكن لتحدث دون توافر الأرضية الخصبة من تراجع المجالات السياسية والاقتصادية في أواخر عصر مبارك، إلا أن الإنترنت ومواقع التواصل الاجتماعي قد تم استخدامهما لتحقيق الأهداف الأمريكية بإطلاق شرارة الثورة في مصر وثورات الربيع العربي بشكل عام، والتي كان بعض النشطاء الذين شاركوا فيها عملاء تم توظيفهم لتحقيق أهداف أمريكية.

ولعل هذا الأمر هو الذي أدى إلى تعامل عددٍ من الدول على مستوى العالم بحذرٍ شديد، نظرًا للتأثيرات السلبية لمواقع التواصل الاجتماعيٍ الأمريكية مثل الصين وكوريا الشماليةٍ، وهما يعتمدان على مواقع التواصل الاجتماعي المحلية ولم تلجأ هذه الدول مطلقًا لمواقع التواصل الاجتماعي الأمريكية.

إن استخدام مواقع التواصل الاجتماعي الأمريكية في أعمال التنظيمات الإرهابية وعلى رأسها تنظيم «داعش» الإرهابي لم يكن من قبيل الصُدفة، ولكنه كان مقصودًا من قِبَل الولايات المتحدة الأمريكية، لصناعة جماعات إرهابية تتوافق مع عصر ما بعد الحداثة، لتأجيجِ الصراعات الطائفية والمذهبية والعرقية لصالح الكيان الصهيوني في المنطقة العربية.



إن الدولة المصرية في حاجة ملحة الآن إلى أن تنتقل من موقع الدفاع إلى موقع الهجوم باستخدام المقومات الأساسية لقوتها الناعمة، وإن تفعيل مقومات القوة الناعمة للدولة المصرية لا يمكن أن يتم بمجهودات فردية مبعثرة، بل يجب أن يتم بمجهودات جماعية تنضوي تحت منظومة فاعلة، ويكون لها أهدافٌ محددة في إطارٍ زمني واضح، اعتمادًا على قطاعٍ الشباب في تفاعله الدؤوب والمُبدع مع أجهزة الكمبيوتر والإنترنت وشبكات التواصل الاجتماعي وتكنولوجيات العصر كافة، ومن هنا فإنني أقترح أن يتم استحداث وزارة جديدة للقوة الناعمة للدولة المصرية.

وبينما نناقش القوة الناعمة للدولة المصرية ونقترح إمكانية تنسيقها من خلال وزارة أو كيَانٍ مؤسسي، بدأت بعض الدول العربية الشقيقة في استيعاب مفهوم «القوة الناعمة»، وبدأت في استكشاف مصادر هذه القوة، وبدأت في اتخاذ خطوات جادة في تمكين قوتها الناعمة من الترويج لها، وعلى رأسِ هذه الدول الإمارات العربية المتحدة.

وقد أعلن الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي في ٢٩ أبريل ٢٠١٧ تشكيل «مجلس القوة الناعمة لدولة الإمارات العربية المتحدة» والذي يهدف لتعزيز سمعة الدولة إقليميًا وعالميًا، وترسيخ احترامها ومحبتها بين شعوب العالم، ويختص برسم السياسة العامة واستراتيجية القوة الناعمة للدولة. هذا ويتبع مجلسُ القوة الناعمة بشكل مباشر مجلسَ الوزراء ويعمل على صياغة منظومة وطنية متكاملة تشمل الجهات الحكومية والخاصة والأهلية لنقل قصة الإمارات للعالم بطريقة جديدة.

لقد سبقتنا بريطانيا والإمارات العربية المتحدة في تنسيق جهود القوة الناعمة في كلا البلديْن، ومصر الحضارة والتاريخ والعلم والأدب والفنون والآثار والمساجد والكنائس والسياحة والشواطئ والزراعة والصناعة يجب أن تأخذ الخطوة التالية على مستوى العالم في هذا المضمار، فمصر تستحق الكثير على مستوى العالم، فهل تستجيب الدولة المصرية لمقترحنا بإنشاء وزارة جديدة للقوة الناعمة؟.



د / حسن عماد مكاوي
أستاذ الإعلام وخبير تكنولوجيا المعلومات

الاتصال عبر الفضاء



أصبحت ظاهرة التواصل عبر الشبكات الإلكترونية سمة واضحة في المجتمع المعاصر، وانتشر مصطلح «المجتمع الشبكي» وهو عبارة عن مزيج من الشبكات الإعلامية والاجتماعية الواقعية والافتراضية.

وقد ساعدت تطبيقات برامج الإنترنت على انتشار المجتمع الشبكي، حيث يتوفر كثير من بنوك وشبكات المعلومات في جميع مناحي الحياة الاجتماعية والثقافية والاقتصادية والسياسية والعلمية.

إضافة إلى تطبيقات الحكومة الإلكترونية التي تتيح تقديم الخدمات والتفاعل بين الأفراد والمؤسسات، فضلا عن إتاحة التعليم الإلكتروني، والتعلم مدى الحياة، وظهور التجارة الإلكترونية التي أتاحت فرصا جديدة للشركات المتوسطة والصغيرة والأفراد للدخول إلى سوق العمل المحلي والدولي.

كما أسهم المجتمع الشبكي في ظهور جماعات للضغط على السلطات الحاكمة للاستجابة لمطالبها مهما كان بها شطط أو مغالاة، وأتاح الفضاء الإلكتروني للأفراد إمكانية التفاعل مع الأحداث لحظة حدوثها، والتعليق على الأخبار بشكل فوري، وإمكانية المساهمة في الأنشطة المختلفة عبر مواقع التواصل الاجتماعي.

هذا ويتيح الفضاء الإلكتروني مجموعة من المميزات غير المسبوقة على مستوى التفاعل الفردي والجماعي، لعل من أبرزها إتاحة حرية التعبير عن الرأي في مختلف الموضوعات والقضايا الشائكة، وإشراك القوى الاجتماعية في التأثير علي القرارات ليتحول الأفراد من متلقين سلبيين إلى مشاركين إيجابيين في القضايا المجتمعية، وعدم اقتصار ذلك على نخبة محدودة.

وقد أتاح الفضاء الإلكتروني توفير منافذ جديدة للتعبير عن الآراء بأكبر قدر من الحرية والصراحة في إطار ديمقراطي يستخدم أساليب التصويت الإلكتروني واستطلاعات الرأي السريعة التي تتجاوز حواجز الزمان والمكان لتيسير تبادل الأفكار والحوار بين الثقافات، والتواصل مع أشخاص قد يصعب الالتقاء بهم في الواقع الحقيقي، فلم يعد هناك ضرورة لاستنزاف الوقت والجهد في البحث عن معلومات حول واقعة محددة أو قضية ما، حيث أتاحت وسائط المجتمع الشبكي الحصول على المعلومات بسهولة أكثر وسرعة أكبر، كذلك ساعد المجتمع الشبكي على رواج التجارة الإلكترونية، وتسهيل الخدمات المصرفية والمالية، وخدمات السياحة والسفر، ووسائل الترفيه الإلكترونية من ألعاب ومسابقات، وانتشار التعليم عن بُعد من خلال بعض الجامعات والمراكز العلمية المتخصصة، واستطاعت العديد من الجامعات توظيف تكنولوجيا الاتصال باستخدام المكتبات الرقمية لإتاحة المعلومات للمستفيدين بأسرع الطرق وأقلها كلفة مادية، كما أثر المجتمع الشبكي على البحث العلمي بشكل إيجابي من خلال تكوين المجموعات البحثية بصورة سريعة وأكثر فعالية، وتتكون هذه المجموعات من متخصصين وخبراء في مجال معين على مستوى العالم يتبادلون الأفكار والرؤى للوصول إلى حلول واقعية للمشكلات القائمة، وقد عزز الفضاء الإلكتروني من القدرة على التعلم مدى الحياة باستخدام الوسائط المتعددة التي تمزج بين النص المكتوب والأصوات والصور بكلفة مادية زهيدة مما يجعلها متاحة للجميع. يتطلب كل ذلك إعادة تأهيل مستمرة للكوادر البشرية لتأمين مواكبتها لمستجدات العلوم والتقنية، والقدرة على توظيفها لزيادة الإنتاج القومي، والإفادة من مزاياها الجديدة التي أصبحت تمثل أحد أهم مرتكزات البنية التحتية لأي تطور ينشده المجتمع.



حامد حسن
خبير تكنولوجيا المعلومات

ما التحول الرقمي ؟

اكتشاف الحقيقة وراء هذه الكلمة «الطنانة»



قد يبدو التحول الرقمي وكأنه وسيلة «طنانة» للقول بأنك قمت بترقية مكان عملك، ولكنها أكثر من مجرد كلمة طنانة، إنها عملية مهمة لأخذ أعمالك وعملياتها وقوتها العاملة وتنفيذ التغيير التكنولوجي.

إن الانتقال إلى أنظمة تكنولوجيا المعلومات الجديدة ، أو تنفيذ الخدمات الرقمية ، أو حتى نقل أعباء العمل إلى أبنية الحوسبة السحابية ، ليست عملية بسيطة على الإطلاق. فغالبًا ما تتضمن التحويلات الرقمية إعادة التدريب وإعادة التنظيم وحتى إنشاء وظائف جديدة داخل الشركة. وعلى سبيل المثال، إذا كانت مؤسستك تركز على أن تكون البيانات جزءًا كبيرًا من نموذج الأعمال ، فمن المحتمل أن تكون هناك حاجة إلى مسؤول حماية البيانات.

غالبًا ما يستخدم التحول الرقمي كمصطلح شامل لوصف ترقيات متعددة داخل المؤسسات والهيئات، قد تضيف نظامًا جديدًا ، لكن يمكن أن يكون له تأثير على عدد من الأجزاء المختلفة من عملك، وطريقة عمله قد تتطلب إضافة تقنية واحدة هنا إضافة تكنولوجيا جديدة إلى مكان آخر ، قد تحتاج أجهزة الكمبيوتر الأحدث والأسرع إلى خوادم أكبر، فعلى سبيل المثال.

يقول المركز العالمي لتحويل الأعمال الرقمية: إن «التغيير التنظيمي هو أساس تحول الأعمال الرقمية»؛ ذلك لأن تغيير طبيعة المنظمة يعني تغيير طريقة عمل فريق العمل وتحدي عقلياتهم وإجراءات العمل والاستراتيجيات اليومية التي يعتمدون عليها، في حين أن هذه تمثل أصعب المشكلات ، إلا أنها تحقق أيضًا المكافآت الأكثر قيمة ، مما يتيح لهيئة ما أن تصبح أكثر فاعلية وقائمة على البيانات، وتنجز أعمالها أسرع مما سبق ، مع الاستفادة من توفير المزيد من فرص العمل.

في حين أن خفض التكاليف وتحسين عمليات المنظمة باستخدام أحدث التقنيات الرقمية أمر جذاب بما يكفي من تلقاء نفسه ، فإن تبني مبدأ التحول الرقمي يمكن أن يجعل المؤسسات أيضًا أكثر أمانًا وقوة في مواجهة انقطاع تكنولوجيا المعلومات.

قد يقوم العديد من مسؤولي تقنية المعلومات ومديري تقنية المعلومات بتمديد فضائل امتلاك تطبيق أو خادم قاعدة بيانات محلي، حيث يكون الوصول المباشر متغيراً إذا حدث خطأ ما، وأنه من خلال إبقاء هذه البنية التحتية بالقرب من قسم تكنولوجيا المعلومات ، يمكنه ضمان أمانها.

قد يكون هذا صحيحًا منذ عقد من الزمان ، ولكن نمو الخدمات السحابية والمنصات والبنية التحتية قد شهد تحسينات هائلة في كيف يمكن أن تكون التطبيقات والخدمات المستضافة السحابية الموثوق بها والخدمات السحابية الأصلية موثوقة.

يستثمر كبار مزودي الخدمات السحابية مثل Amazon Web Services و Microsoft Azure و Google Cloud Platform الملايين بملايين الدولارات في بناء البنية التحتية السحابية الخاصة بهم ، من توسيع القدرات إلى تعزيز التكرار والأمن، في هذه الأيام ، يمكن لموفري الخدمات السحابية تقديم خدمات وأمن أفضل من جميع المراكز باستثناء مراكز البيانات الخاصة وغرف الخادم الأكثر قوة، ويمكنهم تقديم هذه الخدمات السحابية بأسعار تنافسية للغاية.

على هذا النحو ، فإنه يجعل متابعة التحول الرقمي ، خاصةً من منظور «الانتقال إلى السحابة» عملية أسهل وأكثر جاذبية أكثر مما كانت عليه من قبل.

التحول الرقمي هو مصطلح «أنيق» في شرح مبدأ تحديث البنية التحتية القديمة لتكنولوجيا المعلومات ، ولكنه يتجاوز مجرد تبني التكنولوجيا ؛ إنه– كذلك– تحول في ثقافة الهيئات والمؤسسات.

يتضمن الجزء الرقمي من التحول الرقمي الانتقال من الأنظمة والبنية التحتية الحالية إلى الأنظمة الأساسية والبرامج الحديثة المقدمة كخدمات عبر السحابة بدلاً من تطبيقات سطح المكتب التقليدية.

يتطلب القيام بذلك توفير الأدوات والمهارات المناسبة لإطلاق العنان للمعلومات المحتملة فيما يبدو أنه بيانات متباينة، لكن من المرجح أن يتبنى الأشخاص المستثمرون في رحلة التحول الرقمي للهيئات أدوات رقمية من شأنها أن تجعل حياتهم أسهل وتمنحهم ميزة تنافسية.

يتضح من خلال المقال أهمية النطاقات والأهداف في استراتيجية التحول الرقمي، مع مراعاة الاعتبار الأخير، إنها التكنولوجيا التي تمكن من تحقيق العمليات، ولكن الطريقة التي يتم تنفيذها بها سيكون لها أثر كبير على النجاح.

باختصار، إن إمكانات التحول الرقمي واسعة ومتنوعة، مع مشروعات تتراوح من تحديث الأنظمة إلى تطوير العمليات الأساسية للهيئات والمؤسسات.

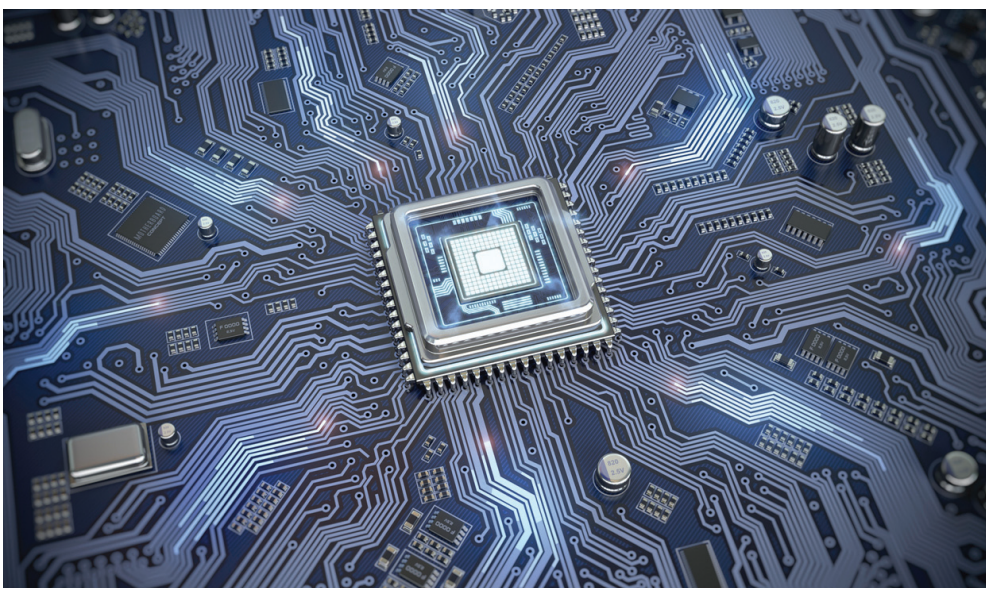


م / إسلام غانم
استشاري تكنولوجيا المعلومات

عصر التفوق الكمي

يسيطر الآن داخل المجتمعات التكنولوجية والشركات العالمية والدول و الحكومات الغربية ما يطلق عليه «التفوق الكمي» والذى قدمته شركة «جوجل» بالتعاون مع وكالة ناسا الأمريكية ، ولهذا المصطلح قفزة في عالم الحوسبة الكمية التي ترتكز المنافسة فيها بين شركة جوجل و IBM ، ولكن دعونا نعرف أولا ما تكنولوجيا التفوق الكمي ؟

التفوق الكمي عبارة عن صنع حاسب أو حواسب قدراتها أعلى بكثير من قدرات الحواسب العادية،بحسب ما أفادت صحيفة فاينانشال تايمز.



وهذه الحواسب نوع جديد قادرة على إجراء بعض المهام أسرع بكثير من الآلات العادية، إذ إنها تستخدم مواصفات في الجزئيات تسمح لها بالالتفاف على قواعد الفيزياء الأساسية.

دعنا نعطى بعض الأمثلة على تلك السرعات لهذه التقنية، حيث يؤكد الباحثون في شركة جوجل في دراستهم والتي أسموها حاسوب « سيكامور الكمي» أن معالجهم قادر على إجراء عملية في خلال ثلاث دقائق وعشرين ثانية بدلا من ١٠ آلاف سنة، وذلك في ظِلّ توافر ظروف معينة ، وهي المدّة التي يستغرقها في هذه المهمة الحاسوب الحالي الأكثر تقدما على مستوى الحواسب الحالية المتقدمة والضخمة.

هذا وقد أوضح الباحثون أن الحواسب التقليدية و الحواسب المحمولة وكذا الحواسب الضخمة تستخدم نظاماً ثنائياً من رقمين ا و٠، أما الحواسب الكمية فتستخدم «بتات» كمية تسمى «كيوبيتس» كي تجري عملياتها الحسابية.

ولذا بدلًا من الاقتصار على احتمالين فحسب في البت الواحدة، فإن البت الكمية قد تكون ا و٠ في الوقت ذاته، ويعني ذلك أن قوة الحوسبة تزداد بعلاقة طردية كلما زاد عدد «البتات الكمية».

ويتضمن حاسوب سيكامور الكمي ٥٢ بت كمية، ولذا يحسب ١٠ ملايين مليار احتمال في المرة الواحدة، وفقًا لمقطع فيديو قصير نشرته جوجل.

للعلم ، مجال الحوسبة الكمية هو حقل فرعي لعلوم المعلومات الكمية ، والذي يتضمن تشفير الكم والاتصال الكمي، عندما أقرأ في هذا الموضوع يدور في ذهني أسئلة كثيرة، منها: مَن المستخدم النهائي لهذه التقنية ؟ وما أشكال تطبيقاتها؟ وهل لها علاقة بالبحث العميق أو ما يسمى Deep Web ؟ وهل أجهزة عقل الدولة التي أشار إليها الرئيس قائمة عليها أم لا ؟ أسئلة كثيرة تراود الفكر، ومن المؤكد أنها ستكون إضافة حقيقية إلى قطاع Machine leaning بسبب تلك السرعة الرهيبة التي تمتاز بها، وهل من الممكن أن تساعد تلك التقنية في إصدار عملة إلكترونية رقمية مصـرية مثل البيتكوين (Bitcoin) ؟ هذا وسيساعدنا إثبات تفوق الحواسب الكمية على حل مشكلات معقدة بصورة أسرع.

وتستطيع شركات المستحضرات الدوائية استخدام التقنية في إنتاج مركبات معقدة للاستخدامات الطبية، وقد تستخدم النماذج المالية الحوسبة الكمية لمعرفة اتجاهات السوق.

ويبقى السؤال هنا: ما القطاعات المستهدفة بهذه التقنية ؟ على مستوى المستخدم النهائي سيوجد الكثير مثل المعاملات الحكومية، والأكاديمية، والجيش ، والجيولوجيا / الطاقة، وتكنولوجيا المعلومات ، والنقل والخدمات اللوجستية، المالية / الاقتصادية، وعلم الأرصاد الجوية، كل تلك القطاعات تعتمد بشكل كلى على تدفق رهيب من البيانات يحتاج إلى معالج قوى؛ حتى يستطيع أن يعالجها دون توقف أو أعطال، فمن الممكن أن نستخلص أن تقنية الحوسبة الكمية ستساعد في حل مشاكل ما يطلق عليهBig DataI ، أما إذا ذكرنا على سبيل التطبيقات فتوجد تطبيقات البحث الأساسي، ومحاكاة الكم ومشاكل التحسين، و أخذ العينات، أو أي نوع من التطبيقات التي تحتاج إلى معالجة برمجية كبيرة، أخيرا يتبقى سؤال متعلق بالتقنية الجديدة وأثرها على الأمن السيبراني. ويحذر العلماء من أن الحواسب الكمية قد تنجح نظريًا في اختراق معايير التشفير الحالية بسبب تمتعها بقدرات حوسبة هائلة، لكن ذلك ما زال مجرد توقعات، فالباحثون لم يحددوا بعد الظروف المتوفرة لتلك الحواسب القوية.



م/ محمد مصباح محمد
باحث واستشاري أمن المعلومات

تأمين البنية التحتية للدول
(المخاطر والتحديات)

تخيل لو أنك استيقظت يوما فوجدت أن مَن يتحكم في شبكة الكهرباء في دولتك هي دولة معادية، ماذا سيحدث؟

ستتوقف المواصلات، الإعلام، الاتصالات، حركة الطيران المدني والعسكري، والدفاع الجوي، .....إلخ، سوف تكون هذه الدولة في حالة ما قبل اختراع الكهرباء.

تخيل لو سيطرت دولة معادية على أنظمة الدفاع الجوي لدولة أخرى، ماذا سيحدث؟

سيكون مجالها الجوي مباحاً بلا رادع ، ويكون مواطنوها ومبانيها المهمة تحت رحمة طيران العدو..

الدول بصفة عامة تُقسم البنية التحتية الخاصة بها إلى نوعين (بنيه تحتية عادية، وبنية تحتية حرجة) وفي هذا العصر الحديث الذي يُطلق عليه عصر ثورة المعلومات أصبحت المعلومات عنصرا أساسيا في كل شيء في حياتنا اليومية.

فلو تخيلنا شكل الحروب منذ ٣٠ عاماً كيف كانت، فقد كانت الحروب عبارة عن سلاح مقابل سلاح، طائرة مقابل طائرة، دبابة مقابل دبابة، أما اليوم فقد تغير شكل الحروب كثيراً، ومن أهمها ـ وفي مقدمتها ـ حرب أمن المعلومات أو ما يطلق عليه (الحرب السيبرانية) وبالتحديد أمن المعلومات الخاص بالبنية التحتية الحرجة وأنظمة التحكم الصناعي.

في معظم الدول هناك فريق يتبع الحكومة يقوم بالتصدي والتعامل مع الهجمات الإلكترونية يُسمي هذا الفريق (Computer Emergency Readiness Team "CERT")، ولكن المفارقة هنا أن بعض هذه الدول يوجد لديها فريقان للتعامل مع طوارئ الهجمات الإلكترونية، أحدهما يتبع وزارة الدفاع، والثاني يتبع وزارة الأمن الداخلي وهو الفريق الخاص بأنظمة التحكم الصناعي، مثل ما يوجد في الولايات المتحدة الأمريكية، حيث يتبع فريق ICS–CERT وزارة الأمن الداخلي التي تشكلت بعد أحداث ١١ سبتمبر ٢٠٠١ مباشرة، وإن دل هذا على شيء فإنما يدل على أهمية وخطورة أنظمة التحكم الصناعي.

- ما أنظمة التحكم الصناعي؟

نظام التحكم الصناعي (Industrial control systems) هو نظام مبنى على أسس نظريات التحكم الكلاسيكية والحديثة ، ويستخدم مختلف الأنواع والأجهزة اللازمة لتشغيل منظومة صناعية متكاملة أو جزئية.

تُستخدم أنظمة التحكم الصناعي في معظم الصناعات الثقيلة والمهمة. مثل (المفاعلات النووية، المطارات المدنية والعسكرية، أنظمة الدفاع الجوي، شبكات الكهرباء، شبكات المياه،

أنظمة النقل والمواصلات، محطات استخراج البترول والغاز، ..... إلخ) هذه بعض الأمثلة لما يُستخدم فيها أنظمة التحكم الصناعي.

- العالم والهجمات الإلكترونية على أنظمة التحكم الصناعي:

انتبه العالم إلى أهمية أمن المعلومات في أنظمة التحكم الصناعي بداية من عام ٢٠١٠ حيث كانت بداية الهجمات المؤثرة حينما هوجم أحد المفاعلات النووية بفيروس أطلق عليه «Stuxnet» , حيث عُطّل عمل المفاعل نهائيا، وكان معقداً عشرين مرة أكثر من أي فيروس آخر، ويعد هذا أول سلاح من البرمجيات.

منذ ذلك الحين وحتى يومنا هذا وضعت الدول أنظمة التحكم الصناعي في قمة أولويات الأنظمة المطلوب حمايتها.

تكررت الهجمات الإلكترونية على أنظمة التحكم الصناعي، وكان من أشهرها الهجمات التي تمت على شبكات الكهرباء الأوكرانية.

- الدول العربية والهجمات الإلكترونية على أنظمة التحكم الصناعي:

طبقا لشركه كاسبرسكي تعد الدول العربية من أكبر الأهداف للهجمات الإلكترونية في أنظمة التحكم الصناعي لأسباب كثيرة، منها ضعف حماية البنية التحتية في بعض الدول, ومنها– أيضا ـ أنه يوجد بها عدد كبير من مستخدمي أنظمة التحكم الصناعي على مستوى العالم مثل شركات البترول والغاز, على سبيل المثال لا الحصر شركة آرامكو للبترول.

- علاقة الهجمات على أنظمة التحكم الصناعي والمواقف السياسية بين الدول:

المواقف السياسية بين الدول والهجمات الإلكترونية وجهان لعملة واحدة، من هنا نأتي إلى أنه من يقوم بالهجمات على البنية التحتية لدولة ما، هى هجمات منظمة ترعاها أجهزة مخابرات دولة أخرى لها مواقف معادية تستهدف إحداث ضرر في البنية التحتية لهذه الدولة.

كان هناك خلاف بين أمريكا وإسرائيل من جهة وإيران من جهة أخرى على البرنامج النووي الإيراني فخرج فيروس Stuxnet، وكان هناك خلاف بين روسيا وأوكرانيا فأعادت روسيا إنتاج فيروس Black Energy هاجمت به شبكات الكهرباء.

نتيجة لكل ذلك أصبحت في كل الجيوش وحدات خاصة بحرب المعلومات والهجوم على الخصم، فهي حرب لا خسارة فيها لأرواح البشر، ولكن لها آثار عظيمة تفوق الاجتياح البري لحدود دولة أخرى.

كل هذا وأضعافه من الممكن أن يحدث من الهجمات الإلكترونية على أنظمة التحكم الصناعي.

الهجمات الإلكترونية على أنظمة التحكم الصناعي لها تأثير على الأمن القومي والاقتصاد.



محمد منير غازي
باحث معلوماتي في مجال
المناهج وطرق التدريس

كيف نُعد أبناءنا لمواجهة سيطرة الروبوتات على وظائف المستقبل؟



يتخوف الكثيرون من النمو التكنولوجي المتسارع ومخاطر سيطرة الروبوتات على سوق العمل، ويسمع الكثيرون عن أحاديث وتوقعات في سيطرة الروبوتات على أغلب الأعمال البشرية في المستقبل، فكيف لأبنائنا العمل في المستقبل وكسب العيش؟!!

وفقاً لتقرير المنتدى الاقتصادي العالمي الصادر في مايو عام ٢٠١٧ بعنوان «مستقبل الوظائف ومهارات في الشرق الأوسط وشمال إفريقيا» فإن التعليم والعمل في منطقة الشرق الأوسط وشمال إفريقيا سيحدد سبل عيش أكثر من ٣٠٠ مليون شخص وطرق دفع عجلة النمو والتنمية للأجيال القادمة، حيث تشير التقديرات المبدئية للتقرير إلى أن ٤٩٪ من جميع أنشطة العمل في مصر عرضة لتتحول إلى التشغيل الآلي، وكذلك من المتوقع أن تتحول الكويت بنسبة ٤١٪، وبنسبة ٤٦ ٪ في كل من البحرين والمملكة العربية السعودية، وبنسبة ٤٧٪ في الإمارات، وبنسبة ٥٠ ٪ في المغرب.

ويشير أحد تقارير شركة الهندسة الإنجليزية العملاقة mace إلى أنه من المتوقع بحلول عام ٢٠٤٠ أن يخسر السوق البريطاني للإنشاءات ما يقدر بحوالي ٦٠٠ ألف وظيفة بشرية من إجمالي ٢.٢ مليون وظيفة للأبد بسبب الروبوتات، كما أكدت العديد من التقارير الدولية أن التطور التكنولوجي سينهي بعض الوظائف، ولكنه في المقابل ابتكر المزيد من الوظائف التي لم تكن موجودة من قبل، وهو غالباً ما سيحدث في المستقبل، لذا لا تخف على مستقبل أبنائك، فمن المتوقع ظهور

أكثر من ١٥٧ وظيفة جديدة لأبنائنا بحلول عام ٢٠٤٠ وفق تقرير «مؤسسة دبى لاستشراف المستقبل».

صحيح أن الروبوتات ستقوم بأعمال البشر في المستقبل إلا أنها غالباً لن تتمكن من التفكير الإبداعي والتطوير، لذلك فإنه من المتوقع أن تحتاج روبوتات القيادة الآلية إلى وظائف بشرية تعمل على برمجتها ومراقبة تشغيلها إلى جانب مطورين لمهارات التواصل لديها وربما جراحين، كما تحتاج الطائرات بدون طيار «الدرونز» إلى مبرمجين وموظفين في مراكز القيادة ومصممين ومطورين ووكلاء مبيعات.

من المتوقع أن تزيد الحاجة لوظائف ومهن الفضاء التي تمتد ما بين المراقبين والمستكشفين والمساحين وربما مهندسي تعدين للكواكب، أما السيارات ذاتية القيادة فإنها تحتاج إلى مهندسين متخصصين في إنشاء وتطوير الطرق الذكية ومحللين ومطورين، ولا ننسى الوظائف المرتبطة بالذكاء الاصطناعي المعزز للبشر.

والجدير بالذكر، أنه في عام ٢٠١٥ أنتج العالم «بيانات ضخمة» Big Data بما يساوي ٧.٩ زيتا بايت، حيث تمثل وحدة الـ ١ زيتا بايت (١٠٠٠.٠٠٠.٠٠٠.٠٠٠.٠٠٠.٠٠٠ بايت) وهو الذى يتم تخزينه على ٢٥٠ مليار قرص DVD، ومن المتوقع أن يصل حجم الإنتاج العالمي من البيانات إلى ٤٤ زيتا بايت بحلول عام ٢٠٢٠، أما فيما يتعلق بمستقبل وظائف البيانات الضخمة Big Data فمن المتوقع وجود طلب هائل على وظائف مثل علماء البيانات، والمحققين في مجال البيانات، ومستخرجي ومحللي ومراقبي ووسطاء البيانات وغيرها من التخصصات من البيانات الضخمة والمفتوحة.

لا تستغرب لمثل تلك الوظائف أو حتى للأكثر منها غرابة، فإنه وفقاً لتقرير الخبير العالمي «توماس فري» بعنوان استشراف المستقبل، فإن هذه الوظائف مخصصة لجيل يطلق عليه علمياً «الجيل ألفا» «Generation Alpha»، وهم الأطفال المولودون بعد عام ٢٠١٠م، فيما تعتبر الأجيال السابقة له خارج حسابات وظائف المستقبل وهما «الجيل الميلينيا» Millennia Generation من مواليد الفترة من (١٩٨١ إلى ١٩٩٩)، « والجيل إكس» Generation X من مواليد الفترة من (١٩٦٥ إلى ١٩٨٠).

لـذا علينا أن نمتلك الجرأة لمواكبة التغيرات الإجبارية المتسارعة في التعليم وسوق العمل للحاضر والمستقبل، وعلينا أن نتجنب اعتمادنا على مبدأ «ما تعرفه أفضل مما لا تعرفه»، فعالمنا متغير ويجب على أساليب التربية أن تواكب هذا التغيُّر.

من المهم التوقف عن توجيه أصابع الاتهام للتكنولوجيا ووصمها بأنها سبب بطالة أبنائنا أو حتى أحفادنا، وأن نعمل على إعداد أبنائنا لما يتناسب مع متطلبات وظائف المستقبل، خاصةً في ظل توجه الدولة نحو التوسع في الكليات والمعاهد الفنية والتكنولوجية المتقدمة.



موضوع العدد

الأمن السيبراني
Cyber security



أعد الملف : م. إيمان محمود

ما الأمن السيبرانى؟

الأمن السيبراني هو ممارسة الدفاع عن أجهزة الكمبيوتر، والخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات من الهجمات الخبيثة، كما يُعرف أيضًا باسم أمان تكنولوجيا المعلومات، أو أمن المعلومات الإلكترونية.

علام ينطبق مصطلح الأمن السيبراني؟

- ينطبق هذا المصطلح على مجموعة متنوعة من السياقات، بدءًا من قطاع الأعمال، وصولًا إلى الحوسبة المتنقلة، وبالإمكان عمومًا تقسيمها إلى عدّة فئات شائعة كما يلي:

- **أمن الشبكات** (Network security)

هو ممارسة تأمين شبكة الكمبيوتر من العناصر المتطفلة والانتهازية، سواء المهاجمين المستهدفين، أو البرامج الضارة.

- **أمان التطبيقات** (Application security)

يركز على الحفاظ على البرامج والأجهزة خالية من التهديدات، إذ يمكن أن يوفر التطبيق المخترق الوصول إلى البيانات المصممة للحماية، وإنّ تطبيق مفهوم الأمان الناجح يبدأ في مرحلة التصميم الأوّلي قبل نشر البرنامج أو الجهاز.

- **أمن المعلومات** (Information security)

يحمي سلامة وخصوصية البيانات، سواء في مرحلة التخزين أو التناقل.

- **الأمن التشغيلي** (Operational security)

يشمل العمليات والقرارات التي تتعامل مع أصول البيانات، وتكفل حمايتها.

- **الاسترداد بعد الكوارث واستمرارية الأعمال**
(Business continuity planning (BCP)/disaster recovery planning (DRP))

يحدد كيفية استجابة المؤسسة لحادث أمان إلكتروني، أو أي حدث آخر يتسبب في فقدان البيانات، وهذا ينطوي على آلية عمل المؤسسة في استعادة بياناتها وعملياتها للعودة إلى نفس القدرة التشغيلية التي كانت عليها قبل الحادث، وإنّ استمرارية العمل هي الخطة التي تعتمد عليها المنظمة بينما تحاول العمل بدون موارد معينة.

- **تعليم أو تثقيف المستخدم النهائي** (End-user education)

أي التعامل مع عامل الأمن الإلكتروني الذي لا يمكن التنبؤ به؛ وهو الأشخاص؛ إذ يمكن لأي شخص عن طريق الخطأ إدخال فيروس إلى نظام ما آمن.



إنّ توجيه المستخدمين لحذف مرفقات البريد الإلكتروني المشبوهة، وعدم توصيلUSB غير معروفة، والعديد من الدروس المهمة الأخرى هو أمر حيوي لأمن أي منظمة.

أنواع التهديدات السيبرانية

هناك أنواع عديدة من التهديدات السيبرانية التي يمكنها مهاجمة الأجهزة والشبكات، ولكنها تقع عمومًا في ثلاث فئات، وهي : الهجمات على السرية، النزاهة، والتوافر.



- **الهجمات على السرية (Confidentiality)**

تشمل سرقة معلومات التعريف الشخصية، والحسابات المصرفية، أو معلومات بطاقة الائتمان، حيث يقوم العديد من المهاجمين بسرقة المعلومات، ومن ثم بيعها على شبكة الإنترنت المظلمة (Dark Web) لكي يشتريها الآخرون، ويستخدموها بشكل غير شرعي.

- **الهجمات على النزاهة (Integrity)**

تتكون هذه الهجمات من التخريب الشخصي أو المؤسساتي، وغالبًا ما تسمى بالتسريبات؛ إذ يقوم المجرم الإلكتروني بالوصول إلى المعلومات الحساسة، ثم نشرها، بغرض كشف البيانات، والتأثير على الجمهور لإفقاد الثقة في تلك المؤسسة أو الشخصيّة.

- **الهجمات على التوافر (Availability)**

الهدف منها هو منع المستخدمين من الوصول إلى بياناتهم الخاصة إلى أن يدفعوا رسومًا ماليّة، أو فدية معيّنة.

كيفية تحقيق الأمن السيبراني

قد تساعدك الخطوات الأمنية البسيطة في الحفاظ على مستوى جيّد من الأمان والسلامة السيبرانية:

1.الموثوقيّة

استخدم فقط المواقع الموثوق فيها عند تقديم معلوماتك الشخصية، والقاعدة الأساسية الفضلى هنا هي التحقق من عنوان URLإذا كان الموقع يتضمن https في بدايته، فهذا يعني أنه موقع آمن، أمّا إذا كان عنوان URL يحتوي على http بدون s؛ فتجنّب إدخال أيّ معلومات حساسة مثل بيانات بطاقة الائتمان، أو رقم التأمين الاجتماعي.

2.البريد الاحتيالي

لا تفتح مرفقات البريد الإلكتروني أو تنقر فوق روابط الرسائل من المصادر غير المعروفة؛ إذ إنّ إحدى الطرق الأكثر شيوعًا التي يتعرض فيها الأشخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها مرسلة من شخص تثق فيه.

3.التحديثات (Always up-to-date)

احرص دائمًا على تحديث أجهزتك، فغالبًا ما تحتوي تحديثات البرامج على معالجات مهمة لإصلاح مشكلات الأمان، وإنّ هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان.

4.النسخ الاحتياطي

قم بعمل نسخ احتياطية من ملفاتك بانتظام لمنع هجمات الأمان على الإنترنت، وإذا كنت في حاجة إلى تنظيف جهازك (Format) بسبب هجوم إلكتروني سابق، فسيساعدك ذلك على تخزين ملفاتك في مكان آمن ومستقل.

إن مفهوم الأمن السيبراني وعملياته المرتبطة يتطوران باستمرار، مما يجعل من الصعب حقًا مواكبة كلّ التفاصيل، وعمومًا، فإن البقاء على اطلاع، والتحلّي بالحذر على الإنترنت هما خير وسيلة للمساعدة في حماية نفسك وعملك.



مصطلحات تكنولوجية

1 الأمن السيبراني

الأمـن السيبراني هو ممارسة الدفاع عن أجهزة الكمبيوتر، والخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات من الهجمات الخبيثة، كما يُعرف أيضًا باسم أمان تكنولوجيا المعلومات، أو أمن المعلومات الإلكترونية.

2 أمن المعلومات

أمن المعلومات (يشار إليه غالبًا بـ InfoSec) وهوعبارةٌ عن مجموعة من استراتيجيات إدارة العمليات، والأدوات، والسياسات الضرورية لمنع وكشف وتوثيق ومواجهة التهديدات على المعلومات الرقمية وغير الرقمية، وهذا يشمل حماية المعلومات من التعديل، والتعطيل، والتدمير، والتفتيش.

3 الفضاء السيبراني

عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه: «فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية»، فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين، كما أن هناك مَن عرّف الفضاء السيبراني بأنه الذراع الرابعة للجيوش الحديثة.

4 الردع السيبراني

يُعرف الردع السيبراني بأنه «منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية»، ويرتكز الردع السيبراني على ثلاث ركائز، هي عماد استراتيجية الدفاع السيبراني، تتمثل في: مصداقية الدفاع Credible Defense، والقدرة على الانتقام An Ability to Retaliate، والرغبة في الانتقام A Will to Retaliate.



5 الهجمات السيبرانية

يمكن تعريفها بكونها: «فعلاً يقوّض من قـدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام».

6 الجريمة السيبرانية

مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها. فهي الجريمة المتصلة باستخدام الكمبيوتر، أي تصرف غير قانوني، يرتكب باستخدام تقنيات المعلومات والاتصالات.

7 القوة السيبرانية

يعد جوزيف.س ناي Nye.S Joseph من أبرز المهتمين بالقوة السيبرانية، حيث يعرّفها بأنها «القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية».

العقد الاجتماعي للأمن السيبراني:
تطبيق نموذج قائم على السوق

The Cybersecurity Social Contract:
Implementing a Market-Based Model for Cybersecurity



عرض الكتاب:
م. محمد السيد



عن الكتاب:

إذا كان لديك ٣٠ دقيقة لتقديم المشورة بشأن الأمن السيبراني، فماذا ستقول؟

هذا هو السؤال الذي طرحناه على ISA قبل عام والجواب جاء في ٤٠٠ صفحة و١٧ فصلاً في هذا الكتاب الذى يحتوي على ١٠٦ توصيات محددة.

كُتب هذا الكتاب في المقام الأول من قبل مجلس(Internet Security Alliance) ISA الذي يتألف من كبار ضباط أمن المعلومات من ٢٠شركة من كبريات الشركات في العالم التي تغطي ١١ قطاعًا اقتصاديًا.

وتبدأ الإجابة ببرنامج مكون من ١٢ خطوة للإدارة الجديدة يتراوح بين تحديد النغمة المناسبة لمعالجة المشكلة، إلى المبادرات الاستراتيجية، وصولاً إلى التوصيات التشغيلية الملموسة.



ملخص:

تم تعميم مفهوم العقد الاجتماعي في القرنين الثامن عشر والتاسع عشر من خلال كتابات جان جاك روسو، جون لوك ، توماس هوبز ، وغيرهم، حيث ركزت في البداية على العلاقة بين الفرد والدولة وما يتبادله كل منهما مع الآخر من أجل تحقيق نظام اجتماعي أوسع والاستفادة للمجتمع، وفي أوائل القرن العشرين تم تكييف العقد الاجتماعي للتبادل بين الشركات والدولة من أجل تحقيق منفعة متبادلة أكبر للنظام الاجتماعي.

في ذلك الوقت كانت التقنيات الحديثة هي الاتصالات (الهواتف) وتوزيع الكهرباء أكثر للشريحة الاجتماعية مرتفعة الدخل، ولم يدرك واضعو السياسات في تلك الحقبة أن الخدمة الشاملة لهذه التقنيات ستحقق فائدة اجتماعية واسعة ولكنهم أدركوا أيضًا أنه لا يمكن للحكومة تحقيق ذلك بمفردها، علاوة على ذلك فإن إجبار القطاع الخاص على تقديم الخدمات دون تعويض مناسب سيكون نموذجًا غير مستدام؛ لذلك تم تطوير عقد اجتماعي بين الدولة والقطاع الخاص أدى إلى موافقة الشركات الخاصة على تقديم خدمة شاملة بأسعار منظمة، في المقابل وافقت الحكومة على ضمان معدل عائد كبير على استثماراتهم.

الدول التي أخذت بمبدأ العقد الاجتماعي بين الدولة والقطاع الخاص حققت تقدمات هائلة، حيث تم نشر البنية التحتية الكهربائية والاتصالات السلكية واللاسلكية بوتيرة متسارعة مقارنة بالدول الأخرى التي اختارت نموذجاً مركزياً للحكومة، علاوة على ذلك فإن البنية التحتية التي تدعمها بشكل كاف الحوافز الاقتصادية المتضمنة في العقد أصبحت باستمرار أكثر تطوراً وابتكاراً، كما وفر التطور السريع لهذه البنى التحتية الأساس للتصنيع المتسارع وخلق فرص العمل والابتكار.

يعتقد ISA أن هناك حالة مماثلة اليوم فيما يتعلق بالأمن السيبراني، فعلى سبيل المثال، على الرغم من وجود تمويل في كل من القطاعين العام والخاص يقوم بتمويل وظيفي وتطبيق دفاعات إلكترونية قوية بسبب الترابط بين النظم إلا أنه لا يمكن للشركات ولا الحكومة التي تعمل من تلقاء نفسها تأمين أنفسهم بشكل كاف؛ حيث يحتاج النظام دائما إلى التطوير ليس فقط تطوير معايير وممارسات بل يحتاج أيضًا إلى دعم اقتصادي لتطبيقه والابتكار السريع والتكيف في مواجهة التهديد السيبراني المتطور باستمرار.

لذا تم إيجاد معايير وممارسات يمكن ـ إذا تم نشرها عالميًا ـ أن تحسن بشكل كبير الأمن السيبراني، على أن تدعو ISA إلى تحديد هذه المعايير والممارسات في شراكة بين القطاعين العام والخاص.

نشر ISA إدراكه الكامل لما هو «العقد الاجتماعي للأمن السيبراني» في كتاب يزيد عدد صفحاته على ٤٠٠ صفحة بمشاركة ٢٥ مؤلفًا مختلفًا يحتوي على ١٠٦ توصيات حيث يغطي الكتاب مجموعة من القضايا الشاملة، مثل تثقيف مجالس إدارة الشركات والإصلاحات اللازمة لعملية تدقيق الأمن السيبراني، وكيف يمكن استخدام التأمين على أفضل وجه لنقل المخاطر ، وكيف يمكن إعادة هيكلة الحكومة للعصر الرقمي وحل التوترات بين الخصوصية والأمن وتحسين الشراكات بين القطاعين العام والخاص.

ويعد الكتاب محاولة لتوفير إطار متماسك ومنهجي للعمل التعاوني الذى يجب فيه دمج التكنولوجيا المتقدمة مع الاقتصاد العملي والسياسة العامة المدروسة لإنشاء نظام مستدام للأمن السيبراني.

Internet Security Alliance (https://isalliance.org/about-isa/)

تم تأسيس Internet Security Alliance في عام ٢٠٠١ كتعاون غير هادف للربح بين تحالف الصناعات الإلكترونية، واتحاد رابطات التجارة، و CyLab بجامعة كارنيجي ميلون، مع التركيز على الأمن السيبراني. يعد ISA منتدى لمشاركة المعلومات والقيادة في مجال أمن المعلومات، كما أنه يمثل ضغطًا من أجل المصالح الأمنية للشركات.




مجلس الوزراء
مركز المعلومات ودعم اتخاذ القرار
مصدرك الآمن
للمعلومات
www.idsc.gov.eg
www.idsc.gov.eg


مجلس الوزراء
مركز المعلومات ودعم اتخاذ القرار
CICPO
مؤتمر القاهرة الدولي الثالث
لاستطلاعات الرأي العام
١٦-١٧ يونيو
"استطلاعات الرأي .. لمستقبل أفضل"
www.pollcenter.idsc.gov.eg

مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء

١ شارع مجلس الشعب - قصر العيني - القاهرة - مصر

رقم بريدي: ١١٥٨٢ ص.ب: ١٩١ مجلس الشعب تليفون: ٢٧٩٢٩٢٩٢(٢٠٢) فاكس: ٢٧٩٢٩٢٢٢(٢٠٢)

www.idsc.gov.eg info@idsc.net.eg

www.idsc.gov.eg