مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

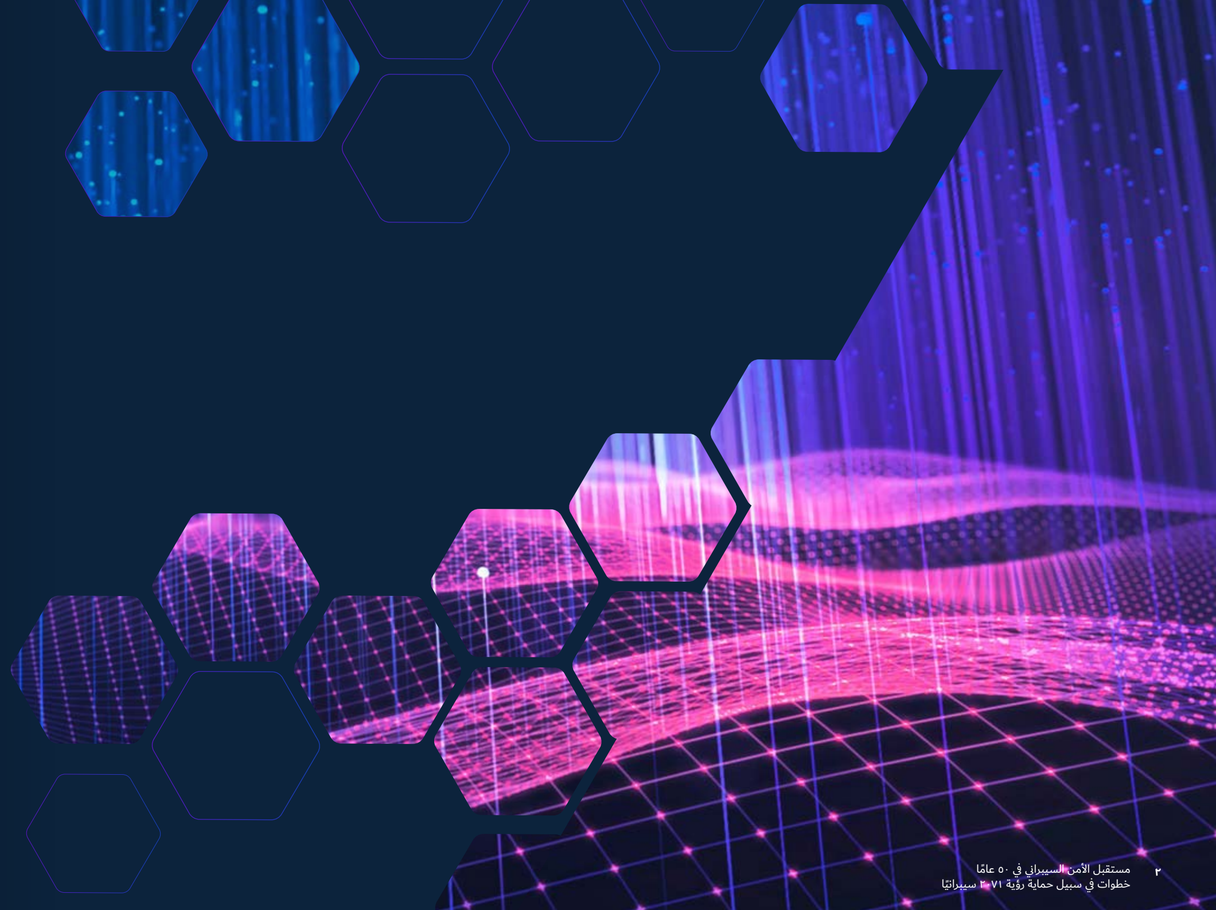
KPMG

مستقبل الأمن السيبراني في ٥٠ عامًا

خطوات لضمان الحماية السيبرانية لرؤية ٢٠٧١

اكتوبر ٢٠٢٣

كي بي إم جي لوار جلف (منطقة جنوب الخليج)



"نحن لا نعيش لليوم أو الغد فحسب، بل نعيش لتأمين مستقبل أحفادنا، وليس أبناءنا فقط."

الشيخ محمد بن زايد آل نهيان
رئيس دولة الإمارات العربية المتحدة

"إن العزم والاستراتيجية والرؤية للمستقبل هم مواردنا الحقيقية في مسعانا للتميز والنجاح."

الشيخ محمد بن راشد آل مكتوم
رئيس مجلس وزراء دولة الإمارات العربية المتحدة

المحتويات

ملخص تنفيذي

أبرمت كي بي إم جي تعاونًا مع مجلس الأمن السيبراني الإماراتي بغرض التعرف على مستقبل الأمن السيبراني خلال ٥٠ عامًا. وينصب تركيز البحث الذي أجريناه في هذا الأمر حول عدد هائل من القضايا التي ظهرت من جراء تبني تقنية المعلومات، وكذلك يسلط البحث الضوء على الاتجاهات في الوقت الراهن والتي نتوقع تأثيرها على مجمل حياتنا في العقود القادمة. ومن كبرى تلك الاتجاهات التركيبة السكانية وتغير المناخ والتحديات الصحية واستهلاك الطاقة.

يُتوقع أن يصل التعداد السكاني للعالم إلى ٩٫٧ مليار نسمة في عام ٢٠٥٠، الأمر الذي يحمل في طياته مخاطر مجتمعية وخيمة لمناطق مختلفة، ويؤثر تغير المناخ الذي تسببه انبعاثات الغازات الدفيئة كذلك على الأمن الغذائي ويُسهم في نزوح السكان وتدهور النظم البيئية. كذلك، تزيد التحديات الصحية من أمثلة مقاومة مضادات الميكروبات وتوقعات العمر الأطول من مخاطر الأوبئة، فضلًا عن كونها تضيف أعباء إضافية على أنظمة الرعاية الصحية. وفي ظل توقع ارتفاع استهلاك الطاقة العالمي ليبلغ ٥٠٪ في ٢٠٥٠، تُعد مصادر الطاقة المتجددة وكفاءة الطاقة ذات أهمية تزيد بزيادة التكاليف والضغوط المناخية.

غير أنّه وبالرغم من وجود تلك المخاطر، إلا أن ثمة بعض الحلول التكنولوجية والعلمية التي تروي بذور الأمل في مستقبل أفضل. وبالرغم من ذلك، فإن التقدم التكنولوجي في معظم الحالات يلزم الحياد فيكون بوسعه أن يأتي بميزات أو عيوب بحسب الطريقة التي يتعامل بها المجتمع معهم. ومن تلك الابتكارات التكنولوجية التي يُتوقع أن تشكل مستقبلنا: الذكاء الاصطناعي والاتصال الفائق والهندسة الحيوية، والحوسبة الكمومية، وتكنولوجيا الفضاء، والروبوتات، والتصنيع الذكي، والواقع المعزز، والاندماج النووي.

الأمر الذي دفع خبراء الشركة "كي بي إم جي" إلى مراجعة الاتجاهات الاجتماعية والاقتصادية والسياسية القائمة في الوقت الحالي، بالإضافة إلى اتجاهات تكنولوجيا المعلومات المستقبلية، وخلصت من تلك المراجعة إلى وضع عدد من سيناريوهات "الاحتمالات المستقبلية" والتي تلقي الضوء على الآثار الاجتماعية والسياسية المحتملة للتقدم التكنولوجي. وتغطي تلك السيناريوهات موضوعات عن العالم الافتراضي والروبوت والذكاء الاصطناعي وأثر المعرفة الكُلّيّة والتكامل بين الإنسان والآلة، وكذلك تبعات واقعنا على المدى الطويل.

تعد دولة الإمارات العربية المتحدة في الواقع من الدول الرائدة في السلامة السيبرانية، إذ تُصنَّف ضمن أفضل خمس دول في العالم في مؤشر الأمن السيبراني العالمي للاتحاد الدولي للاتصالات (ITU) التابع للأمم المتحدة. فضلًا عن ذلك، فإن صياغة التشريعات الإماراتية في مجال الأمن السيبراني للاستعداد للمستقبل خلال ٥٠ عامًا القادمة تتطلب منا التطور بما يفي بوضع إطار عمل تشريعي يضم البشر والذكاء الاصطناعي والجمع بينهما على نحو متسق وبوتيرة متزايدة. علاوة على ذلك فإن الموقف الذي تتبناه دولة الإمارات العربية المتحدة من حيث تقديمها للمساعدات الإنسانية دون النظر إلى الدين أو العِرق أو اللون أو الثقافة لأمر جديرٌ بالثناء. أما في المستقبل، فعلى الأغلب يصبح تعريف المساعدة الإنسانية متطورًا ليشمل «مساعدات الأمن السيبراني» لما للهجمات السيبرانية من تبعات حقيقية ومتزايدة يتحمّلها المتعثرون ممن لا يقدرون على التعامل مع تلك الهجمات.

وفي رؤيتنا للمستقبل، نرى أن التطورات في العالم الافتراضي الإندماجي ستمزج بين الواقع والخيال، ومع انتعاش الشركات في العالم الافتراضي، تصبح البيانات هي الصورة الجديدة للمال. كذلك، ستدخل الروبوتات إلى حياتنا بصورة سلسة بداية من الاعتماد عليها في العناية الشخصية ووصولًا إلى الأنظمة العسكرية، فضلًا عن قدرة الذكاء الاصطناعي على التنبؤ بالمستقبل وتشكيله. وتقوم أجهزة الاستشعار ذات الاتصال الفائق والأسلحة المتقدمة بتوفير معرفة كُلية غير مسبوقة بحيث قد تصل الآلة إلى درجة من التطور تجعلها قادرة على قراءة أفكار البشر والتلاعب بالحمض النووي لنا. وسيلجأ الأغنياء وذوي السلطة إلى الاستنساخ والتلاعب الجيني ونقل ذاكراتهم إلى الذكاء الاصطناعي لزيادة أعمارهم. وختامًا، ففي ضوء التركيز على السلامة، ستظهر سلاسل التوريد التي تتسم بالشفافية ويصبح الأمن السيبراني هو شق الدفاع الوطني الأكثر أهمية.

وهنا تظهر الحاجة إلى النماذج الجديدة التي تنطوي على مستويات أعلى من التفاعل المسموح بين الإنسان وأنظمة الذكاء الاصطناعي، إلى جانب الحاجة إلى أطر عمل جديدة للترخيص. ويُتوقع أن تصبح العمليات السيبرانية أكثر آلية بحيث تعقد شراكات بين مختصي الأمن وأدوات الذكاء الاصطناعي وأنظمة صناعة القرار التي تقدم الدعم لهم.

وقد شهدت دولة الإمارات العربية المتحدة تطورًا بعد مرور خمسين عامًا على التأسيس جعلها مركزًا للتقدم والانطلاق ورمزًا للمثابرة، فضلًا عن كونها مجتمعًا يتصف بالسعادة والترابط. وفي أثناء احتفال الدولة باليوبيل الذهبي، وضعنا أربعة ركائز لمئوية الدولة ٢٠٧١ وهم: حكومة تركز على المستقبل، والتعليم الممتاز واقتصاد المعرفة المتنوع والمجتمع المترابط والسعيد. وحرصنا في كي بي إم جي على تبني تلك الركائز ودعم الإمارات في مستقبلها في ٥٠ عامًا القادمة وبعدهم.

ويسر شركة كي بي إم جي -لوار جلف أن تحتفل بالذكرى الخمسين لتأسيسها بالإمارات، وهي تسعى بدأب للوصول إلى النزاهة والتميز والجسارة في أعمالها كافة. ومن الأسس التي تقوم عليها شركتنا هي تقديم الخدمات بجودة استثنائية والالتزام الشديد بتحقيق المصلحة العامة وبناء فرق عمل ذات قدرات عالية. ونلتزم على مدى العقود القادمة بتكريس دعمنا لرحلة الإمارات من نجاح لنجاح آخر: معًا نحقق الأفضل.

ونتناول في هذا التقرير معلومات قيمة عن القرارات المحتملة التي قد تتخذها الإمارات في سبيل تعظيم مرونتها السيبرانية على مدار ٥٠ عامًا المقبلة، ويشمل ذلك وضع إطار عمل قانوني مرحلي مدعومًا بالقوانين الجديدة التي من شأنها أن تُحسن من قدرة الدولة على التعامل مع الصور المتقدمة من التزييف والخداع والتلاعب والنشاط الإجرامي في فضاء المعلومات.

حازت شركتنا على شرف شهادة نمو وازدهار دولة الإمارات العربية المتحدة على مدار السنوات الماضية، والآن نحن نتطلع إلى المساهمة في تحقيقها للتقدم المتواصل في مجال الابتكارات السيبرانية.

سعادة الدكتور محمد الكويتي
رئيس الأمن السيبراني حكومة دولة الإمارات العربية المتحدة

تيموثي وود
شريك السيبرانية
كي بي إم جي لوار جلف

ماذا لو...

لاستكشاف المستقبل وتحقيقه فقد قمنا بتطوير سلسلة من موضوعات "الاحتمالات المستقبلية" والتي تنقسم إلى سيناريوهات افتراضية على النحو التالي:

الخلط بين الواقع والخيال

إنشاء عوالم افتراضية

لن نتمكن من التفرقة بين الواقع والخيال

يفقد البشر هويتهم في العالم الافتراضي

البيانات

قوة الآلة

ظهور الروبوتات والذكاء الاصطناعي

ستنتشر الروبوتات في كل مكان

ستتمكن الآلات من التنبؤ بالمستقبل

ستصبح الآلات أكثر ذكاءً من البشر

أثر المعرفة غير المحدودة

عالم زاخر بشبكات المستشعرات والمؤثرات والمستجيبات

ستجد الأسلحة أهدافها دائمًا بسهولة

سيكون العالم أجمع مكشوفًا للجميع

تنتشر الآلات العاملة بتقنيات النانو والميكرو في كل مكان

العالم الهجين الجديد

بوتقة واحدة تضم البشر والآلات

ستتنبأ الآلات بجميع متطلباتنا

ستتمكن الآلات من قراءة (أو كتابة) عقولنا

ستتمكن الآلات من قراءة (أو كتابة) الحمض النووي الخاص بالبشر

الحياة، ولكن ليست كما عهدناها

ما الذي سيحدث في واقعنا على المدى الطويل؟

سيندمج البشر والآلات في بوتقة واحدة

قدرات فائقة وإمكانيات لا حدود لها في المستقبل

نعرض في الصفحات التالية مجموعة من السيناريوهات الافتراضية التي تتطرق للوسائل التي سيغزو الابتكار التكنولوجي بها حياتنا.

الخلط بين الواقع والخيال

- تسود التجارة العالم الافتراضي مع ظهور العديد من مجالات الأعمال التي تركز على التجربة الاندماجية
- تكرار مشاهد العالم الحقيقي والأشخاص والتلاعب بهم في الوقت الفعلي
- تصبح البيانات هي الصورة الجديدة للمال

قوة الآلة

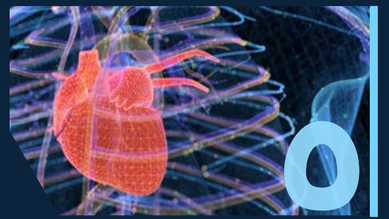
- نتخيل أن تصبح الروبوتات مقبولة في كل منحى من مناحي الحياة ومنها العناية الشخصية والنظم العسكرية
- يصبح الذكاء الاصطناعي قادرًا على توقع المستقبل وتشكيله
- سوف يسود التكامل بين البشر والتكنولوجيا

أثر المعرفة غير المحدودة

- تصبح أجهزة الاستشعار المتصلة بصورة فائقة وآلات النانو والميكرو منتشرة، مما يسمح للدول والشركات بالوصول للمعرفة الكلية
- من المرجح أن تصل الأسلحة إلى أهدافها في أي مكان وبسرعة عالية جدًا

العالم الهجين الجديد

- نتوقع أن تقوم الآلات بتطوير القدرة على قراءة أفكار الناس
- قد تتمكن الآلة من تتبع الحض النووي للبشر وتحليله وكتابته



الحياة، ولكن ليست كما عهدناها

- حلول ٢٠٧١، تقودنا التطورات في الأجهزة الطبية والغرسات العصبية إلى تكامل أجهزة الحواسب والبشر في مجال الموضة والطب وللأغراض الحربية
- الغرسات العصبية قادرة على المساعدة في علاج الأمراض العصبية
- يجد الأغنياء وذوي الصلطة طرقًا لإطالة أعمارهم من خلال الاستنساخ والتلاعب الجيني ونقل ذاكرتهم إلى الذكاء الاصطناعي

مستقبل الامن السيبراني

باستقراء فرضيات "الاحتمالات المستقبلية"، فقد حددنا الإجراءات الأساسية التي يمكننا اتخاذها لتحقيق هذا المستقبل. يتناول هذا التقرير ستة عوامل تعطيل محتملة للعالم كما نعرفه:

- لم تعد هناك أسرار
- لم يثق أحد في تقنية الآخر
- كان لشبكة الإنترنت نظام حماية
- لم تعد أجهزة الكمبيوتر موجودة
- تمكنت أي أمة من الانعزال
- أصبحت الحرب السيبرانية حقيقة واقعة

تحقيق رؤية دولة الإمارات

في حين أننا لن نتمكن أبدًا من التنبؤ بما ستكون عليه الحياة في عام 2071، إلا أنه يمكننا أن نبدأ في رؤية أنماط من التحديات المحتملة. في هذا المنشور، نتعمق في مجموعة متنوعة من المواضيع لفهم الإجراءات التي يمكننا اتخاذها للاستعداد للرياح المعاكسة وضمان غد آمن ومأمون.

- بناء "الثقة" في نسيج مجتمعنا
- الأطر القانونية لعالم جديد من الأشخاص الهجينين والذكاء الاصطناعي والتكنولوجيا
- نماذج أمنية جديدة
- التركيز على الإشراف على أنظمة الذكاء الاصطناعي المستقلة
- التعاون العميق بين المنظمين والتقنيين
- الدفاع في غمضة عين من خلال التكنولوجيا الناشئة
- ما الذي يهم مجتمعنا حقًا؟

كيف يمكننا مساعدتكم في المساهمة في تحقيق رؤية الإمارات العربية المتحدة، بما يتماشى مع مبادئ الخمسين؟

النطاق

لقد تلقينا دعوة من مجلس الأمن السيبراني في دولة الإمارات العربية المتحدة للنظر في مستقبل الأمن السيبراني، والصورة التي سيبدو عليها المشهد عندما تحتفل دولة الإمارات العربية المتحدة بالذكرى المئوية لتأسيسها في عام ٢٠٧١. فوجدنا في تلك الدعوة فرصة لأن نقف مليًا ونتراجع خطوة للخلف على مسار تحديات اليوم والنظر حول الطريقة التي تغير عليها العالم وتطوره خلال العقود القادمة.

دائمًا ما يكون السعي للتنبؤ بأحداث المستقبل بتصور يقيني أمرًا محفوفًا بالخطورة، ولهذا اخترنا أن نسلك نهجًا آخر، فبوسعنا أن نجد بذور الغد اليوم حتى وإن نظرنا إلى ما وراء ٢٠ عامًا. وأخذنا في اعتبارنا كذلك آخر ٥٠ عامًا، وطرحنا على أنفسنا سؤالًا عن الدروس التي يمكننا أن نتعلمها من الماضي.

وانطلاقًا من هذه الاتجاهات الإستراتيجية والتي استقيناها من مجموعة كبيرة من علماء المستقبل، أعددنا مجموعة من السيناريوهات المعقولة ولكنها ليست يقينية بأي حال من الأحوال وهي سيناريوهات "الاحتمالات المستقبلية"، تتناول تلك السيناريوهات التأثير المحتمل للتقدم التكنولوجي على مجتمعنا، وبعض المعضلات التي قد يتسبب فيها من حيث التأثير الاجتماعي والأمن السيبراني والخصوصية.

ثُم حصرنا سيناريوهات "الاحتمالات المستقبلية" في موضوعات، يبدأ كل منها باستخلاص التحديات الكائنة في التعرف على طريقة اختيار المجتمع لتبني تلك التقنيات، مما يفسح المجال ويمهد الطريق أمام القيام بعملية تحليل قضايا الأمن والخصوصية والأخلاق الرئيسية، وكذلك تحليل الطريقة التي قد تستوعب بها دولة الإمارات العربية المتحدة على نحو أفضل تلك القضايا وتشكيل تبنيها لها لصالح مجتمعها.

لا يعرض هذا التقرير رؤية واحدة للمستقبل، إذ يجعله ذلك افتراضيًا وغير واقعيًا، ولهذا فهو يتناول الكثير من الرؤى للمستقبل التي قد تُنشئها التوجهات والسيناريوهات التي نعرضها به. وقد وضعنا نصب أعيننا خيارات ونأمل أن تختار أجيال المستقبل من بينها بحرص وتأنٍ.

"إن الفائدة التي نحصدها من السيناريوهات تتمثل في قدرتها على إجبارنا لنسلك درب المغامرة والخروج عن المألوف ومواجهة استفسارات محفوفة بالتحديات وهي: كيف نسير بعيدًا عن المسارات البائسة، وتحسين النتائج لصالح البشرية، وفضلًا عن تسخير التكنولوجيا لتطويعها للخير؟ تقع مسؤولية اتخاذ هذه الاختيارات وتشكيل مصيرنا المشترك على عاتقنا."

أخيليش توتيجا
رئيس الأمن السيبراني العالمي، وشريك
في شركة كي بي إم جي الهند

الامن السيبراني بين الماضي والحاضر

شكلت السبعينيات العقد الرقمي الذي ميّزه التقدم المحرز في الأجهزة الرقمية، إضافة إلى الأتمتة في الاتصالات اللاسلكية من خلال الاستعانة بتكنولوجيا التحويل الرقمي، وقد زرعت بذور ثورة الحاسوب الشخصي والبريد الإلكتروني والهواتف المتحركة في ذلك العقد، وتحقق النجاح مع تبني التقنية الرقمية المرنة والتصغير والأتمتة، كما رسخت السبعينيات الأسس النظرية الرئيسية لأمن الحاسوب في صورة النموذج Bell-LaPadula (التحكم بالوصول الإلزامي)، وكذلك وأسس التشفير غير المتماثل الحديث في صورة الخوارزمية RSA.

أما عن الثمانينات، فهي عقد الحاسوب الذي شهد تطورات في الأجهزة والبرامج وواجهات المستخدم الرسومية، وظهرت بوادر أدوات الأتمتة المكتبية التي نعرفها اليوم في هذا العقد، وكانت أبرز النجاحات التي تحققت في الثمانينات متمثلة في الحوسبة وسرعة المعالجة ومزايا التكنولوجيا التي شملت الشركات والاستخدامات المنزلية كذلك. ورأينا في هذا العقد القرصنة وهي تتوسع في نطاقها في صورة إلحاق الأذى أكثر من كونها عملًا إجراميًا، وكذلك كان عالم الإنترنت أكثر براءة من الآن وفي عام ١٩٨٨ انتشرت دودة الإنترنت وهي أحد الأمثلة الأولية للبرامج الضارة، ثم ظهرت الفيروسات على الساحة وبدأت تظهر برامج متخصصة في مكافحتها.

وصولًا إلى التسعينيات حيث بدأ عصر البرمجيات، وأصبحت أنظمة التشغيل أكثر قوة وظهرت محركات البحث مع ميلاد شبكة العالم الواسع. وكان النمو -أي القدرة على تمديد نطاق التكنولوجيا بسرعة- هو أحد أبرز الدروس المستفادة من التسعينيات وذلك من خلال تبني البنية التحتية المحدودة سريعًا، وكانت البرمجيات ملائمة لذلك بشكل مثالي. كذلك كانت التسعينيات حقبة العولمة بحيث صعدت شبكة الإنترنت لخارج الولايات المتحدة ونتج عن ذلك زيادة نطاق مجال الأمن السيبراني وتصاعد دور رئيس أمن المعلومات، فضلا عن ظهور أول دليل على عملية تجسس إلكتروني حكومية في صورة Moonlight Maze. أي أن زمن براءة الإنترنت قد أوشك على الانتهاء.

وواصلت فكرة التواصل الشبكي مسارها في العقد الأول من القرن الحادي والعشرين – حيث ظهر الهاتف الذكي وكان ميلاد التطبيقات، ثم التطوير السريع في البنية التحتية للاتصال اللاسلكي عبر الهاتف المتحرك إلى الجيل الثالث ثم الجيل الرابع. وكذلك ظهرت بوادر تقنيات الواقع الافتراضي ثم تلاشت، وكانت على رأس الموضوعات المهمة التنقل والتطبيقات وظهور مفهوم الوصول من أي مكان – بداية فكرة العالم المتواجد دائمًا- انتشرت ديدان الإنترنت وغيرها من البرامج الضارة التي تنتشر ذاتيًا مثل كونفيكر (Conficker) في عام ٢٠٠٨. ثم غدا مجتمع أمن الحواسيب ناضجًا على الرغم من كون التركيز منصبًا على أساسيات التصحيح وتقنيات جدار الحماية المبكرة ومنع البرامج الضارة.

كان العقد الثاني من القرن الحادي والعشرين عصر المعلومات، حيث بدأت خدمات وسائل التواصل الاجتماعي والتي كان ميلادها في العقد الأول منه في أن تحدث تأثيرًا هائلًا، وكذلك بدأ ظهور البنية التحتية السحابية العامة إلى جانب البرمجيات بوصفهم خدمة مقدمة، حيث بدأت الشركات تتوسع بطرق جديدة، وكانت بداية العقد شاهدة على ظهور STUXNET وهو أول برنامج ضار يستهدف التكنولوجيا التشغيلية. وكذلك شهدنا زيادة سريعة في السيبرانية المنظمة، بما في ذلك انتشار برامج الفدية التي جرى تفعيلها باستخدام عملة مشفرة. وأصبح الأمن السيبراني مهنة، وطالب مشرعو القوانين تعزيز تدابير حماية البنية التحتية المهمة، وتقدمت تشريعات الخصوصية، فضلا عن ميلاد عمليات التشغيل الأمنية إلى جانب إستراتيجيات ومراكز للأمن السيبراني الوطني.

وعلى ما يبدو فإنه من المبكر جدًا التيقن مما سيجري في **العشرينيات من القرن الحادي والعشرين،** فهذا هو عصر المعلومات ذات الاتصال الفائق والتشبيك وكذلك التلاعب بالمعلومات، بل وإسقاط الطاقة عبر الفضاء الإلكتروني. وهو كذلك عقد الذكاء الاصطناعي والذي يثير أسئلة أخلاقية وقد يحدث تحولًا في القوى العاملة لدينا للأبد، إلا أننا لا نزال في بداية عقد العشرينيات.

وبالنظر إلى دولة الإمارات العربية المتحدة، فإننا نرى تحولًا هائلاً عبر العقود ومنذ أن تأسس الاتحاد في عام ١٩٧١، وهو التحول الذي يعكس ما يحدث حول العالم، مع التركيز على وجه التحديد في السنوات الأولى على الطاقة والنقل واللوجيستيات والبنية التحتية والاستثمارات، ومؤخرًا أصبح لدى قيادة البلاد البصيرة للترويج والاستثمار في مجالات استراتيجية مثل الرقمنة والذكاء الاصطناعي والجيل القادم من اتصال النطاق العريض وقطاع الفضاء، مما يمهد الطريق للإمارات لأن تتبنى التقنيات الرقمية بوتيرة سريعة.

وتعد دولة الإمارات العربية المتحدة في الوقت الراهن إحدى أكثر دول العالم تقدمًا على المستوى التكنولوجي والرقمي بحيث يساهم الاقتصاد الرقمي بنسبة ٤,٣٪ في إجمالي الناتج المحلي – بل ولا يزال النمو مستمرًا. وقد عكفت الإمارات على تعزيز الإمكانات الرقمية من خلال تحسين البنية التحتية لتكنولوجيا المعلومات، وزيادة سرعة خدمات الإنترنت، وتشجيع استخدام الهواتف الذكية وأنظمة الدفع الإلكترونية. وكذلك يحتل الأمن السيبراني مركز التكنولوجيا والذكاء الاصطناعي والثورة الصناعية الرابعة.

الامن السيبراني بين الماضي والحاضر

قبل أن نشرع في رحلتنا إلى المستقبل، علينا أن نتوقف وننظر لتاريخنا عبر ٥٠ عامًا مضت

١٩٧٠

١٩٧١

دودة الحاسوب **Creeper First** وبرنامج مكافحة الفيروسات Reaper

١٩٨٠

١٩٨٨

إطلاق **دودة موريس** أول دودة إنترنت

١٩٩٠

٢٠٠٠

١٩٩٦

بدأت **Moonlight Maze** أول هجوم تجسس إلكتروني واسع النطاق

٢٠١٠

٢٠١٠

عمل برنامج **Stuxnet** أول هجوم على نظام صناعي معلن على نطاق واسع.

٢٠٢٠

٢٠١٧

Wannacry وNot Petya، هجمات برامج الفدية الضخمة على نطاق عالمي لها تأثير وهجمات على مستوى الدول.

والآن .. ما التالي؟

نفخر بماضينا ...لمحة عن تاريخ الإمارات العربية المتحدة

وبالنظر إلى دولة الإمارات العربية المتحدة، فإننا نرى تحولًا هائلاً عبر العقود ومنذ أن تأسس الاتحاد في عام ١٩٧١، وهو التحول الذي يعكس ما يحدث حول العالم، مع التركيز على وجه التحديد في السنوات الأولى على الطاقة والنقل واللوجيستيات والبنية التحتية والاستثمارات، ومؤخرًا أصبح لدى قيادة البلاد البصيرة للترويج والاستثمار في مجالات استراتيجية مثل الرقمنة والذكاء الاصطناعي والجيل القادم من اتصال النطاق العريض وقطاع الفضاء، مما يمهد الطريق للإمارات لأن تتبنى التقنيات الرقمية بوتيرة سريعة.

وتعد دولة الإمارات العربية المتحدة في الوقت الراهن إحدى أكثر دول العالم تقدمًا على المستوى التكنولوجي والرقمي بحيث يساهم الاقتصاد الرقمي بنسبة ٤,٣٪ في إجمالي الناتج المحلي – بل ولا يزال النمو مستمرًا. وقد عكفت الإمارات على تعزيز الإمكانات الرقمية من خلال تحسين البنية التحتية لتكنولوجيا المعلومات، وزيادة سرعة خدمات الإنترنت، وتشجيع استخدام الهواتف الذكية وأنظمة الدفع الإلكترونية. وكذلك يحتل الأمن السيبراني مركز التكنولوجيا والذكاء الاصطناعي والثورة الصناعية الرابعة.

بداية من ١٩٧١

أعلن حكام أبوظبي ودبي والشارقة وعجمان والفجيرة وأم القيوين تأسيس الدولة الجديدة..

١٩٧٣

أصبح الدرهم عملة دولة الإمارات العربية المتحدة

١٩٨١

انطلاق مجلس التعاون الخليجي رسميًا في أبوظبي

١٩٨٥

افتتاح الخطوط الجوية الإماراتية

٢٠٠٤

صاحب السمو الشيخ خليفة بن زايد آل نهيان رئيسًا لدولة الإمارات العربية المتحدة

٢٠٠٦

تسجيل الرئيس في السجل السكاني ونظام بطاقة الهوية، وبدء التدشين الرسمي لهذا البرنامج الوطني، أكبر برنامج تكنولوجي في منطقة الشرق الأوسط

٢٠٠٩

أبوظبي تصبح مقرًا للوكالة الدولية للطاقة المتجددة إطلاق مترو دبي، أطول نظام قطار آلي بدون سائق في العالم وأول مترو في منطقة الخليج

٢٠١٣

افتتاح "شمس ١"، أكبر محطة للطاقة الشمسية في العالم في مدينة زايد

٢٠١٤

الإمارات تعلن إنشاء وكالة الإمارات للفضاء للإشراف على مهمة المريخ

٢٠١٧

إطلاق استراتيجية الإمارات للذكاء الاصطناعي، كأحد أهداف مئوية الإمارات ٢٠٧١

٢٠١٨

«خليفة سات» يصنع تاريخ الإمارات مع وصول أول قمر صناعي على أرض الإمارات إلى الفضاء

٢٠١٩

الإمارات تصنع التاريخ بوصول هزاع المنصوري إلى الفضاء

٢٠٢٣

أعلن صاحب السمو الشيخ محمد بن زايد آل نهيان، رئيس الدولة، أن عام ٢٠٢٣ سيكون «عام الاستدامة»، مع استلهام العمل الجماعي من خلال الالتزام الوطني بالممارسات المستدامة، تماشيًا مع الاستراتيجية الوطنية لدولة الإمارات العربية المتحدة.

الاتجاهات الكبرى

ماذا تحمل جعبة الأمن السيبراني في ٥٠ عامًا القادمة؟ تضم الاتجاهات الكبرى التي تشكل عالمنا :

التركيبة السكانية

يُتوقع أن يصل التعداد السكاني في العالم إلى ٩,٧ مليار نسمة بحلول عام ٢٠٥٠، مع اختلاف معدلات النمو السكاني بحسب المنطقة، حيث تبلغ أوروبا وأمريكا الشمالية ذروة تعدادها في أواخر ٢٠٣٠، ويتضاعف تعداد سكان أفريقيا جنوب الصحراء الكبرى بحلول عام ٢٠٥٠. وبذلك تتسبب الطبيعة المتغيرة للتركيبة السكانية في جلب تحديات شديدة الاختلاف تتراوح من السكان البالغين سن الشيخوخة وانخفاض معدلات الخصوبة وزيادة أعباء الدين/ الضرائب في بعض الاقتصادات المتقدمة والصين، وكذلك تحديات البنية التحتية والتعليم وسط التعداد السكاني المتزايد مع افتقاره للتحضر في أفريقيا جنوب الصحراء الكبرى وجنوب أسيا.

أما عن تعداد دولة الإمارات العربية المتحدة، فمن المتوقع أن يزيد إلى ١٠,٩ مليون نسمة في السنوات العشرين المقبلة مع تضاعف التعداد السكاني لإمارة دبي وبعد انتهاء موجة الهجرة بعد الوباء، فضلًا عن مساهمة عوامل مثل التنويع الاقتصادي وجذب العمال الأجانب ومساهمتهم إلى حد كبير في الزيادة السكانية.

التغير المناخي

من المتوقع أن تؤدي السياسات المطبقة حاليًا إلى مزيد من الاحترار العالمي بمقدار ٢,٨ درجة خلال الفترة التي تسبق عام ٢١٠٠، مع تضاؤل دور الإجراءات العالمية للحد من ذلك الاحترار إلى ١,٥-٢ درجة. ومن المتوقع أن تؤدي التغيرات في المناخ إلى مشكلات الأمن الغذائي ونزوح السكان وتدهور النظام البيئي أيضًا، وكذلك احتمالية اشتعال الصراعات.

تراقب دولة الإمارات العربية المتحدة واقع ارتفاع درجات الحرارة الأليم والجفاف الناجم عن التغير المناخي، الأمر الذي دفعها إلى تدشين مبادرات متعددة للعمل المناخي لتحقيق التوازن بين المكاسب القصيرة المدى من الوقود الأحفوري وحتمية البقاء الناشئة عن تغير المناخ.

التحديات الصحية

يتسبب تزايد مقاومة مضادات الميكروبات ذات الصلة بزيادة خطر انتقال العدوى بين البشر بمسببات الأمراض الحيوانية نتيجة زيادة الكثافة السكانية والتنقل، في زيادة خطر الوباء. ومع توقعات زيادة الأعمال تنتج ضغوط على أنظمة الرعاية الصحية المرتبطة بمرض السكري وأمراض القلب والأوعية الدموية والسرطان وأمراض الجهاز التنفسي المزمنة.

يستهدف مشروع المئوية ٢٠٧١ الذي أطلقه مجلس الوزراء الإماراتي أن تصبح دولة الإمارات العربية المتحدة أفضل دولة في العالم بحلول عام ٢٠٧١، بحيث ينعم سكانها بصحة جيدة وإمكانية الوصول إلى أعلى معايير الرعاية الصحية. وكذلك، تركز أجندة الرعاية الصحية لدولة الإمارات العربية المتحدة لعام ٢٠٧١ على السياحة الطبية والمعالجة الطبية عن بعد واستخدام الذكاء الاصطناعي والتكنولوجيا السحابية في مجال الرعاية الصحية وتنظيم استخدام وسائل المعالجة الطبية عبر الإنترنت.

وحتمًا ستشكل اتجاهات التكنولوجيا عاملًا محددًا رئيسيًا في العالم الذي نحيا فيه، وبعضها من شأنه أن يساعدنا في التعامل مع التحديات، والبعض الآخر قد تكون له تبعات أكثر تعقيدًا وقد تغير من أنماط حياتنا للأبد، فالثورة الصناعية الرابعة في مهدها وقد يمر وقتًا طويلًا عليها لحين ٢٠٧١.

الذكاء الاصطناعي

يأتينا الذكاء العام الاصطناعي بعد ما شهده الذكاء الاصطناعي من تطور سريع، وستزيد التطبيقات المتخصصة في المجال خلال العقد القادم.

الاتصال المفرط

يسمح التطور الذي تشهده البنية التحتية للشبكات بتمكين عرض نطاق ترددي أكبر وربطًا بينيًا كبيرًا للأجهزة، وكذلك يدعم المزيد من التطوير لإنترنت الأشياء وأجهزة الاستشعار والمؤثرات المنتشرة

الهندسة الحيوية

التطور في الأجهزة الطبية والمعدات الطبية المركبة داخل الجسم (بما يشمل الوصلات العصبية والأطراف الصناعية المتقدمة)، وفي تسلسل الجينوم ومعالجته للاستخدامات النافعة وغير النافعة، وفي علاجات مركبة خصيصًا.

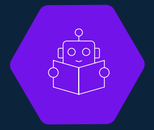
الحوسبة

تطور الحوسبة مما أدى إلى تعطيل نموذج الحوسبة الرقمية الحالي وزيادة قوة الحوسبة زيادة هائلة، وذلك بسبب التطورات في الاتصالات الآمنة الكمية.

تكنولوجيا الفضاء

يستمر السباق نحو الفضاء مع زيادة فرص الوصول وانخفاض تكاليف الإطلاق، وتعزيز وجود البشر بين الكواكب، فضلا عن المهمات الفضائية الأكثر تطورًا، إلا أنه لا تزال هناك مخاطر من حطام المركبات الفضائية والهجمات المضادة من الفضاء.

الروبوتات



يشهد عالم الروبوتات مجموعة كبيرة من التطورات بحيث تصبح أكثر تعقيدًا وانتشاراً في جميع مجالات الحياة بدءًا من التطبيقات الصناعية والعسكرية المرتفعة المخاطر، مروراً بالطائرات بدون طيار المتقدمة، ووصولًا إلى الروبوتات المجسمة للعناية الشخصية والأجهزة الروبوتية الجراحية المصغرة.

التصنيع الذكي

التطور المستمر لتقنيات الطباعة الثلاثية الأبعاد والقدرة على توفير أنظمة تصنيع مخصصة للغاية ومخصصة، والمتصلة بنماذج التسليم في الوقت المناسب

تقنية الواقع المعزز

ابتكار أنظمة الواقع المعزز العالية الدقة وغير التدخلية وبيئات واقع افتراضي إندماجي للغاية، وذلك بسبب التطورات المحتملة في غرسات الخلايا العصبية وتقنيات التحفيز العصبي

الاندماج النووي

إتاحة الاندماج النووي على نحو متزايد بما في ذلك تطورات المفاعلات الصغيرة يؤدي (إلى جانب زيادة مصادر الطاقة المتجددة) إلى تغييرات جوهرية في الاعتماد على مصادر الطاقة المعتمدة على النفط والغاز.

سيناريوهات "الاحتمالات المستقبلية"

لتجسيد شكل المستقبل على أرض الواقع، أعددنا سلسلة من سيناريوهات "الاحتمالات المستقبلية" التي ينطوي كلٌّ منها على التداعيات الاجتماعية السياسية المحتملة لعمليات المزج بين التقنية والتوجهات المعاصرة.

الخلط بين الواقع والخيال

ماذا لو... لم نتمكن من التفرقة بين الواقع والخيال

الواقع المُعزّز

الذكاء الاصطناعي

> "أين سنضع الحدّ الفاصل، أو ماذا سيحدث في حالة حدوث هجرة ذات اتجاه واحد من العالم المادي إلى العالم الافتراضي؟ إذا ما فكرنا في طبيعة هذه الأسئلة، لا نستبعد أن يكون للفلسفة دور في هذا الشأن."

براساد جارايامان

رئيس الأمن السيبراني على نطاق دول الأمريكتين وشريك في شركة كي بي إم جي في الولايات المتحدة

تتناول المجموعة الأولى من المجموعات الخمسة لسيناريوهات "الاحتمالات المستقبلية" إنشاء عوالم افتراضية وقيمة الأصول في هذه العوالم من وجهة نظرنا وقدرتنا على التفرقة بين الواقع والتجربة الاصطناعية.

بحلول عام ٢٠٧١، ستؤدي التطورات في الواقع الافتراضي المنتشر وتقنيات التزييف العميق والتلاعب السلوكي إلى الخلط بين الواقع والخيال. ففي هذا العالم، لن نكون على يقين من أن الكيانات المحيطة بك واقعية أم خيالية. إذ يمكن نسخ ومحاكاة مشاهد العالم الواقعي والتلاعب بها في الوقت الحقيقي، وإيجاد نسخ طبق الأصل من البشر والتعامل معها كأنها حقيقية ولا مراء فيها. إذ سنتمكن من تجاوز هذا الوادي الخارق للطبيعة.

كانت الحقيقة دائمًا شيئًا غير موضوعي، ولكن لن يكون أمام البشر في هذا العالم الجديد وسائل عديدة للتفرقة بين الواقع والخيال، كما أنهم سيكونون على استعداد أكثر لتصديق ما يتمنون أن تكون "حقائق" فعلية. سيؤدي التفكير الجمعي إلى نشأة غرف صدى ذاتية التعزيز تضم وجهات نظر متطرفة بصورة متزايدة، يعززها الاختيار الذاتي للمحتوى إضافة إلى لوغاريتمات تؤكد الظواهر الاستثنائية. ستزخر شبكة الإنترنت بعدد لا حصر له من الحالات المنفصلة متعددة الأشكال.

ينبغي أن تعثر المجتمعات على وسائل من شأنها الحفاظ على الثقة والحدّ من الحالات المتطرفة للتلاعب بالواقع إلى جانب توفير الأدوات المساعدة لذلك للبشر (أو للآلات). تستغل بعض السلطات هذا الأمر لتوفير بيئات تحكّم متكاملة، وتتولى سلطات أخرى إنشاء مصادر معلومات محددة وموثوقة ولكنها تميل للتلاعب في هذه الحقائق.

وسيكتسب مفهوم الثقة أهمية متزايدة مثل مفهوم تأمين "الواقع". إذ تجد الجريمة عدة وسائل للتلاعب من خلال الهندسة الاجتماعية، تمامًا مثلما تفعل الدول والشركات التي تسعى إلى التحكم في سرد الأخبار والقصص والتأثير في سلوكيات الشعوب والسكان. ومن ثم يكون لصحة المعلومات أولوية قصوى مع الحاجة إلى وجود آليات قوية ومتكاملة لكشف التلاعب والتزوير. وتصبح الفلترة والإيقاف التلقائي لبعض المعلومات هو النمط السائد والدارج. وتنتشر المخاوف بشأن الخصوصية في ظل نشأة أشخاص مزيفة والتلاعب في هويات الأشخاص الحقيقيين. وهنا تنشأ أطر عمل قانونية تهدف إلى حماية الصور الشخصية ولكنها تسعى في الوقت نفسه لمواكبة التطور في التلاعب القائم على الذكاء الاصطناعي.

الخلط بين الواقع والخيال

ماذا لو... فقد البشر هويتهم في العالم الافتراضي

الواقع المُعزّز

الهندسة البيولوجية

استمر تطور تقنية الواقع الافتراضي من خلال تتبّع حركة شبكية العين والنماذج المُصغّرة لنظم الواقع الافتراضي وردود الفعل اللمسية المُحسنة. كما شهد استخدام الواقع المُعزّز انتشارًا هائلاً. ونشأت العديد من نماذج الأعمال الجديدة في العالم الافتراضي القائمة على توفير تجارب مُصممة بحسب طلب العملاء وإيجاد أنماط تفاعل جديدة ووسائل لتعزيز التحفيز. أصبح جمع البيانات الشخصية والسلوكية على نطاق واسع أمرًا مألوفًا في ظل سعي الشركات لتوفير أنماط تفاعل مُصممة بحسب حاجة العملاء ولا يمكن الاستغناء عنها.

وتزداد أهمية وقيمة الأصول الافتراضية في ظل إقبال الأشخاص (والشركات) على صياغة تجاربهم وصورهم الرمزية بحسب الرغبة.

كما تجد ظواهر مثل التدليس والابتزاز والسلب والرشوة تجليات ومظاهر جديدة. تناضل وسائل إنفاذ القانون والأطر القانونية الشرعية من أجل مجاراة وتيرة الابتكار والإبداع. تتحول الخصوصية إلى مشكلة كبرى في ظل تنامي القدرة على تجميع البيانات الشخصية واستغلالها. كما يجب أن تتطور القواعد والمعايير الرامية إلى حماية المساحات الشخصية في العالم الافتراضي وتجنّب التسلل إليها واقتحامها.

تتطور تحديات الأمن السيبراني فيما يتعلق بحماية الأصول الافتراضية ووسائل التحكم في الوصول في العوالم الافتراضية، إلى جانب وسائل التحكم الدقيقة في عمليات التفاعل المسموح بها بين العناصر، بما في ذلك الصور الرمزية.

”في سباق التميز نحو الاقتصاد الرقمي المستدام سيكون السبق لتلك الحكومات التي يمكنها تحقيق التوازن بين متطلبات الأمن السيبراني والنمو الاقتصادي. يستلزم تحقيق هذا التوازن صياغة اللوائح والسياسات التي تمكن القطاعات المختلفة من الازدهار مع ضمان المرونة في مواجهة التهديدات السيبرانية المتطورة باستمرار. على الحكومات المستشرفة للمستقبل الاستثمار في التقنيات المبتكرة، واعتماد استراتيجيات مرنة، تعزز ثقافة تأمين مستقبل مزدهر رقميا.“

سعادة يوسف حمد الشيباني
مدير عام مركز دبي للأمن الإلكتروني

الخلط بين الواقع والخيال

ماذا لو... كانت البيانات ثروة حقيقية

الواقع المُعزّز

التواصل المفرط

بحلول عام ٢٠٧١، ستصبح البيانات هي الشكل الجديد من النقود وسيستفيد الأشخاص ماديًا من خلال مدى استغلال البيانات الخاصة بهم وتحويلها والاستفادة منها. وستصبح حقوق استغلال البيانات أحد الأصول الأساسية في الشركات إلى جانب عناصر الميزانيات العمومية التقليدية. وسيحصل الأشخاص على تعويضات ومزايا في مقابل المعاملات الدقيقة على البيانات.

في المستقبل، ستصبح حقوق الحصول على البيانات الخاصة بسمات وسلوكيات الأشخاص واستغلالها إحدى السلع التجارية الرئيسية. وهذا لدرجة أن الأشخاص لن يقدموا البيانات بشكل مباشر، نظرًا لإمكانية استنتاجها بسهولة من خلال عمليات تحليلية متطورة.

ستطبق مختلف المجتمعات نماذج مختلفة للغاية على حقوق الأشخاص (بل وربما على وسائل الذكاء الاصطناعي) وذلك للتحكم في كيفية استغلال هذه البيانات. ستتطور لوائح الخصوصية لأنها ستسعى إلى التعامل مع هذا التعقيد، في ظل وجود العديد من الضغوط التجارية لاستغلال البيانات لمصلحتها لتحقيق مكاسب، مما يؤدي إلى تجاوز الابتكار للوائح وتطور المعايير المجتمعية.

وستجد الجرائم السيبرانية وسائل عدة للاستيلاء على البيانات الشخصية بطرق جديدة والاستفادة منها جيدًا لاستغلال الأشخاص والتلاعب بهم. فهل سيتمكن الأشخاص من تتبّع بياناتهم الشخصية وإدراك كيفية استفادة تلك الجماعات الإجرامية منها واستغلالها؟

ماذا لو... انتشرت الروبوتات في كل مكان

الروبوتات

الذكاء الاصطناعي

"إذا حققت الآلات السيطرة الكاملة، ما الأمور التي سنفقدها؟ وإذا فقدنا القدرة على الإبداع والعبقرية والتكيف المجتمعي، فهل سيتم التخلي عن المهارات والخبرة البشرية؟"

جيمس مابوت
شريك في فيوتشرز كي بي إم جي،
كي بي إم جي استراليا

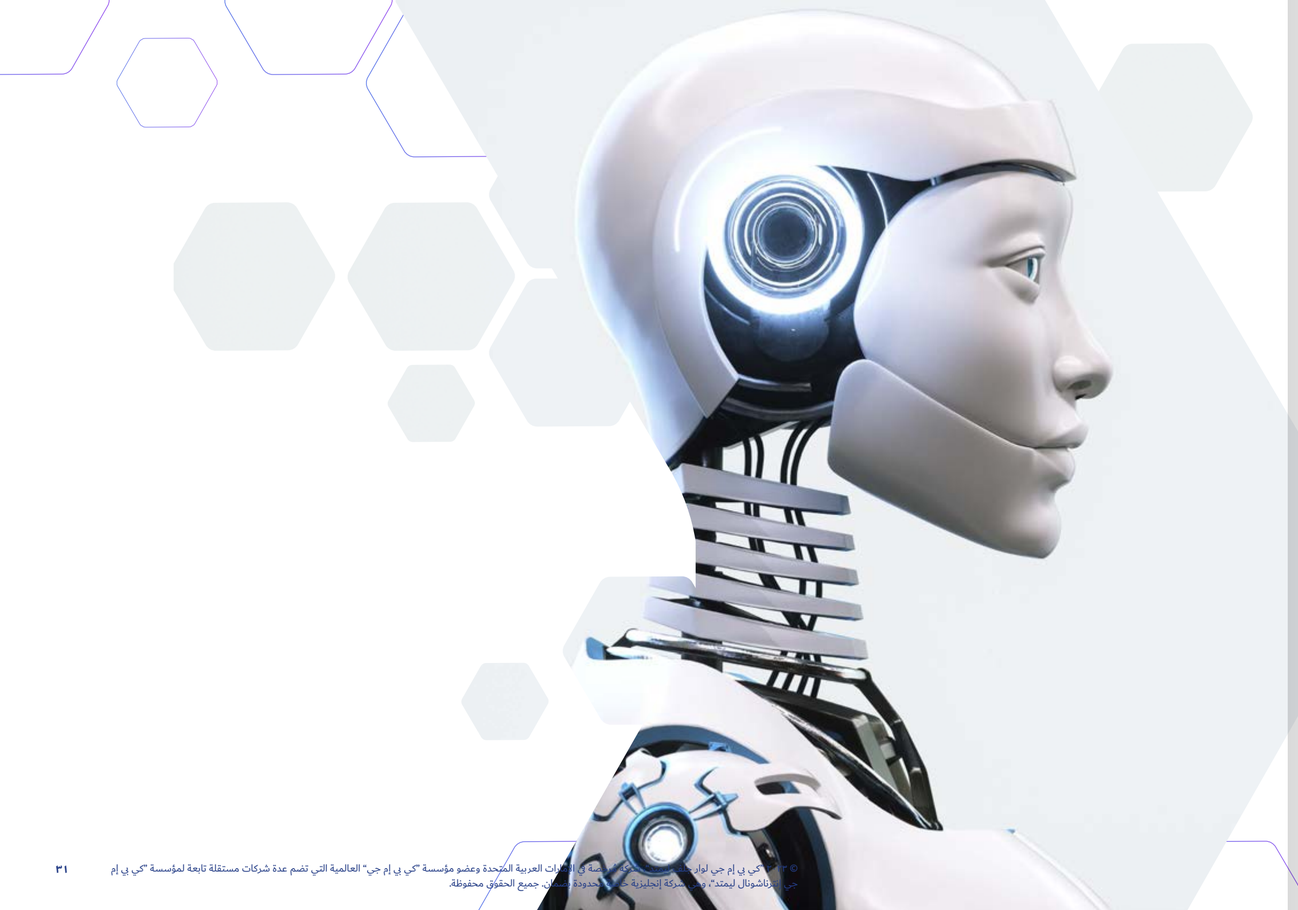
المجموعة الثانية من مجموعات سيناريوهات "تخيل لو" تركز على تطوير الروبوتات والذكاء الاصطناعي، وما قد يعنيه هذا لمجتمعنا.

بحلول عام ٢٠٧١، تغيرت أنماط العمل واصبحت الروبوتات تقوم بالعديد من المهام اليدوية، وتم إعادة تشكيل العديد من مهن الخدمات الشخصية مع تولي الروبوتات أدوار الرعاية. أصبحت الصيانة والتصنيع أنشطة روبوتية.

هناك عدد من الأسئلة الجوهرية التي تتعلق بالمعايير التي تحكم كيفية استخدام هذه الروبوتات، والحدود المفروضة على تعاملها مع الكائنات البشرية. قد أدت احتمالية التلاعب في الروبوتات الى تطبيق معايير أكثر صرامة على صعيد الأمن السيبراني وسلامة الأدوات والأجهزة التي تتفاعل معنا مباشرة أو التي سيؤدي التالعب بها الى عواقب مهلكة.

خلال الثورتين الصناعيتين الأولى والثانية، تعايشت الآلات مع البشر فقط كأدوات أساسية أو كانت تعمل بشكل مستقل. الثورة الصناعية الثالثة كانت بمثابة تحول نحو تعاون ديناميكي، حيث يشارك البشر والآلات مساحة العمل والموارد بشكل مؤقت. مع ظهور "الصناعة ٤,٠" و تكنولوجيا المعلومات المتقدمة، من المتوقع أن تتطور العلاقة بين الإنسان والآلة وفقا لنموذج C5: التعايش، التعاون، التشارك، الرحمة، والتطور المشترك.

لقد فتح التقدم السريع للتكنولوجيا إمكانية للآلات لتحقيق مستوى من الذكاء يسمح لها بأداء المهام دون تعليمات محددة. وبالتالي، فإن تكنولوجيا واجهة الإنسان والآلة تتحول تدريجيا من نظاما معلوماتيا إلى وكلاء مستقلين.



ماذا لو... أصبحت الآلات أكثر ذكاءً من البشر

الذكاء الاصطناعي

بحلول عام ٢٠٧١، ستسفر التطورات في الذكاء الاصطناعي عن ابتكار آلات تتمتع بالإحساس والذكاء العام. وقد بدأت الآلات بالفعل في التفوق على البشر في بعض المجالات. وبدأ الذكاء الاصطناعي في إعادة تشكيل وصياغة عالمنا وتغيير طبيعة العمل. وقد أدى الاستغلال الفعّال للذكاء الاصطناعي إلى استفادة الدول والمؤسسات من ميزة تنافسية في العديد من المجالات.

أسفر تطور عمليات الذكاء الاصطناعي عن إحداث فوضى بمجتمعنا. ففي أفضل الأحوال، يمكننا عقد شراكة مفيدة مع عمليات الذكاء الاصطناعي، وفي أسوأها قد تتسبب هذه العمليات في إحداث فوضى مجتمعية أقرب إلى الثورة الصناعية حيث يُحرم الناس من حقوقهم ويتعرضون للإهمال.

ويجب أن تتطور أطر العمل المعنية بالإشراف على تطبيق الذكاء الاصطناعي ومراقبته بوتيرة سريعة ومن المحتم أن ينطوي ذلك على الإشراف على عمليات الذكاء الاصطناعي من قبل عمليات ذكاء اصطناعي أخرى.

ستؤدي قواعد البيانات المجتمعية التي تتجاوز حدود قدرة الذكاء الاصطناعي والتعقيدات الأخلاقية التي تنطوي على تطبيقها إلى تأخير تطور التقنية نفسها. ويستمر الجدل القانوني حول الحالة المؤسسية لعمليات الذكاء الاصناعي وأحقيتها في تمثيل البشر، إضافة إلى المسؤولية عن الأضرار التي تنجم عن استخدام تقنية الذكاء الاصطناعي.

وقد يسفر تطبيق تقنية الذكاء الاصطناعي عن إطلاق سباق تسلّح جديد. ومن المتوقع أن تستخدم الأنظمة الشمولية الذكاء الاصطناعي لتعزيز أمنها الوطني ومكتسباتها، بينما ستتعاون المجتمعات الأكثر انفتاحًا لابتكار أدوات قائمة على الذكاء الاصطناعي ولكنها ستسعى جاهدة إلى وضع معايير تنظيمية في ضوء وتيرة تطور التقنية.

وستستغل الجريمة المنظمة التقنية من خلال عمليات الذكاء الاصطناعي العدائية، ولكن الدول الوطنية ستفعل الشيء نفسه دفاعًا عن مصالحها. ستتجاوز التفاعلات بين أدوات وأجهزة الذكاء الاصطناعي قدرة البشر على الفهم والتحكم في تفاعلاتهم وسلوكياتهم الناشئة عن ذلك.

”غرس الثقة في الذكاء الاصطناعي يعتمد على بناء الأنظمة الذكية بشكل مسؤول واتباع المعايير الدولية التي تحمي خصوصية وأمن الدول والحكومات.“

م. أحمد بن سعيد الصياح
مدير عام هيئة الحكومة الإلكترونية

ماذا لو... تمكنت الآلات من التنبؤ بالمستقبل

الحساب الكمّي

الذكاء الاصطناعي

بحلول عام ٢٠٧١، ستتمكن الآلات من التنبؤ بأفعال البشر وتصرفات المجموعات الاجتماعية بمستويات أعلى من الثقة، إلى جانب التعرّف على كيفية وتوقيت التدخّل لتشكيل ذلك المستقبل.

وهنا تنشأ أسئلة جوهرية بشأن أطر العمل التي تحكم تشغيل عمليات الذكاء الاصطناعي عندما تصل هذه العمليات إلى النقطة التي يمكنها فيها التلاعب بصورة مؤثرة في البشرية من خلال ملاحظة سلوكياتنا والتحكم في جوانب فضائنا المعلوماتي وعالمنا الافتراضي، وذلك من خلال السياسة والدين.

هل ستؤدي عمليات الذكاء الاصطناعي إلى تطوير التفكير المستقل وحرية الإرادة .... وهل ستتحدد ردود أفعالنا من خلال تدخلات عمليات الذكاء الاصطناعي نفسها؟ هل ستحتفظ البشرية بالإرادة الحرة والابتكار والإبداع في هذا العالم الجديد الزاخر بالتحديات؟ تركّز المجموعة الثالثة من سيناريوهات «الاحتمالات المستقبلية» على نماذج المعرفة غير المحدودة والسلطة المطلقة في هذا العالم الجديد القائم على التقنية.

أثر المعرفة غير المحدودة

ماذا لو... كان العالم أجمع مكشوفًا للجميع

التقنيات المحورية: تقنية الفضاء | التواصل المفرط | الذكاء الاصطناعي

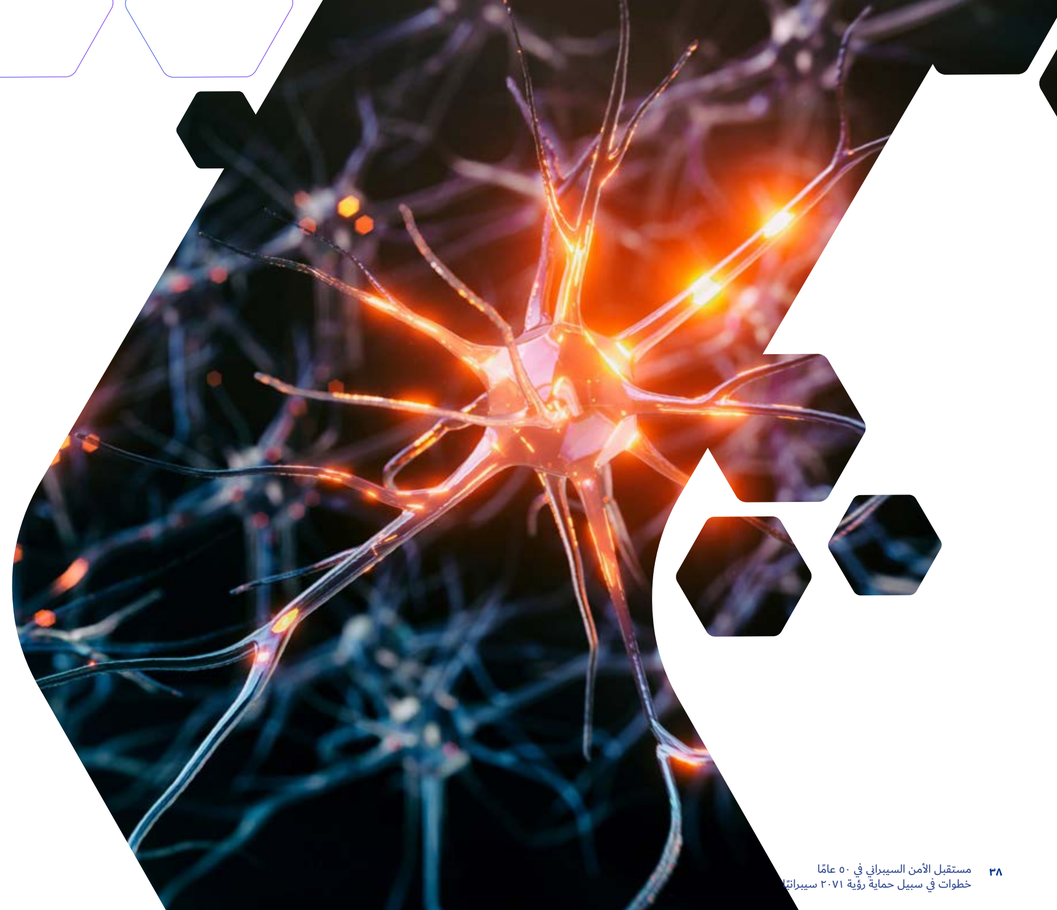
> ”السلطة في هذا العالم الجديد ستقع في يد من يمكنهم التدخّل في العالم الواقعي والافتراضي على نطاق واسع وبسرعة وبوسائل غير متوقعة.“

ديفيد فيربراش
رئيس عالمي لابتكارات الأمن السيبراني
كي بي إم جي انترناشيونال

بحلول عام ٢٠٧١، ستنتشر المستشعرات شديدة التواصل والترابط في جميع أنحاء المدن الذكية وقائمة على تطورات في تقنية الأقمار الاصطناعية الصغيرة وطائرات الدرون. تتيح شبكة الرصد والمراقبة المتصلة بتقنية ذكاء اصطناعي متطورة للدولة (أو المؤسسة) الحصول على المعرفة غير المحدودة. يتيح تجميع البيانات الشخصية ودمجها استنتاج العديد من الأمور حول سلوكنا البشري.

تغيرت أنماط الجريمة في ظل هذه البيئة الجديدة الزاخرة بوسائل المراقبة بفضل القدرة على كشف الاعتداءات الجسدية وعمليات السطو وجرائم الممتلكات بسرعة والإبلاغ عنها. نشأت أنماط جرائم جديدة، بما في ذلك الخداع واستغلال شبكة المستشعرات، إلى جانب اللجوء إلى الجريمة في العالم الافتراضي باستخدام وسائل تخفّي سيبرانية متطورة.

تضع بعض المجتمعات توقعات معقدة بشأن الخصوصية، بما في ذلك إنشاء مساحات خالية من المراقبة، وتضع أيضًا قيودًا على تجميع بيانات المراقبة ومعالجتها إضافة إلى فرض عقوبات على إساءة استغلالها. وفي مجتمعات أخرى، تتمكن الدولة أو الشركات من فرض هيمنتها من خلال الاستخدام الخيّر والمؤذي لهذه الميزة المعلوماتية. وتبدو المعايير العالمية المرتبطة بالخصوصية خادعة ومستقلة من الجانب الثقافي.



أثر المعرفة غير المحدودة

ماذا لو...
انتشرت الآلات العاملة بتقنيات النانو والميكرو في كل مكان

الروبوتات

عمليات التصنيع الذكيّة

بحلول عام ٢٠٧١، ستنتشر الآلات العاملة بتقنية النانو والميكرو في كل مكان وستكون قادرة على استخلاص الطاقة من بيئاتها. وستتولى هذه الآلات القيام بالعديد من الأدوار بداية من طائرات الدرون العاملة بتقنية الميكرو والمستشعرات الميكروسكوبية والمجسّات العاملة بتقنية النانو وصولاً إلى المؤثرات العاملة بتقنية الميكرو القادرة على التعامل مع الجسد البشري.

يمكن نشر وسائل المراقبة في كل مكان بفضل استخدام طائرات الدرون العاملة بتقنيات الميكرو دقيقة الحجم والتي ستتيح استخدام تطبيقات شديدة السريّة إلى جانب توفير المرونة من خلال نشرها بأعداد هائلة. تنتشر الأجهزة الدقيقة في كافة التطبيقات الطبية التي ستتيح إجراء فحوصات داخلية وتشخيصات، وفي الوقت نفسه تتيح إمكانية إجراء تدخلات جراحية وطبية شديدة الدقة والتعقيد.

كما تؤدي الأجهزة الدقيقة أدوارًا في عمليات الإصلاح والصيانة في المدن الذكية، الأمر الذي يؤدي إلى تعزيز واستكمال الروبوتات المنتشرة في أعمال الصيانة. يتيح تنفيذ خوارزميات السرب المتطورة لهذه الأجهزة تنظيم نفسها ذاتيًا للقيام بمهام معقدة ومتطورة. وفجأة، يبدو أن هذه الآلات المتشابكة والمتداخلة منتشرة في كل مكان.

تفرض هذه الأجهزة تحديات أمنية جديدة نظرًا لمحدودية ميزانية الطاقة المتاحة لتأمين روابط الاتصالات الخاصة بها والقدرات المحدودة المتاحة للمعالجة. إن خوارزميات السرب الخاصة بالتحكم وإمكانية نشأة سلوكيات جديدة تثير تساؤلات جديدة بشأن التحقق من موثوقية هذه الأجهزة وتكاملها.

أثر المعرفة غير المحدودة

ماذا لو... وجدت الأسلحة أهدافها دائمًا بسهولة

الروبوتات | التواصل المفرط | الذكاء الاصطناعي

بحلول عام ٢٠٧١، ستتسم الأسلحة بالذكاء بل وقد تجد أهدافها في أي مكان وفي أي وقت، وقد يصل الأمر إلى العثور على شخص بعينه وسط الزحام وبسرعة تتجاوز غمضة العين. وتتنوع الأسلحة ما بين القذائف الأسرع من الصوت وطائرات الدرون المحلّقة في أسراب والأسلحة البيولوجية المُصنّعة بحسب متطلبات العملاء.

ستتضمن العديد من نظم الأسلحة إمكانيات ذكاء اصطناعي متطورة لعملية تشغيلها، سواء أكانت روبوتات أو إلكترونيات طيران أو إلكترونيات المركبات القتالية. وأصبح الأمن السيبراني للنظم العسكرية عنصرًا جوهريًا للأمن الوطني، في ظل استثمار القوات المسلحة أموالاً متزايدة في عمليات هندسة الدفاعات الأمنية السيبرانية، ومن أجل تطوير أساليب حربية سيبرانية وإلكترونية هجومية مُصممة لتعطيل الوسائل الدفاعية والنظم الهجومية للخصم.

تشهد الأنماط التقليدية للحروب تغييرات بصورة لا يمكن التعرّف عليها، وبالمثل الطرق التي تستعرض من خلالها الدول والأطراف الأخرى قوتها. هناك مصلحة وطنية ترتبط بتلك الدول (والجماعات الأخرى بخلاف الدول) التي يمكنها استعراض قدرتها على التطور بسرعة واقتناء تقنيات أسلحة جديدة، إلى جانب الجاهزية للتفكير بطرق غير تقليدية عن طريقة استخدام تلك التقنيات.

تؤدي «قرصنة» نظم الأسلحة العسكرية إلى حوادث خطيرة، حيث تؤدي الهجمات السيبرانية إلى مخاطر تصعيد حالات النزاع. وتسعى قوانين الصراعات المُسلّحة (والمعايير الدولية المرتبطة بها) إلى مواكبة تطور نظم الأسلحة.

ماذا لو... تتنبأ الآلات بجميع متطلباتنا

"لن يقتصر الأمر على عدم إمكانية تمييز الآلات عن البشر فحسب، بل قد تتمكن التقنيات من تغيير جوهر الحمض النووي وكيفية تصرّف البشر. وهنا تبدو التداعيات الاجتماعية والثقافية في هذه الحالة هائلة وعميقة."

كارولين ريفيت
شريك ورئيس قسم علوم الحياة السيبرانية على النطاق العالمي، كي بي إم جي المملكة المتحدة

التواصل المفرط

الذكاء الاصطناعي

تتناول المجموعة الرابعة من سيناريوهات «الاحتمالات المستقبلية» التفاعل بين البشر والآلات وكيفية تهيئة المشهد لتقارب محتمل بين الطرفين.

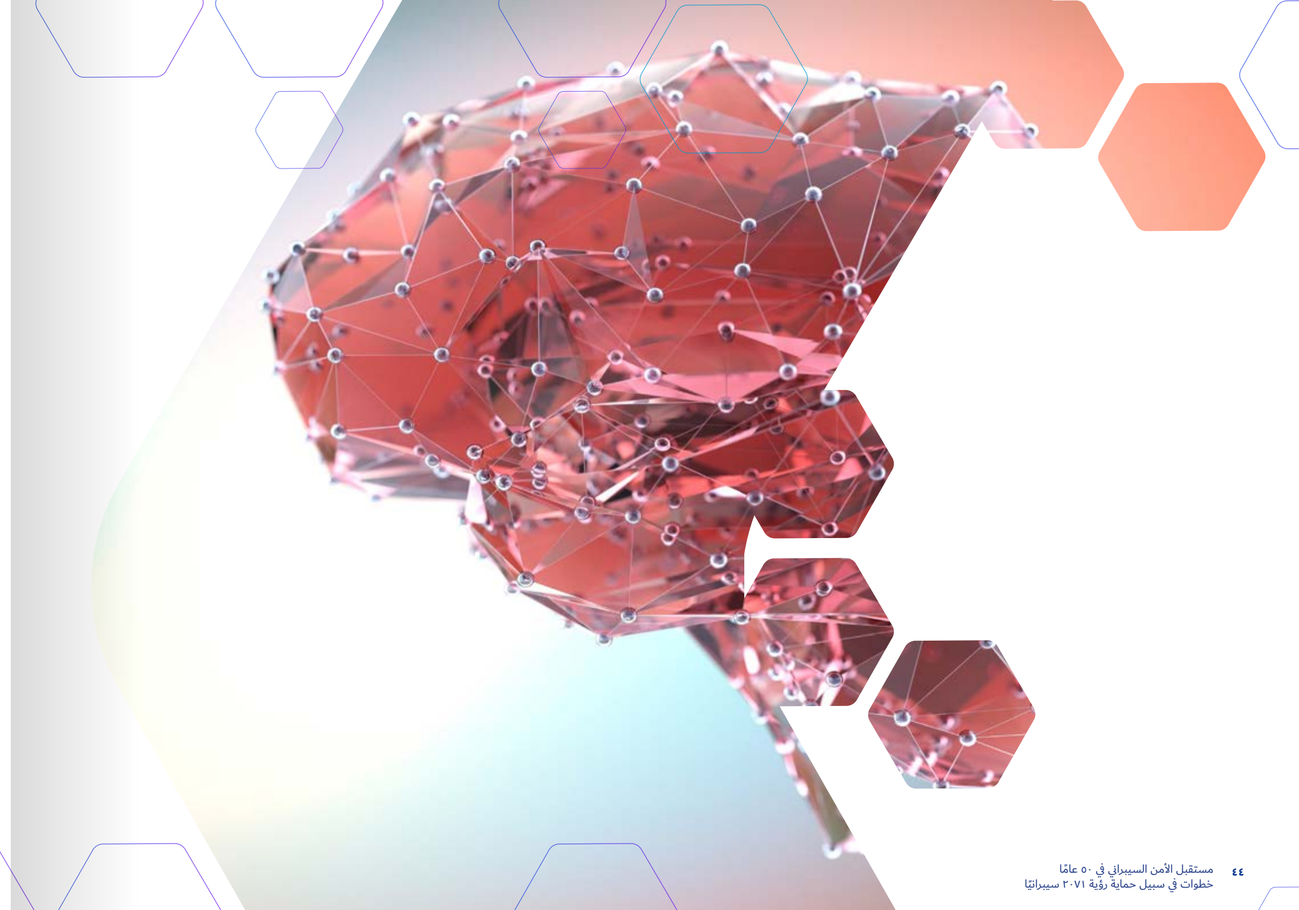
بحلول عام ٢٠٧١، قد يتوقع المساعدون الشخصيون جميع متطلباتنا والتأكد من تلبية تلك المتطلبات حتى قبل أن ندرك أننا بحاجة إليها. يتولى المساعدون الشخصيون الإشراف على تفاعلاتنا مع الإنترنت والعالم الافتراضي ومساعدتنا في الاستفادة القصوى من هذه العوالم وحمايتنا في تفاعلاتنا.

يرتبط المساعدون الشخصيون بحياتنا بصورة وثيقة. وينبغي إيجاد توازن بين المصالح التجارية للمزوّد الخاص بالمساعد واستقلالية ذلك المساعد في تلبية متطلباتنا. ستخضع هذه المساحة للتنظيم بصورة متزايدة في ظل تزايد المخاوف المجتمعية بشأن أوجه وأشكال التحيّز التي تبدو على هؤلاء المساعدين.

وستتطور أيضًا مخاوف الخصوصية بشأن قدر تلك البيانات التي يتولى هؤلاء المساعدون جمعها والاحتفاظ بها، إلى جانب أوجه التعقيد المقترنة بتحديد حجم التفويض الذي يمكن أن يظهره هؤلاء المساعدون خاصة عندما يتوقعون متطلباتنا المستقبلية.

ستجد الجريمة السيبرانية طرقًا للتلاعب بهؤلاء المساعدين بهدف الاستيلاء على البيانات الشخصية علاوة على الاحتيال على الأفراد الذين يدعمهم هؤلاء المساعدون. على الرغم من ذلك، سيؤدي هؤلاء المساعدون دورًا جوهريًا للحد من الجرائم ضد مالكيهم من خلال تنفيذ لوغاريتمات متطورة للحد من الاحتيال.

وبمرور الوقت، ننتقل من نموذج حماية النقاط النهائية ونظم الحاسب الآلي إلى نموذج حماية نمط الحياة ومصالح ذلك الفرد.



العالم الهجين الجديد

ماذا لو.. تمكنت الآلات من قراءة (أو كتابة) ما يجول بخاطرنا وعقولنا

الذكاء الاصطناعي

الهندسة الحيوية

بحلول عام ٢٠٧١ ستتطور قدرة الآلات على قراءة أفكارنا وذلك عن طريق الملاحظات الدقيقة لتعبيراتنا من خلال زراعة الشرائح والغرسات العصبية أو متابعة النشاط الدماغي، وقد استُخدِمَ تحفيز الدماغ، المُطور بالأساس لأغراض طبية، على نطاق أوسع للسعادة وبالنهاية السماح بالتفاعل المباشر فيما بين الآلات والأشخاص.

إلا أن المعايير المجتمعية المتعلقة بتلك التقنيات لا تزال ضعيفة. تشمل الأجهزة الطبية غرسات متطورة بناءً على التحفيز العصبي المباشر تعمل على منع التشوهات العصبية وتسمح بخوض تجارب حسية، فضلًا عن توفير واجهات حركية للأطراف الصناعية. علاوة على ذلك، انتشرت أيضًا الاستخدامات العسكرية لتلك التقنية مما أدى إلى رفع مستوى الأداء البشري والتفاعلات مع أجهزة الإنسان الآلي والهياكل الخارجية، وتولد عن تسويق تلك التقنية خلق سوقًا لتقنية التعزيز البشري، بالإضافة إلى استقطاب الدول لتطبيق تلك التقنية للتحكم في شعوبها بما في ذلك المستويات المتطرفة من السلوك الإجرامي وربما السيطرة أيضًا على وجهات النظر الأكثر مقتًا.

ولا غنى عن توفير الأمن السيبراني لتلك الغرسات نظرًا لقدرتها على التلاعب مباشرةً بالأشخاص، فضلًا عن إمكانية الوصول إلى العقل البشري والرؤى الإنسانية لأفكارنا ونوايانا الخاصة للغاية.

على الجانب الآخر، ستشق العصابات الإجرامية طريقها نحو استغلال عملية تحفيز الدماغ بوصفها مخدرًا جديدًا للشعوب مما يخلق أنماط جديدة من الإدمان وأنواع جديدة من الجرائم التقنية.

العالم الهجين الجديد

ماذا لو..
تمكنت الآلات من قراءة (أو كتابة) الحمض النووي البشري

الاتصال المتطور

الذكاء الاصطناعي

بحلول عام ٢٠٧١، ستتمكن الآلات من تتبع الحمض النووي وتحليله سريعًا، ومن ثَمّ تكتب حمض نووي جديد لتحويل تتبع الجينات خاصتنا أو تصنيع بروتينات وفقًا لما هو مطلوب. تساعد تقنية تسلسل الحمض النووي في تتبع ملايين القواعد، كما يعمل الربط الجيني على تعديل الحمض النووي الريبوزي / الحمض النووي البشري على نحوٍ انتقائي، فضلًا عن التطور السريع الذي تشهده تقنيات تخليق البروتين.

إلا أن إن معايير استخدام مثل تلك التقنيات واهية التطور، بينما لا تزال المناقشات المجتمعية حول إرساء المعايير المقبولة للسيطرة على التلاعب بشكل عام، ولكن من المتوقع أن يختبر الأثرياء والدول «المارقة» حدود تلك التقنيات، فها نحن على أعتاب حقبة لا تتسم بوجود أفراد بشرية مصممة فحسب، وإنما حقبة يسودها طفرة من التطورات الطبية التي ترمي إلى إطالة العمر وتأخير الشيخوخة. أخذت بيانات الحمض النووي في الانتشار وأضحت في كل مكان ويمكن الحصول عليها بسهولة مما أدى إلى استنباط معلومات حساسة للغاية حول الأمراض العامة ونمذجة الخصائص البيولوجية، الأمر الذي أدى إلى تزايد المخاوف المتعلقة بخصوصية تلك البيانات نظرا لاحتمالات استغلالها واستهداف الأفراد وحتى استخدامها في هندسة الأسلحة البيولوجية المصممة خصيصاً لتناسب الشريط الوراثي الخاص بهم.

يؤدي التلاعب بنُظم الهندسة الوراثية واستغلالها إلى خلق مخاطر جمة- بل وقد يؤدي إلى تصنيع أسلحة بيولوجية مصممة خصيصًا أو تعديلات مهلكة في العمليات/ النُظم الطبية.

ماذا لو .. أصبح الأشخاص والآلات شيئًا واحدًا

الروبوتات | الهندسة الحيوية | الذكاء الاصطناعي

”سيختلف العالم تمامًا إذا ما تراجعت عملية الشيخوخة أو انعكست، فمن سيحدد المدة التي سنعيشها، وما تأثير ذلك على العالم؟“

ناشيكتا أنجاده
الشريك المختص بشؤون الخدمات الاستشارية
المختصة بالمخاطر في شركة كي بي إم جي في جنوب أفريقيا

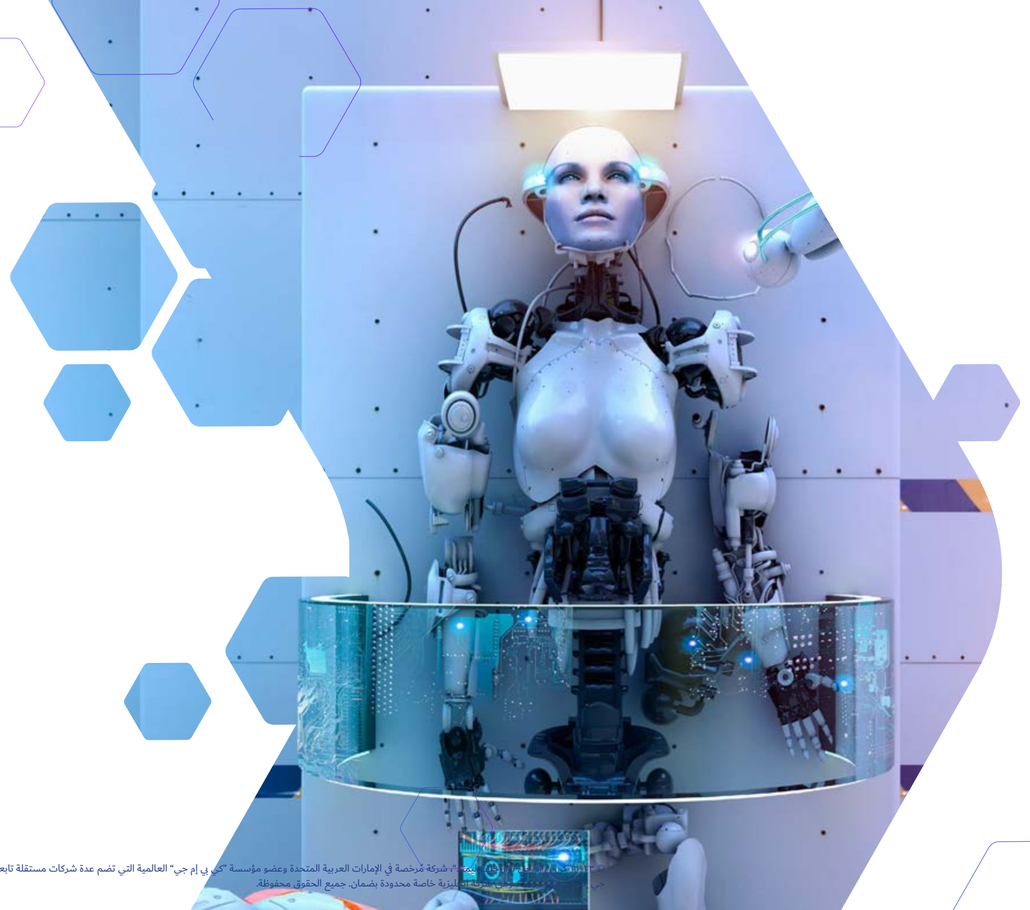
ربما تكون المجموعة التي نستعرضها أخيرًا من «الاحتمالات المستقبلية» هي الأكثر تحدياً حيث تتطلب منا التفكير فيما إذا كانت رؤيتنا للحياة نفسها ستظل كما هي دون تغيير حتى عام ٢٠٧١، أو سيختلف عالمنا تمامًا عما هو الآن.

بحلول عام ٢٠٧١، ستؤدي الطفرات التقنية في الأجهزة الطبية والغرسات العصبية إلى دمج أجهزة الكمبيوتر والبشر... لأغراض الموضة، والطب والحرب وقد حلت الأطراف الصناعية المتطورة محل الأطراف البشرية وعززتها بالفعل كما رفعت الغرسات العصبية القدرة على التعامل مع الأمراض العصبية ووفرت البصر للمكفوفين والصوت للصُم. ولم يستطع البعض مقاومة جاذبية تضمين المعالجات المساعدة في عقولهم ربما لم يكن لديهم خيارًا آخر. أما اتجاهات الموضة فهي تحتضن غرسات التقنية الآلية.

أصبحت حدود تقنية تعزيز الآلات محل نقاش مجتمعي حيث يتحول علاج المرض إلى تحسين الحالة المرضية مع تطور تقنيات زراعة الخلايا العصبية والأطراف الصناعية. وتسعى الجيوش إلى الحصول على ميزة قتالية وهي ميزة لا تسعى اليها إلا الجيوش التي تتوافر لديها موارد مالية لإقتناء مثل هذه القدرات. كما أن الأجهزة الطبية أصبحت أكثر تطورًا وأكثر تدخلا بشكل متزايد. ومع كل ما سبق تتزايد حالة الاعتماد والاتكالية أو حتى الإدمان.

ولا تزل المناقشات حول حدود تكنولوجيا تعزيز الآلات مستمرة، ولكن يبدو أن دفع بعض الدول (والشركات) بهذه الحدود إلى أبعد من ذلك أضحى أمرًا حتميًا ولكن في ظل تخلف القواعد التنظيمية. ومع عبور الأفراد (الخاضعين لتكنولوجيات التعزيز البشري) للحدود، فما هي الآثار المترتبة على تلك الحركات والهجرات؟

يشكل الأمن السيبراني للغرسات الآلية مصدر قلق متزايد حيث أصبحت هذه الأجهزة هدفًا للاستغلال، وأصبحت الخصوصية حقاً يتمثل في التحرر من التدخل غير المصرح به في حياة البشر في عالم تندمج فيه الآلات والبشر. ويترتب على اختراق الغرسات عواقب حقيقية متزايدة على الأرواح والرفاهية، وليس هناك خيار للبقاء خارج الشبكة عندما تعتمد الغرسات الطبية على المتابعة المستمرة.



إنها الحياة .. ولكن ليست كما عهدناها

قدرات فائقة وإمكانيات لا حدود لها في المستقبل

الروبوتات الهندسة الحيوية الذكاء الاصطناعي

بحلول عام ٢٠٧١، سيجد أغنى وأقوى الأفراد طرقًا لإطالة العمر سواء من خلال الاستنساخ أو من خلال التلاعب الجيني أو عن طريق نقل ذكرياتهم وشخصياتهم إلى الذكاء الاصطناعي أو أجهزة الإنسان الآلي.

تتجلى أسئلة أساسية حول ما يعنيه أن تكون إنسانًا وإلى أي مدى يمكن لكائن اصطناعي أو مستنسخ أن يجسد شخصية بحق وينتحل شخصية الشخص الحي. فبينما تسعى الأسر إلى الحفاظ على جوهر أحبائها للسماح بالتواصل بعد الموت، ويسعى الأفراد إلى نوع ما من الخلود، فسيأخذ الخط الفاصل بين الحياة والموت في التلاشي، مما يثير أسئلة جوهرية في القانون والدين.

بالطبع، ستكون هناك أسئلة حول مدى قدرة المستنسخات والصور التشخيصية على الاستمرار في التصرف نيابة عن الشخص المتوفى، وماذا يعني ذلك بالنسبة للميراث وحقوق الأحفاد من ذلك الفرد. من له الحق في صورة وشخصية الشخص المتوفى، أم أن هذه الحقوق ممنوحة للمستنسخ؟

إلا أن هناك مخاوف بشأن سلامة عملية النقل وكذلك الأمن السيبراني للنسخة أو الصورة التشخيصية نفسها، ومدى إمكانية التلاعب بها في شكلها الجديد. وإذا أصبح مثل هذا التحول مقبولا لدى المجتمع، فسيكون لذلك آثار جوهرية على بنية المجتمع نفسه واستقراره، مع تغير مفهوم الشيخوخة والموت.

مستقبل الأمن السيبراني نفسه

بالطبع من المتوقع أن يتطور الأمن السيبراني نفسه كنظام، وكذلك سوف تتطور تصرفات الدول والجريمة المنظمة في التخطيط للهجمات السيبرانية وتنفيذها. إضافة إلى ذلك، قد تكون هناك دول بدون جيوش عسكرية على الإطلاق حيث تصبح أجهزة الاستشعار والعقد الشبكية هي وسائل الدفاع الرئيسية بها، وتصبح كافة البنى التحتية ملكًا للشراكات بين القطاعين العام والخاص. وقد استخدمنا رؤية مماثلة لافتراض معطلات الحرب السيبرانية ومعطلات الأمن السيبراني:

"تُمثل السيطرة على المعلومات واحداً من أكبر مصادر القوة. وإذا أصبحت منظومة الإنترنت غير قابلة للاختراق، فمن المؤكد أن ذلك سيساعد في تقليل اعتمادنا على الأمن السيبراني."

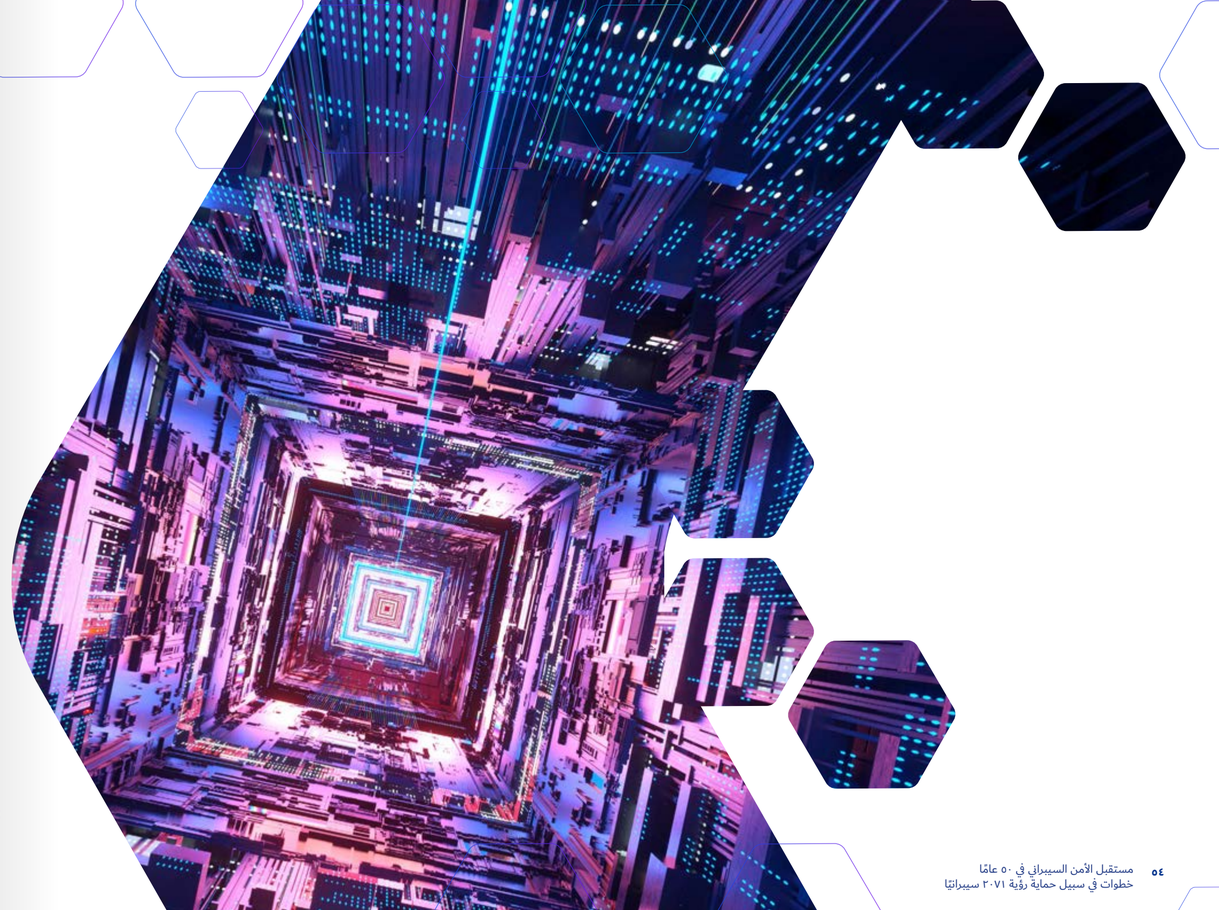
اللواء الدكتور مبارك سعيد بن غافان الجابري
الوكيل المساعد للإسناد والصناعات الدفاعية بوزارة الدفاع

"إيقاف الحرب السيبرانية بالأساليب التكنولوجية"

- لا مزيد من أجهزة الكمبيوتر
- يمكن تعريض أي أمة إلى الحرمان
- أصبحت الحرب السيبرانية واقعًا

مُعطلات الأمن السيبراني

- لا يثق أحد في تقنية الآخر
- لم يعد هناك أي أسرار بعد الآن
- يُحفظ الإنترنت بنظام حماية



مستقبل الأمن السيبراني نفسه

ماذا لو.. لم يعد هناك أسرار بعد الآن

الحوسبة الكمية

بحلول عام ٢٠٧١، ستؤدي التطورات التي يشهدها قطاع الحوسبة الكمية إلى تقويض أمن جميع خوارزميات التشفير لأولئك المسموح لهم بالوصول إلى أحدث التقنيات الكمية - ولكن ربما أدت التقنيات الكمية أيضًا إلى التلاعب بقنوات الاتصال الواضحة التي تسمح بالثقة الكاملة في خصوصية هذه الاتصالات. أضحى الحفاظ على ميزة التقنية الكمية مثابة ميزة للأمن القومي.

في هذا العالم الجديد، وبمرور الوقت جرى الكشف والإفصاح عن كثير من الأسرار بالنسبة لأولئك الأشخاص والمؤسسات التي تم جمع بياناتها، الأمر الذي أدى إلى أن تصبح الأسرار الدبلوماسية والتكنولوجية التاريخية معروفة، أما المؤسسات الأقل تطورًا فتجد نفسها تحت المراقبة، بل وتصبح حماية الملكية الفكرية والأبحاث الحساسة من الأمور الأكثر صعوبة، كما تكتشف البلدان طرقًا لإعادة ابتكار التقنيات بناءً على الأسرار المسروقة.

وبدلاً من ذلك، يمكن أن يكون الأشخاص أكثر ثقة في اكتشاف عمليات التنصت وقد يجدون طرقًا جديدة لحماية اتصالاتهم الأكثر حساسية للمضي قدمًا باستخدام توزيع المفتاح الكمي والتشابك الكمي.

وفي كلتي الحالتين، تصبح التقنيات الكمية مصدراً للميزة التنافسية الوطنية، وينقسم العالم إلى مالكي تلك التقنيات وغير مالكيها.

”في ظل التطور التكنولوجي المستمر، وتأثيره على استشراف الاحتمالات المستقبلية المتوقعة للأمن السيبراني، أصبح حتام علينا تسليح وتمكين أجيالنا القادمة بالمهارات والمعرفة اللازمة لتسخير الفرص ومواجهة أي تبعات قد يحملها المستقبل.“

سعادة. نور علي النومان
مدير دائرة الحكومة الإلكترونية

ماذا لو... لم يثق أحد في تقنية الآخر

الاتصال المتطور

الأحداث الهدّامة

بحلول عام ٢٠٧١، لن تضع أي دولة ثقتها في التكنولوجيا ما لم يتم إنتاجها من قبل أحد الحلفاء أو إذا كان لديها رؤية واضحة مستهدفة من عمليات الإنتاج. وكانت هناك حالات كثيرة جدًا من المهام الوظيفية الخفية ولأصبحت سلاسل توريد التكنولوجيا أكثر شفافية مع زيادة التركيز على التحقق من سلامة تلك السلاسل، فضلًا عن استعانة الدول بالعمليات الأولية لإنتاج المكونات الرئيسية.

لقد أصبح العالم أكثر استقطابًا مع تزايد حدة الانقسامات القائمة بين كتل القوى، مما أدى إلى التشكيك في المكونات والأنظمة المتحصل عليها من خارج الحدود الوطنية، والتي يغذيها الاستخدام المتزايد لتقنيات الهجوم على سلسلة التوريد من قبل مجموعات الجريمة المنظمة التابعة للدول أو التي تعمل بالإنابة، مما أدى إلى نقل أنشطة إنتاج التكنولوجيا الرئيسية.

لقد أتاحت تطورات التصنيع الذكي إمكانية التصنيع بالقرب من الوجهة المقصودة، على الرغم من ضرورة توفير مستويات عالية من الأمان حول كل من عمليات التصنيع وحماية الملكية الفكرية الحساسة.

تكتسب النماذج الأمنية القوية في مواجهة مكونات الأجهزة والبرامج غير الموثوق بها قدرًا أكبر من الاهتمام، إلى جانب التحسينات المستمرة في مراقبة سلوك النُظم المختلفة المرتبطة باستغلال المكونات غير الموثوق بها.

استمرت التوترات بين الأسواق المفتوحة التي تطبق الحد الأدنى من الحواجز أمام حركة السلع والخدمات، والتداعيات الأمنية الوطنية الناجمة عن الاعتماد على الأنظمة المقدمة من الخارج في النمو في ظل غياب إجماع دولي على النهج المشترك.

ماذا لو ... كان للإنترنت نظام حماية

الاتصال المتطور

الأحداث الهدّامة

بحلول عام ٢٠٧١، لكان الإنترنت قد طور نظام حماية ضد العديد من الهجمات السيبرانية، قادر على إعادة الهيكلة والتكيف مع الهجمات، لمواجهة المهاجمين والرد عليهم، ولكان الإنترنت نظامًا أكثر مرونة من الأنظمة التي تعكس أهميته للمجتمع الحديث.

لا يوجد إجماع كبير حول هوية المتحكم في «الإنترنت» حيث تتخذ الدول أساليب مختلفة لممارسة السيادة على تلك الشبكة والدفاع عن أجزائها في الشبكة العالمية. وأصبحت العديد من أجزاء الإنترنت الآن قادرة على مواجهة الأنشطة الضارة بسرعة، والرد خلال أجزاء من الثانية. وفي بعض الأحيان تتفاعل أجهزة الإنسان الآلي المهاجمة بنفس السرعة، في حين يتراوح زمن الاستجابات من الحظر الوقائي إلى الهجمات المضادة الآلية التي تهدف إلى تدمير تلك الأنظمة بشكل دائم.

وتعمل خوارزميات مماثلة على اكتشاف «المعلومات الخاطئة» ومواجهتها ومراقبة مساحة المعلومات، ويكون الإنترنت نفسه أكثر مرونة وقدرة على الإصلاح الذاتي، وإعادة التشكيل للتعامل مع أعطال النظام وانقطاع التيار.

إن وضع معايير دولية بشأن التدابير المضادة المقبولة أمر بعيد المنال - كما هو الحال بالنسبة لوضوح حقوق الدولة أو الشركة أو الأفراد في اتخاذ مثل هذه الإجراءات. ويهدف البعض إلى استغلال استجابات الشبكة (وأجهزة الذكاء الاصطناعي المسيطرة عليها) لتحقيق أهدافهم الخاصة - مما يؤدي إلى خلق استجابة مناعية ذاتية بشكل فعال.

”تمكنت قوة التعلم الآلي من تطوير أنظمة مستقلة تعمل إلى حد كبير مثل الإنسان، وتوظف شبكاتها للتعلم وصد الهجمات، والتغلب على التحديات.“

سعادة المهندس محمد إبراهيم الزرعوني
نائب مدير عام الهيئة لقطاع المعلومات والحكومة الرقمية

ماذا لو... تمكنت أي أمة من الانعزال

الاتصال المتطور

الأحداث الهدّامة

بحلول عام ٢٠٧١، يمكن عزل أي دولة من الفضاء الإلكتروني - سواء عن طريق الهجوم السيبراني، أو عن طريق قطع الكابلات البحرية أو التشويش على اتصالات الأقمار الصناعية. على الرغم من أن الاتصالات أصبحت أكثر مرونة وتنوعًا، وأقل عرضة للفشل في نقطة واحدة، إلا أننا أصبحنا نعتمد بشكل متزايد على الروابط ذات النطاق الترددي العالي والفواصل الزمنية المنخفضة.

لقد طورت الدول مجموعة من التقنيات الهجومية السيبرانية (والهجومية التقليدية) التي تهدف إلى تعطيل البنية التحتية للبلدان الأخرى. واستجابةً لذلك، اتخذت الدول أيضًا خطوات لتنويع وصولها باستخدام مزيج من البنية التحتية للاتصالات الفضائية والأرضية، مع زيادة قدرتها على الصمود في مواجهة هجمات الإنترنت على نطاق أوسع. وقد اختارت بعض الدول عزل نفسها عن المجتمع العالمي لأغراض منها على سبيل المثال التحكم في تدفق المعلومات (والمعلومات المضادة) إلى دولها، فضلا عن ضمان قدرتها على الصمود في مواجهة الإجراءات التي تتخذها الدول الأخرى لمعاقبتها أو عزلها.

لا يزل التفاعل بين الجغرافيا الطبيعية والاتصال بالإنترنت معقدًا، مع بقاء نقاط الاختناق الطبيعية في البنية التحتية التي تدعم عالمنا الرقمي، حيث أصبحت حماية نقاط الاختناق هذه استراتيجية تتبعها العديد من الدول.

"قدرات الذكاء الاصطناعي تمكن الدول من حماية مساحتهم على الإنترنت، فالجرائم الإلكترونية لا تعرف حدودا دولية. "

سعادة المهندس / خالد الشامسي
مدير عام دائرة أم القيوين الذكية

ماذا لو... أصبحت الحروب السيبرانية واقعًا

الاتصال المتطور

الأحداث الهدّامة

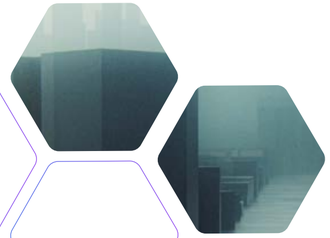
بحلول عام ٢٠٧١، ستصبح الحرب السيبرانية شائعة مع بناء الدول قدراتها الهجومية، وسيكون للهجمات السيبرانية عواقب حقيقية وخيمة على البنى التحتية وحياة البشر. لقد استثمرت كل دولة (وبعض الشركات والجماعات الإرهابية) لتطوير القدرات السيبرانية الهجومية بالإضافة إلى استكشاف تكاملها مع القدرات العسكرية التقليدية الأخرى.

على الرغم من عدم إتفاق الدول حتى الآن على تعريف محدد للحرب السيبرانية ومعايير السلوك الدولي فيما يتعلق بمثل هذه «الصراعات»، فإن تأثير الهجوم السيبراني الهجومي أصبح مسألة حقيقية الى حد كبير، حيث طورت المجموعات طرقًا للتلاعب بمساحة المعلومات الخاصة بالأهداف لتحقيق الاستفادة منها، فضلاً عن إضعاف الأنظمة المادية السيبرانية والتلاعب بها. فمنذ زمن بعيد، تلاشى الخط الفاصل بين السلام والحرب، إن كان هذا الخط موجوداً بالأساس. وستتمكن الدول من الانتقال من الحرب إلى حالة السلام أو العكس بين عشية وضحاها بفضل نموذج التدمير المؤكد المتبادل القائم على الردع السيبراني.

وتكافح الأمم لتحديد معايير التصعيد ووضع إطار للردود المناسبة على الأعمال الهجومية، حيث أصبح استخدام الهجوم السيبراني الهجومي أمرًا طبيعيًا. تلعب أنظمة الذكاء الاصطناعي دورًا رئيسيًا في تنسيق الأعمال الهجومية على نطاق واسع وفي رد مثل هذه الهجمات.

يتم التركيز بشكل أكبر على تصميم أنظمة تصمد أمام الهجمات وضمان قدرة الأنظمة على استرداد عافيتها بأمان تحت الهجوم. وقد أصبح الأمن السيبراني مرادفا للأمن القومي، حيث تسعى الدول جاهدة إلى تكييف المفاهيم التقليدية للقوة والدفاع في ظل بيئة مختلفة تمامًا.

تستمر وتيرة الهجوم والرد في التزايد، مما لا يترك سوى القليل من الوقت لتهدئة الموقف الذي قد تكون عواقبه أبعد من الفضاء الإلكتروني.



ماذا لو..
لم تعد أجهزة الكمبيوتر موجودة يومًا ما

الاتصال المفرط

حدث تخريبي

بحلول عام ٢٠٧١، تعمل النبضة الكهرومغناطيسية (النبضات الكهرومغناطيسية النووية أو قذف المادة الإكليلية الشمسية) على تعطيل وتدمير الكثير من البنية التحتية لتكنولوجيا المعلومات التي أصبحنا نعتمد عليها، وفجأة لا يوجد أجهزة كمبيوتر في العالم. لقد أصبح عالمنا الرقمي مترابطًا بشكل مفرط ومن المحتمل أن يكون هشًا بسبب الأحداث ذات الاحتمالية المنخفضة ولكن ذات التأثير الكبير.

يستمر الانتشار النووي مع وجود العديد من البلدان التي لديها القدرة على إطلاق أنظمة إيصال باليستية قادرة على بدء انفجار نووي خارج الغلاف الجوي والتسبب في نبض كهرومغناطيسي كبير. ولا تزال المخاوف بشأن احتمال وقوع حدث كارينغتون مثل العاصفة المغناطيسية التي أثرت على الأرض في عام ١٨٥٩ قائمة.

وأي من الحدثين من شأنه أن يكون مدمرًا للغاية لعالمنا الرقمي، وخاصة لأنظمتنا الفضائية الحيوية.

تكافح الدول من أجل تهيئة الظروف للاستثمار في البنية التحتية المرنة القادرة على النجاة من مثل هذه الأحداث، على الرغم من أن البعض يختار القيام بهذا الاستثمار لحماية وظائف الأمن القومي والدفاع الأكثر حساسية، على الرغم من أن تعطيل الإنترنت الأوسع سيظل يخلق تأثيرات هائلة على المجتمع.

هل سنرى وقوع مثل هذا الحدث؟ وماذا سيكون ردنا بعد مثل هذا الحدث؟ هل نبني عالمًا مختلفًا.. وهل يقوم على الكربون أم السيليكون؟

الامن السيبراني العالمي لعام ٢٠٧١

”إن التعايش مع الآلات كأحد أشكال الحياة الأخرى التي يجب أن نتعاون معها، يؤدي بطبيعة الحال إلى وضع سياسات وتحديد الحقوق والمخالفات التي تتعلق بطريقة تعاملنا مع الآلات وكيفية تعاملها معنا “

سعادة عهود علي شهيل
مدير عام حكومة عجمان الرقمية

لقد وضعنا العديد من سيناريوهات ”الاحتمالات المستقبلية“، حيث يثير كل منها مجموعته الخاصة من مشكلات الأمن السيبراني والخصوصية والتنفيذ. وعلى الرغم من عدم إمكانيتنا من التنبؤ على الإطلاق بما ستكون عليه الحياة عام ٢٠٧١، فإنه يمكننا الشروع في أن نتصور أنماطاً من التحديات المحتملة.

يمكننا أن نتوقع تطوير موضوعات حول تعزيز الواقع، وتطوير الذكاء الاصطناعي، والتقارب بين الإنسان والآلة، وربما حتى إمكانية أن يحل أطفالنا السيليكون محل الحياة البشرية.

توفر التكنولوجيا إمكانات كبيرة لمعالجة بعض التحديات التي تواجهها البشرية حاليًا، وتمكين التنمية الاقتصادية، والمساعدة في معالجة التحديات الصحية وشيخوخة مجتمعنا، وحتى إطالة الحياة في نهاية المطاف.

وبطبيعة الحال، ستلعب القضايا السياسية دورًا في هذه البيئة المعقدة، ويمكننا أن نتوقع من الدول أن تسعى إلى الحصول على ميزة تنافسية في تبني التكنولوجيا وتسخيرها للأغراض العسكرية والأمن القومي، وفي عالم يبدو أن التوترات الجيوسياسية آخذة في الارتفاع – فنحن في خطر الحرب السيبرانية أيضا.

سيكون عالمنا شديد الاتصال والممكّن من التكنولوجيا أيضًا عرضة للاضطراب سواء بسبب الأحداث المتطرفة التي من صنع الإنسان أو الأحداث الطبيعية (مثل النبضات الكهرومغناطيسية) أو الحرب السيبرانية.

من الواضح أن الأمن السيبراني سيظل يشكل تحديًا في أي عالم جديد يمكننا تصوره، ولكن ما هي التداعيات الرئيسية لهذا العالم الجديد؟

بناء "الثقة" في نسيج مجتمعنا

A

"لا ينبغي لنا أن نفترض أن أي شيئًا موجودًا اليوم سيكون كما هو بعد ٥٠ عامًا. إن كيفية تسخير الحقيقة وتشويهها مسألة بالغة الأهمية. من الممكن جدًا أن نخلق واقعًا غير صحيح."

روني ميشيل
شريك في شركة كي بي إم جي في إسرائيل

ستصبح الثقة موضوعًا رئيسيًا في المستقبل. في عالم تطمس فيه الحقيقة والخيال، ستصبح معرفة من أو ما الذي يمكن الوثوق به أكثر أهمية من أي وقت مضى. وسوف تصبح أطر الثقة الرقمية، مثل عمل المنتدى الاقتصادي العالمي، جزءا متزايد الأهمية من حوكمة الشركات بما في ذلك آليات الشفافية المناسبة.

سوف تتوصل المجتمعات إلى تسويات سياسية مختلفة للغاية حول مدى قدرة الدولة (أو التجارة في الواقع) على تشكيل والسيطرة على السرد المقدم لشعبها. وفي عالمنا العالمي المترابط، سوف تتعارض وجهات النظر العالمية هذه، وستصبح المعايير الدولية ذات أهمية متزايدة، ولكنها أيضًا بعيدة المنال. وفي حين أنه من الممكن التوصل إلى توافق في الآراء حول الأشكال الأكثر تطرفًا من التزييف والخداع والنشاط الإجرامي، إلا أن هذا لن يمتد إلى محتوى اجتماعي أو ديني أو سياسي أكثر دقة. بالإضافة إلى ذلك، ستحتاج أطر الثقة إلى أن تظل مرنة مع السرعة التي يمكن بها معالجة المعلومات من خلال انتشار الذكاء الاصطناعي والقوة الحاسوبية.

تلبي قوانين الجرائم الإلكترونية الحالية في دولة الإمارات العربية المتحدة الاستخدام الاحتيالي للوسائل الرقمية وتركز بقوة على الأمن الوطني ومكافحة نشر المحتوى الإجرامي أو التشهيري أو الضار. ستحتاج الأطر القانونية إلى مزيد من التطور للتعامل مع الأشكال الجديدة من التلاعب بالمعلومات، على سبيل المثال التزييف العميق للتلاعب بالخطاب السياسي، مما يتطلب نهجًا قائمًا على المبادئ يركز على النية بدلًا من الآلية. ستحتاج الأطر القانونية إلى معالجة المشهد الرقمي المتطور باستمرار من أجل استمرار أهميتها وتضمين آليات للتنقل بسرعة التقدم التكنولوجي.

[انقر هنا للعودة الى **نقاط إجراءات التنفيذ**]

الأطر القانونية لعالم جديد من الأشخاص الهجينين والذكاء الاصطناعي والتكنولوجيا

B

"إن التعايش مع الآلات كشكل آخر من أشكال الحياة التي يجب أن نتعاون معها، في شكل شراكة، يؤدي بطبيعة الحال إلى سياسات وحقوق وانتهاكات فيما يتعلق بكيفية تعاملك مع الآلات وكيفية تعاملها معنا."

كارولين ريفيت
شريك ورئيس قسم علوم الحياة السيبرانية على النطاق العالمي، كي بي إم جي المملكة المتحدة

سيؤدي التطور السريع لتكنولوجيا الذكاء الاصطناعي إلى طرح أسئلة رئيسية حول الشخصية القانونية لأنظمة الذكاء الاصطناعي، وقدرتها على ممارسة الوكالة نيابة عن الشركات والأفراد، وحول مسؤولية الشركة المصنعة للذكاء الاصطناعي عن سلوكياتها وأفعالها، وفي النهاية حول إطار العمل. الضوابط التي ستحكم وتحد من حرية عمل أنظمة الذكاء الاصطناعي هذه.

في حين أنه سيكون من المغري صياغة أطر قانونية خاصة بأنظمة الذكاء الاصطناعي، إلا أنها ستواجه تحديات متزايدة عندما يبدأ الناس وأنظمة الذكاء الاصطناعي في التقارب. وفي نهاية المطاف سوف تكون هناك حاجة إلى إطار قانوني لا أدري ما إذا كان الكيان المعني شخصًا أم ذكاءً اصطناعيًا أم مزيجًا من الاثنين معًا.

سيتم توسيع البنى القانونية التقليدية مثل السرقة أو الاعتداء أو حتى القتل لتطبق على العالم الافتراضي. ومن خلال القيام بذلك، ستكون هناك مناقشات مجتمعية كبرى حول كيف أن الصدمة العاطفية في هذا العالم الافتراضي تعادل الاعتداء في العالم الحقيقي، وكذلك حماية الملكية الفكرية والأصول في هذا العالم الافتراضي.

وسوف تحتاج التجارة العالمية إلى التنقل بين هذه الأطر التنظيمية والقانونية المختلفة حتى تظل فعّالة، ومن المرجح أن تجد الاختلافات بين هذه الأطر أكثر صعوبة في التوفيق بينها. ربما تحتاج الشركات إلى كبير مسؤولي الفلسفة الآن.

[انقر هنا للعودة الى **نقاط إجراءات التنفيذ**]

نماذج أمنية جديدة

C

”إذا تجاوزت دوافع مجرمي الإنترنت أنشطة استخراج الأموال إلى التلاعب أو حتى السيطرة على حياة الناس، فهل سنحتاج بعد ذلك إلى الكشف والاستجابة المُدارة للجسم (MDR)؟ “

جيمس مابوت
شريك في فيوتشرز كي بي إم جي،
كي بي إم جي استراليا

سوف تبدو النماذج الأمنية قديمة على نحو متزايد، مع التركيز على حماية سرية البيانات وسلامتها وتوافرها. سنهدف إلى بناء نماذج جديدة توفر مستوى أعلى من التجريد للتفاعلات المسموح بها بين الكيانات - سواء الأشخاص أو أنظمة الذكاء الاصطناعي.

تخيل واقعًا افتراضيًا تتفاعل فيه الصورة الرمزية الخاصة بك مع المحتوى المقدم من الآخرين. ما الذي يمكنهم معرفته عنك وبأي قدر من التفاصيل، وما مقدار سلوكك الذي يمكنهم وصفه، وكيف يمكنهم التفاعل معك، وما الذي قد تجده غير مقبول ومهينًا في سلوكياتهم؟ أثناء قيامهم بجمع البيانات عنك، كيف يمكنك التحكم في الاستخدامات التي توضع فيها تلك البيانات، كيف يمكن مكافأتك على استغلالها واستخدامها، هل يمكنك طلب إبطالها أو تعديلها أو تصحيحها في الوقت الفعلي؟

سينتقل مفهومنا للخصوصية إلى ما هو أبعد من التحكم في جمع ومعالجة المعلومات الخاصة بنا، نحو مفهوم أوسع لإدارة التطفل على حياتنا والتحكم في كيفية حدوث تلك التفاعلات. كل ذلك يتضمن طريقة أكثر تطورًا لإنشاء تفاعلات مسموح بها بينك وبين الكيانات الأخرى، ولكن أيضًا مراقبة ما إذا كانت هذه الحدود قد تم انتهاكها أو خرقها. كيف سيتم التحكم في الوصول عندما تكون عمليات الوصول التي نناقشها موجهة إلى أفكارنا وعواطفنا وكل سلوكياتنا؟

[انقر هنا للعودة الى **نقاط إجراءات التنفيذ**]

التركيز على الإشراف على أنظمة الذكاء الاصطناعي المستقلة

D

وستكون هناك حاجة أيضًا إلى أطر ترخيص جديدة للأنظمة المستقلة، سواء كانت أنظمة الذكاء الاصطناعي العاملة في الفضاء السيبراني أو المظاهر الآلية لأنظمة الذكاء الاصطناعي هذه في العالم الحقيقي. يمكننا أن نتوقع فرض التزامات أكبر على الشركات المصنعة لتحمل المسؤولية (والمسؤولية) عن سلوك مثل هذه الأنظمة. سيؤدي ذلك إلى زيادة التركيز على تصميم مثل هذه الأنظمة، وكذلك إنشاء أنظمة محددة للإشراف على سلوك الذكاء الاصطناعي واستخلاص الدروس من مجتمع السلامة في استخدامهم لأنظمة أدوات السلامة. وسوف ينمو تعقيد هذه المحددات مع تطور المعضلات الأخلاقية حول استخدام الذكاء الاصطناعي.

يمكننا أن نتوقع أن يكون النظام القانوني منشغلًا لبعض الوقت في محاولة حل هذه المشكلات وإنشاء سوابق قضائية يمكنها التعامل مع التعقيد المتزايد لعمل الأنظمة المستقلة واعتمادنا الأكبر على مثل هذه الأنظمة. وسوف تتباين الدول في قراراتها بشأن هذه القضايا، مما يزيد من التعقيدات أمام التجارة العالمية وإنشاء المعايير الدولية.

[انقر هنا للعودة الى **نقاط إجراءات التنفيذ**]

التعاون بين المنظمين والتقنيين

E

”سيتحقق النجاح للجهات التنظيمية للتكنولوجيا التي تتمتع بأكبر درجة من الاستنارة، مما يوفر منظومة يمكن أن يزدهر فيها الابتكار لصالح البشرية“

سعادة محمد حيي الكعبي
المدير العام لهيئة أبوظبي الرقمية بالإنابة

هناك حاجة إلى هذا التطور المشترك حتى نتمكن من تقييم التأثير المجتمعي المحتمل للتكنولوجيات، والحفاظ على تحديث تقييم التأثير عندما تجد التكنولوجيا تطبيقات جديدة، وغير متوقعة في كثير من الأحيان.

هناك ميزة في إنشاء نماذج لمثل هذه المشاركة التنظيمية، بناءً على تجارب العديد من الدول مثل سنغافورة والمملكة المتحدة في تصميم البيئة التجريبية التنظيمية التي تعزز هذا الحوار وتسمح بالاختبار العملي وتجريب التقنيات.

وستساعد بيئات الحماية التنظيمية هناك أيضًا في كشف القضايا التي قد تكون هناك مناقشات مجتمعية أكثر جوهرية في وقت مبكر، بالإضافة إلى مساعدة الدول على صياغة استجابتها لاعتماد التقنيات الجديدة. وسوف تحتاج القواعد التنظيمية أيضًا إلى المرونة والتطور جنبًا إلى جنب مع التكنولوجيات، وهناك فائدة في النظر في النظرة الطويلة الأمد عند صياغة مثل هذه القواعد التنظيمية.

وأخيرًا، تسمح لنا المشاركة المبكرة أيضًا بتوقع الحاجة إلى تطوير التكنولوجيا الإشرافية (Suptech) والتكنولوجيا التنظيمية (Regtech) والتي يمكن أن تساعد في الإشراف على تطبيق التقنيات الجديدة وتوفير الثقة في تطبيقها الآمن.

[انقر هنا للعودة الى **نقاط إجراءات التنفيذ**]

الدفاع الاستباقي باستخدام التكنولوجيا الناشئة

F

” دولة الإمارات بتقدمها الواضح وخطاها المتسارعة في مجال الأمن السيبراني، تصنع مشهداً رقمياً مميزاً للدولة وتمكن التقدم الآمن في العقود القادمة تماشياً مع أهداف مئوية الإمارات 2071 “

معالي عمر سلطان العلماء
وزير دولة للذكاء الاصطناعي والاقتصاد الرقمي وتطبيقات العمل عن بُعد

نظرًا لأن أدوات الهجوم السيبراني أصبحت آلية ومتطورة بشكل متزايد، بما في ذلك تسخير تقنيات الذكاء الاصطناعي لتخطيط وتنفيذ كل من الاستطلاع والاختراق الفعلي واستغلال الأنظمة؛ وسيقابل ذلك زيادة في استخدام تحليلات البيانات المتطورة داخل مجتمع الأمن السيبراني لاكتشاف الهجمات السيبرانية ومواجهتها بسرعة. سيؤدي ذلك إلى توسيع نماذج الدفاع النشطة الحالية التي تطورها الدول لمنع الهجمات السيبرانية لتشمل مؤسسات وقطاعات وإجراءات مضادة وطنية أكثر نشاطًا وحتى تدابير انتقامية آلية.

ستصبح العمليات السيبرانية تلقائية بشكل متزايد لتشكل شراكة بين متخصصي الأمن وأدوات الذكاء الاصطناعي وأنظمة اتخاذ القرار التي تدعمهم. سوف تمتد أنظمة الدفاع السيبراني لتشمل ليس فقط التسوية الفنية للأنظمة، ولكن أيضًا مواجهة التلاعب الأكثر تعقيدًا بأنظمة الذكاء الاصطناعي (الذكاء الاصطناعي الخصمي) وكذلك مساحة المعلومات في العالمين الحقيقي والافتراضي.

سيتم تطوير نماذج دفاعية جديدة «على مستوى النظام» والتي توفر إطارًا لدمج البيانات معًا عبر المجتمع، كما تمكّن نماذج الدفاع «الجهاز المناعي» الموزعة التي تعمل فيها التدابير المضادة وأنظمة الاستجابة المتعددة بطريقة منسقة لمواجهة و تعطيل الهجمات. وهذا من شأنه أن يثير أسئلة جوهرية حول السيطرة على الإنترنت (والعوالم الافتراضية الأحدث)، والطرق التي تسعى بها الدول إلى تخفيف وتقييد الوصول إلى العنصر «الخاص بها» في هذه البيئات.

ما الذي يهم مجتمعنا حقًا؟

في هذا العالم الجديد، يمكن لهياكل السلطة أن تجد طرقًا عديدة لفرض إرادتها على الناس، وستكون الخيارات التي تتخذها المجتمعات وحكوماتها بشأن الحريات والسلوكيات المقبولة بمثابة تمييز رئيسي بين الأمم. ستتخذ الدول مسارات مختلفة تمامًا وستكون هناك توترات متزايدة عندما تلتقي هذه النماذج المجتمعية المختلفة في الفضاء الإلكتروني - قد يكون الإجماع الدولي وهميًا وستدخل القوة الاقتصادية حيز التنفيذ عندما تسعى الدول إلى تحقيق ميزة تكنولوجية وبالتالي فرض نظرتها العالمية على الآخرين.

سوف يستمر مفهوم الدول القومية في التحول والتطور - كما سيعتمد التوازن بين قوة الشركات على التجارة والتبادل التجاري، وقوة الدولة على أساس السيطرة الجغرافية، وقوة المجموعات الأخرى على أساس الأيديولوجية.

وفي عالم التغيير هذا، توجد فرص للدول التي يمكنها خلق بيئات يتطور فيها الابتكار والسلطة التشريعية مع رؤية واضحة للمستقبل. يمكننا أن نختار إنشاء عالم رقمي مفتوح وحر وشفاف. إن خياراتنا ستقود أنماط الاستثمار وكذلك هجرة العمالة الماهرة سواء كانت بشرية أو هجينة أو آلية.

[انقر هنا للعودة الى **نقاط إجراءات التنفيذ**]

ضمان تحقيق رؤية الإمارات

حددت دولة الإمارات العربية المتحدة المبادئ التي ستبني عليها قبل عامها المئوي في عام ٢٠٧١. وترسم هذه المبادئ خارطة الطريق الاستراتيجية لعصر جديد من النمو الاقتصادي والسياسي والاجتماعي في دولة الإمارات العربية المتحدة - من تعزيز الاتحاد والمؤسسات إلى وضع التكنولوجيا الرقمية والتقنية والتنمية العلمية في قلب تنميتها الاقتصادية.

وستكون بمثابة مبادئ توجيهية لجميع المؤسسات في دولة الإمارات العربية المتحدة مع اقتراب الدولة من مرحلة جديدة من التطور على مدى العقود الخمسة المقبلة. إنهم جزء من حملة «مشاريع الخمسين»، وهم كذلك على النحو التالي.

٧٦ مستقبل الأمن السيبراني في ٥٠ عامًا
خطوات في سبيل حماية رؤية ٢٠٧١ سيبرانيًا

مبادئ الخمسين

١- تدعيم الاتحاد:

سيظل التركيز الوطني الرئيسي هو تعزيز الاتحاد ومؤسساته وسلطته التشريعية وقدراته وموارده المالية.

٢ - أفضل نظام اقتصادي:

سنسعى جاهدين خلال الفترة المقبلة لبناء الاقتصاد الأفضل والأكثر ديناميكية في العالم.

٣ - سياسة خارجية حكيمة:

إن السياسة الخارجية لدولة الإمارات هي أداة تهدف إلى خدمة أهدافنا الوطنية العليا وأهمها المصالح الاقتصادية للإمارات.

٤ - رأس المال البشري:

المحرك الرئيسي للنمو في المستقبل هو رأس المال البشري. إن تطوير النظام التعليمي، وتوظيف المواهب، والاحتفاظ بالمتخصصين، وبناء المهارات بشكل مستمر.

٥ - علاقات الجوار:

حسن الجوار هو أساس الاستقرار. إن الموقع الجغرافي والاجتماعي والثقافي للدولة في منطقتها هو خط الدفاع الأول عن أمنها وسلامتها وتطورها المستقبلي.

٦ - مركز التميز والامتياز:

ترسيخ سمعة الإمارات عالميًا مهمة وطنية لجميع المؤسسات. الإمارات وجهة واحدة للأعمال والسياحة والصناعة والاستثمار والتميز الثقافي.

٧ - تبني الابتكارات:

إن التفوق الرقمي والتقني والعلمي لدولة الإمارات سيحدد حدودها التنموية والاقتصادية.

٨ - منظومة القيم:

تبقى منظومة القيم الأساسية في دولة الإمارات قائمة على الانفتاح والتسامح، وحفظ الحقوق، وسيادة العدالة والقانون.

٩ - المساعدات الإنسانية:

تشكل المساعدات الإنسانية الخارجية التي تقدمها دولة الإمارات جزءًا أساسيًا من رؤيتها وواجبها الأخلاقي تجاه الشعوب الأقل حظًا.

١٠- السلام والاستقرار:

إن الدعوة إلى السلام والوئام والمفاوضات والحوار لحل كافة الخلافات هي أساس السياسة الخارجية لدولة الإمارات.

نقاط إجراءات التنفيذ

ومع تحديد خارطة الطريق لمستقبل دولة الإمارات العربية المتحدة بوضوح، كيف يمكن لقادة الأمن السيبراني المساهمة بشكل أفضل في خارطة الطريق هذه، بالنظر إلى سياق المواضيع العالمية المحتملة المحددة لعام ٢٠٧١؟ بالنسبة لكل مبدأ، نحدد كيف يمكننا المساعدة في تنفيذه وتحقيق مستقبل إلكتروني أفضل للبلاد.

المبدأ الأول

تدعيم الاتحاد

سيتطلب تصميم تشريعات دولة الإمارات العربية المتحدة في مجال الأمن السيبراني استعدادًا لعام ٢٠٧١، خلال العقود المقبلة، تطورًا نحو إطار تشريعي يتعامل مع البشر والذكاء الاصطناعي ومزيج من الاثنين بشكل متسق بشكل متزايد. بالإضافة إلى ذلك، يجب أن يكون الإطار التشريعي قابلًا للتطبيق في كل من العالمين المادي والافتراضي حيث يتلاشى التمييز مع مرور الوقت. سوف يتطور قانون الجرائم الإلكترونية المنشور في عام ٢٠٢١ على مدى العقود القادمة ليغطي هذه الديناميكيات المتغيرة، حيث يتبنى التشريع بشكل متزايد نهجًا قائمًا على المبادئ لتعريف النشاط الإجرامي حيث أصبحت الأساليب القائمة على التكنولوجيا قديمة بسرعة بسبب سرعة التغير التكنولوجي.

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

A B C

المبدأ الثاني

أفضل نظام اقتصادي

ولإنشاء الاقتصاد الأفضل والأكثر ديناميكية في العالم بحلول عام ٢٠٧١، ستحتاج قدرات الأمن السيبراني في دولة الإمارات العربية المتحدة والنظام البيئي والشراكات إلى أن تعكس هذا الموقع باعتباره ديناميكيًا للغاية وقابلًا للتكيف مع المشهد التكنولوجي سريع التغير.

تقليديا، يُنظر إلى تنظيم الأمن السيبراني على أنه يعيق التقدم الذي ينبغي تمكينه. على مدار العقود المقبلة، يجب على الهيئات التنظيمية وشركات التكنولوجيا في دولة الإمارات العربية المتحدة العمل جنبًا إلى جنب، والعمل في بيئات معزولة حيث يتم استكشاف متطلبات الأمن السيبراني التنظيمية والتشغيلية بشكل متكرر. يمكن دمج شركاء التكنولوجيا في الذكاء الاصطناعي والسحابة وإنترنت الأشياء والميتافيرس وغيرها من التقنيات الناشئة في نموذج تنظيمي مرن وتعاوني للغاية؛ مما يتيح التبني السريع للتقنيات عبر النظام البيئي لدولة الإمارات العربية المتحدة.

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

A B C G

المبدأ الثالث

سياسة خارجية حكيمة

تم تصنيف دولة الامارات العربية المتحده باسعد مكان للعيش في العالم العربي ، وفقًا لأحدث تقرير للأمم المتحدة عن السعادة العالمية ٢٠٢٣. وبحلول عام ٢٠٧١، ستتحدد نوعية الحياة والسعادة بشكل متزايد من خلال عالم مادي ورقمي هجين آمن ومأمون حيث يعيش المواطنون (الإنسان والهجين والذكاء الاصطناعي) يمكنهم الاختلاط والعمل واللعب بحرية. وفي هذا العالم المستقبلي، ستحتاج دولة الإمارات العربية المتحدة بشكل متزايد إلى التركيز على تحديد ومحاسبة التلاعب بالمعلومات والتزييف العميق من قبل مجرمي الإنترنت والجهات الفاعلة الحكومية الخارجية التي ستتطلع إلى استخدام هذا العالم الهجين لتحقيق مكاسب استراتيجية واقتصادية.

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

A B C G

المبدأ الرابع

رأس المال البشري

إن الموقع الحالي لدولة الإمارات العربية المتحدة كمركز إقليمي للأمن السيبراني، إلى جانب البرامج الجاري تنفيذها لجذب مهارات الأمن السيبراني وتدريب المواهب الإماراتية، يشكل أسسًا قوية للمستقبل. ومع ذلك، فإن بناء رأس المال البشري اللازم في مجال الأمن السيبراني استعدادًا لعام ٢٠٧١ سيطرح العديد من التحديات على مدى العقود المقبلة. ستكون مهارات المراقبة والإشراف وتحديد حواجز الحماية المناسبة للذكاء الاصطناعي أمرًا بالغ الأهمية. وكذلك الأمر بالنسبة لفهم تأثير الذكاء الاصطناعي على متطلبات المهارات للمستقبل.

على نطاق أوسع، يجب إطلاق الأحكام على موضوعات أساسية تتعلق بالذكاء الاصطناعي والعالم الافتراضي، مثل خصوصية الذكاء الاصطناعي وبيانات الصور الرمزية، وهي موضوعات تتعلق بجوهر وعي الذكاء الاصطناعي. إن تدريب السكان الإماراتيين البارعين في مجال التكنولوجيا وفهمهم العميق للذكاء الاصطناعي سوف يضع دولة الإمارات العربية المتحدة في مكانة جيدة لاتخاذ هذه القرارات في المستقبل. ربما ستقوم دولة الإمارات العربية المتحدة بتعيين وزير للفلسفة لإجراء هذه القرارات المعقدة؟

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

B C

المبدأ الخامس

علاقات الجوار

تعد العلاقات السياسية والاقتصادية والاجتماعية المستقرة والإيجابية مع الدول المجاورة لدولة الإمارات العربية المتحدة مفيدة للغاية في قيادة المواءمة الاستراتيجية، وتعزيز التعاون في المجال السيبراني، على سبيل المثال، المنتديات المتعلقة بمكافحة عصابات الجرائم السيبرانية التي تركز على المنطقة. بحلول عام ٢٠٧١، مع استبدال الحدود المادية بحدود افتراضية، قد يمتد مفهوم حسن الجوار إلى دول خارج الحدود المادية لدولة الإمارات العربية المتحدة إلى تلك البلدان والمنظمات والشركات والمؤسسات التي تتاخم الحدود الافتراضية لدولة الإمارات العربية المتحدة.

يعد الأمن السيبراني ومكافحة الجرائم السيبرانية من المواضيع المثالية لإقامة علاقات إقليمية عميقة يكون التعاون في جوهرها. لقد تم إحراز تقدم قوي في هذا المجال من خلال مبادرات دول مجلس التعاون الخليجي التي تجمع قادة الإنترنت حول هذه المواضيع بالذات. وتمهد مؤسسات الأمن السيبراني الإقليمية هذه الطريق، وستكون ذات أهمية متزايدة لتعزيز الأمن في جميع أنحاء المنطقة، ولكن أيضًا لتعزيز الثقة والتعاون مع الجيران الإقليميين.

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

F

المبدأ السادس

تبني الابتكارات

ومع وجود التكنولوجيا في قلب الاستراتيجية الاقتصادية لدولة الإمارات العربية المتحدة ورؤيتها لعام ٢٠٧١، فإن ضمان أن الأمن السيبراني هو عامل تمكين للتطور التقني السريع أمر بالغ الأهمية. سوف يزدهر اقتصاد دولة الإمارات العربية المتحدة على نطاق أوسع مع العلم بأن الشركات والحكومة والمواطنين يتمتعون بالسلامة والأمان من التهديدات السيبرانية. وقد قطعت دولة الإمارات العربية المتحدة بالفعل خطوات كبيرة في هذا الاتجاه، حيث وصلت إلى المركز الخامس في مؤشر الأمن السيبراني العالمي للاتحاد الدولي للاتصالات. ويجب أن يستمر هذا الاتجاه، مع التوصية بإعطاء الأولوية للبحث والتطوير والاستثمار الرئيسي في المجالات التي من المحتمل أن تكون حاسمة لأمن دولة الإمارات العربية المتحدة خلال العقود المقبلة. إن الأبحاث والاستثمارات والمبادرات في مجال الذكاء الاصطناعي المستقل الإشرافي، ومن الأفضل أن يتم ذلك بالتعاون العميق مع العديد من مبادرات الذكاء الاصطناعي في جميع أنحاء دولة الإمارات العربية المتحدة، بالإضافة إلى البحث في العمليات السيبرانية الآلية والذكية على مدى العقود المقبلة، من شأنها أن تضع دولة الإمارات العربية المتحدة بقوة في مواجهة وجهات النظر العالمية المحتملة التي تصورناها في عام ٢٠٧١.

وبشكل أكثر تحديدًا، وضعت دولة الإمارات العربية المتحدة بالفعل الذكاء الاصطناعي في قلب استراتيجية دولة الإمارات العربية المتحدة، مما جعل الإمارات مركزًا تكنولوجيًا واقتصاديًا للخدمات والحلول المتعلقة بالذكاء الاصطناعي. تتمتع دولة الإمارات العربية المتحدة بموقع مثالي كمبتكر عالمي ورائد في مجال الذكاء الاصطناعي لضمان أن دولة الإمارات العربية المتحدة في وضع متساوٍ لتأمين الذكاء الاصطناعي - وهو الأمر الذي سيمكن من اعتمادٌ الذكاء الاصطناعي بشكل أسرع ودفع التنمية الاقتصادية للدولة. وسيشمل ذلك مراقبة مجموعات البيانات والنماذج المختلفة التي يعتمد عليها الذكاء الاصطناعي، ولكن الأهم من ذلك هو الأطر الإشرافية التي ستكون ذات أهمية متزايدة مع تزايد قدرات الذكاء الاصطناعي ومدى وصوله ومسؤولياته.

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

F D

المبدأ السابع

مركز التميز والامتياز

تعمل دولة الإمارات العربية المتحدة على تعزيز مؤسساتها الاتحادية منذ عقود. وهذا ليس أكثر وضوحا مما هو عليه في مجال الأمن السيبراني حيث تم إنشاء العديد من المؤسسات الفيدرالية لإدارة الأزمات السيبرانية وتحديد الاستراتيجيات والتشريعات وحماية البنية التحتية الحيوية للمعلومات (CII) من الضرر. وبحلول عام ٢٠٧١، من المرجح أن تبدو هذه المؤسسات مختلفة تمامًا عما هي عليه اليوم، حيث ستتولى دورًا أوسع وأكثر شمولًا للردع والحماية والكشف والاستجابة والتعافي من التهديدات في العالم المادي والافتراضي الهجين. إن تعزيز صلاحيات الجهات الاتحادية والتشريعات التي تلتزم بها، من شأنه أن يعزز مكانة دولة الإمارات العربية المتحدة كدولة واحدة، ذات إطار مشترك واحد لحماية الأمة من التهديدات.

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

A B

المبدأ الثامن

منظومة القيم

سيكون الانفتاح والشفافية والالتزام بإنترنت حر ومفتوح هو المفتاح لأمننا العالمي الجماعي في عام ٢٠٧١.

وسوف يصبح التعاون مع المؤسسات في المجال الرقمي التي تدفع التعاون الإيجابي وأطر الثقة والقواعد الدولية، مثل الاتحاد الدولي للاتصالات، ذا أهمية متزايدة. وتتمتع دولة الإمارات العربية المتحدة بموقع مثالي للتعاون مع هذه المؤسسات لتطوير واعتماد نماذج أمنية جديدة تتماشى مع هذا المشهد المتطور.

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

G

المبدأ التاسع

المساعدات الإنسانية

إن موقف دولة الإمارات العربية المتحدة في تقديم المساعدات الإنسانية بغض النظر عن الدين أو العرق أو اللون أو الثقافة أمر يستحق الثناء. على مدى العقود المقبلة، من المرجح أن يتطور تعريف المساعدات الإنسانية ليشمل «مساعدات الأمن السيبراني»، حيث أن الهجمات السيبرانية لها بشكل متزايد عواقب حقيقية على أولئك الأقل حظًا والقدرة على التعامل مع مثل هذه الهجمات. علاوة على ذلك، بحلول عام ٢٠٧١، قد تمتد هذه المساعدات الإنسانية إلى ما هو أبعد من المساعدات المادية، إلى العالم الافتراضي. وتقوم دولة الإمارات العربية المتحدة بالفعل بتنفيذ برامج لبناء القدرات لدعم الدول الأخرى في بناء قدراتها وبرامجها في مجال الأمن السيبراني، فضلًا عن تقديم المساعدة للأشخاص الأكثر احتياجًا. يمكن توسيع هذه البرامج وربما دمجها مع مرور الوقت لتقديم مساعدة الأمن السيبراني للدول التي تحتاج إلى الدعم.

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

A G

المبدأ العاشر

السلام والاستقرار

وقد وضعت دولة الإمارات العربية المتحدة نفسها كشريك رئيسي للأمن السيبراني في المؤسسات العالمية والإقليمية، بما في ذلك دور قيادي في مجال الأمن السيبراني في مجلس التعاون الخليجي ومساهم في المبادرة الدولية لمكافحة برامج الفدية. بالإضافة إلى ذلك، فإن المنتديات الأخرى التي تسعى إلى بناء الثقة والتعاون، مثل المنتدى الاقتصادي العالمي والأمم المتحدة، ستكتسب أهمية متزايدة خلال العقود المقبلة لضمان أن دولة الإمارات العربية المتحدة في وضع جيد لدفع السلام والوئام في المجال الرقمي.

[انقر على الأيقونات التالية لاكتشاف المزيد حول موضوعات الأمن السيبراني لعام ٢٠٧١ المتعلقة بهذا المبدأ.]

A G

كيه بي ام جي

على مدى ما يقرب من ٥٠ عامًا، قدمت كي بي إم جي لوار جالف ليمتد ولا تزال تقدم خدمات المراجعة المحاسبية والخدمات الضريبية والخدمات الاستشارية على النطاقين المحلي والدولي لنطاق عريض من العملاء من شركات ومؤسسات القطاعين العام والخاص المتخصصة في كبرى مجالات العمل التجاري والاقتصادي داخل كل من الإمارات العربية المتحدة وسلطنة عمان. نحن نساند عملائنا من خلال بناء الثقة والحد من المخاطر وتحديد فرص العمل في النشاط التجاري.

كي بي إم جي لوار جالف ليمتد هي جزء من شبكة عالمية أعضاؤها من الشركات والمكاتب المتخصصة، وهذه الشبكة تابعة لجمعية كي بي إم جي التعاونية الدولية ("كي بي إم جي إنترناشيونال كو أوبراتيف")، تضم شبكة كي بي إم جي ما يقرب من ٢٣٦,٠٠٠ عضو من المتخصصين أصحاب المهن الاختصاصية من ١٤٤ بلد وأكثر. تتواصل كي بي إم جي القائمة في الإمارات وتلك القائمة في عمان مع الشبكة العالمية من خلال شبكات تواصل مُحكمة، وهي تجمع بين ما لديها من العلم والمعرفة المتاحين على المستوى المحلي والعلم والمعرفة المقدمين من خبراء يعملون على المستوى الدولي، وتقدم أصحاب المهارات المتخصصة التي يحتاجها عملاؤنا على مستوى القطاعات.

تعمل كي بي إم جي من خلال مندوبيها المنتشرين في دول الشرق الأوسط: من خلال مكاتبها التي تعمل في كل من الإمارات وعمان، والمملكة العربية السعودية والبحرين والكويت وقطر ومصر والأردن ولبنان وفلسطين والعراق. تأسس مكتب "لوار جالف" في عام ١٩٧٣، ويبلغ عدد الموظفين الذين يعملون فيه حاليًا حوالي ١٧٨٠ موظف، من بينهم حوالي ١٩٠ فرد هم من الشركاء وأعضاء مجالس الإدارة الموجودين في مختلف أنحاء الإمارات وعمان.

وحيث إننا مستمرين في النمو، فنحن نهدف إلى التطور والتقدم ونسعى جاهدين للوصول إلى أعلى مستويات الثقة في عملنا من كل الناس. قيمنا: النزاهة والاستقامة: إذ إننا نتبع في عملنا مبدأ أنه لا يصح إلا الصحيح؛ التميز والامتياز: إذ إننا لا نتوقف مطلقًا عن التعلم وتحسين مستوانا؛ الشجاعة: إذ إن الجرأة في التفكير وفي العمل هي مبدأنا المتبع؛ العمل الجماعي: فكلٌ منا يحترم الآخر ونستمد القوة من الاختلافات القائمة بيننا؛ تحقيق الأفضل: فنحن نسعى لتلبية المتطلبات المتغيرة التي يطلبها عملاؤنا، ونتبع في سبيل ذلك نهجًا يتماشى مع أهدافنا العالمية: الاستلهام، الثقة، المكين، التغيير.

تهدف مبادرة كي بي إم جي إيمباكت KPMG IMPACT (أثر كي بي إم جي) التي نقدمها إلى مساعدة العملاء في التحقق من مقومات النجاح في مشروعاتهم التجارية المستقبلية في ظل مرحلة تسودها مشكلات مثل التغير المناخي وعدم المساواة الاجتماعية. الهدف هو مساعدة العملاء في تحقيق النجاح في إطار "أهداف التنمية المستدامة" السبعة عشر الكبرى، وفي التمكن من أن يصبحوا أكثر قدرة على الصمود والتعافي واكثر وعيًا على الصعيد المجتمعي.

خمسون عامًا مرت على تأسيس الإمارات العربية المتحدة، وخلالها تطورت الإمارات و أصبحت مركزًا للقوى الديناميكية المحركة للاقتصاد، وأصبحت لها وزنها وثقلها الاقتصادي في العالم، وصارت رمزًا للمثابرة والكد والاجتهاد.

في ظل احتفال الدولة بيوبيلها الذهبي مؤخرًا، تفخر كي بي إم جي لوار جالف ليمتد بأن تحتفل هي أيضًا هذا العام بمرور ٥٠ عامًا على تأسيسها في الإمارات.

نحن نرتكز في عملنا على ثلاث ركائز: تقديم مستوى مبهر وغير مسبوق من الخدمات؛ الالتزام الصارم بالصالح العام؛ وتكوين فريق عمل متمكن. هذه الركائز هي الأساس الذي يقوم عليه مكتبنا. خلال العقود القادمة، سنظل ملتزمين بدعم مسيرة دولة الإمارات العربية المتحدة التي ستظل تنتقل فيها من نقطة قوة إلى نقطة قوة أخرى: معًا نحو الأفضل.

شكر وتقدير

مجموعة العمل

معالي الدكتور/ محمد الكويتي
رئيس الأمن السيبراني
حكومة الإمارات العربية المتحدة

تيموثي وود
شريك في الأمن السيبراني
كي بي إم جي لوار جالف

برينيش الفا
مدير الأمن السيبراني
كي بي إم جي لوار جالف

كلير مولهيرون
مدير قسم العملاء والأسواق
في: كي بي إم جي لوار جالف

لافانيا مالهوترا
مدير مساعد قسم العملاء والأسواق،
كي بي إم جي لوار جالف

ويليام نافارو
مدير مساعد قسم العملاء والأسواق،
كي بي إم جي لوار جالف

ساندرا السيوري
مساعد قسم العملاء والأسواق،
كي بي إم جي لوار جالف

ديفيد فيربراش
رئيس عالمي لابتكارات الأمن السيبراني
كي بي إم جي **انترناشيونال**

بيلي لورانس
نائب برنامج الأمن السيبراني العالمي
كبير مديرو كي بي إم جي انترناشيونال

ليونيداس ليكوس
مساعد في برنامج الأمن السيبراني العالمي،
كي بي إم جي انترناشيونال

شبكة كي بي إم جي العالمية

اخيليش توتيجا
رئيس الأمن السيبراني العالمي، وشريك في شركة
كي بي إم جي الهند

اليكس هولت
شريك ومدير قسم الاتصالات ووسائل الإعلام على النطاق
العالمي في شركة كي بي إم جي - الولايات المتحدة الأمريكية

اندرياس توميك
شريك ورئيس الأمن السيبراني السحابي العالمي،
كي بي إم جي النمسا

أتول غوبتا
شريك ورئيس في سايبر تي ام تي جلوبال
كي بي إم جي الهند

باري برونسمان
شريك ورئيس في جلوبال سي آي أو ادفيسوري ،
كي بي إم جي
الولايات المتحدة الأمريكية

بابي سوني
شريك ورئيس لشركة جلوبال تيك كونسلتينج
كي بي إم جي الهند

كارولين ريفيت
شريك ورئيس قسم علوم الحياة السيبرانية على النطاق
العالمي، كي بي إم جي المملكة المتحدة

شارلز جاكو
شريك ورئيس الأمن السيبراني العالمي –
قسم الخدمات المالية
كي بي إم جي الولايات المتحدة الأمريكية

كليف جاستيكا
رئيس شؤون ابتكارات المشاريع،
كي بي إم جي الولايات المتحدة الأمريكية

داني ميشو
شريك ورئيس الأمن السيبراني لشؤون شركاء إدارة
المشاريع كي بي إم جي آيرلندا

هرطاج نجار
رئيس الأمن السيبراني، كي بي إم جي كندا

هنري شيك
رئيس الأمن السيبراني، كي بي إم جي الصين

جيمس مابوت
شريك في فيوتشرز كي بي إم جي،
كي بي إم جي استراليا

جون أنيانوو
رئيس الأمن السيبراني
كي بي إم جي نيجيريا

كريم صديق
شريك شركة رسك كونسلتينج
كي بي إم جي كندا

لكشمي سانكار
مدير الأمن السيبراني
في شركة كي بي إم جي بالولايات المتحدة

ليزا هينيغان
مدير الشؤون الرقمية على النطاق العالمي
وشريك في كي بي إم جي بالمملكة المتحدة

ماتثيو أو كييف
رئيس الأمن السيبراني في شبكة مراكز العلوم
والتكنولوجيا في منطقة آسيا والمحيط الهادئ،
وشريك في شركة كي بي إم جي في استراليا

ميكا لاكسونين
مدير الشؤون السيبرانية
في شركة كي بي إم جي في فنلندا

مينا ذكي
المدير المساعد لتحالف شركات كي بي إم جي
لشؤون الأمن السيبراني في استراليا

ناشيكتا أنجاد
الشريك المختص بشؤون الخدمات الاستشارية المختصة
بالمخاطر في شركة كي بي إم جي في جنوب أفريقيا

أوزتورك تاسبينار
رئيس قسم الابتكارات الرقمية في شركة كي بي إم جي في بلجيكا

براساد جايارامان
رئيس الأمن السيبراني على نطاق دول الأمريكتين
وشريك في شركة كي بي إم جي في الولايات المتحدة

رونالد هيل
رئيس الشؤون السيبرانية المرتبطة بـ بإدارة المشروعات الرقمية
على النطاق العالمي وشريك في شركة كي بي إم جي في هولندا

روني ميشيل
شريك في شركة كي بي إم جي في إسرائيل

ساندر كلاوس
الشريك المختص بشؤون البيانات والتحليلات
في شركة كي بي إم جي في هولندا

سيلفيا كينجسميل كلاسوفيك
مدير شؤون الخصوصية على النطاق العالمي
وشريك في شركة كي بي إم جي في كندا

ستيفن هيل
رئيس قسم الابتكارات على النطاق العالمي
وشريك في شركة كي بي إم جي في الولايات المتحدة

تون دايامونت
مدير الأمن السيبراني وشريك في شركة
كي بي إم جي لوار جالف في المملكة العربية السعودية

والتر ريزي
مدير الأمن في معاهد التكنولوجيا على النطاق العالمي
وشريك في شركة كي بي إم جي في الأرجنتين

ويندي ليم
الشريك المختص بالشؤون السيبرانية في شركة
كي بي إم جي في سنغافورة

ويلهالم دوللي
رئيس الشؤون السيبرانية المرتبطة بـ IGH على النطاق العالمي
وشريك في شركة كي بي إم جي في ألمانيا

طرف خارجي

د. إدوارد آموروزو
مدير تنفيذي للشؤون السيبرانية TAG

المراجع:

١- World Population Prospects: (التوقعات السكانية العالمية): نسخة منقحة صادرة في ٢٠١٧ وتولت نشرها: إدارة الشؤون الاقتصادية والاجتماعية بالأمم المتحدة.

٢- International Energy Outlook ٢٠٢١ (نظرة مستقبلية على شؤون الطاقة على المستوى الدولي للعام ٢٠٢١) – هيئة الاستعلامات الأمريكية لشؤون الطاقة: https://www.eia.gov/outlooks/ieo/narrative/introduction/subtopic-01.php

٣- /https://worldhappiness.report/ed/2023

٤- https://u.ae/en/about-the-uae/economy/digitaleconomy#:~: text=The%20UAE's%20digital%20economy%20contributes,increase%20in%20the%20coming%20period

٥- /seirtnuoc/moc.weivernoitalupopdlrow//:sptth noitalupop-setarime-bara-detinu

٦- https://www.unep.org/resources emissions-gap-report-2022

٧- https://www.itu.int/en/ITU-D/Cybersecurity Pages/ global-cybersecurity-index.aspx

٨- https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/ finance-and-economy digital-economy-strategy

٩- https://www.mofa.gov.ae/en/mediahub/ news/2023/1/21/21-01-2023-uae

اتصل بنا

تيموثي وود
شريك، رئيس الأمن السيبراني
كي بي إم جي لوار جالف
هاتف: +٩٧١ ٥٦ ٤٠٩٦ ٨٤٢
البريد الإلكتروني: timothywood@kpmg.com

ديفيد فيربراش
رئيس عالمي في شركة سايبر فيوتشرز
كي بي إم جي انترناشيونال
البريد الإلكتروني: david.ferbrache@ kpmg.com

اخيليش توتيجا
رئيس الأمن السيبراني العالمي،
كي بي إم جي انترناشيونال وشريك
في كي بي إم جي الهند
البريد الإلكتروني: atute@kpmg.com

براساد جايارامان
قائد ورئيس الأمن السيبراني الأمريكي
كي بي إم جي
البريد الإلكتروني: prasadjayaraman@kpmg.com

داني ميشو
شريك ورئيس الأمن السيبراني لشؤون
شركاء إدارة المشاريع
كي بي إم جي آيرلندا
البريد الكتروني: Dani.michaux@kpmg.ie

مات أوكيف
شريك ورئيس الأمن السيبراني لشؤون
شبكة آسيا والمحيط الهادئ في مراكز العلوم
والتكنولوجيا، كي بي إم جي استراليا
البريد الإلكتروني: mokeefe@kpmg.au

www.kpmg.com/**ae**
www.kpmg.com/**om**

تابعنا على:

@kpmg_lowergulf

اسم النشر: Cyber next 50
رقم النشر: ٤٧٧٥
تاريخ النشر: سبتمبر ٢٠٢٣