سلبيات الذكاء الإصطناعي

الأربعاء 23 مايو 2018 10:05 م

في الوقت الذي أصبح مجال أمن المعلومات أكثر تعقيداً فإن كل أسبوع يحمل لنا أخباراً وآمالاً جديدة تتمثل في التطورات التي تشهدها أبحاث تعلم الآلة والذكاء الإصطناعي وفي دولة الإمارات العربية المتحدة فإن مثل هذه التقنيات تحظى بالثقة أكثر من أي مكان آخر في العالم، وهو ما يتجلى في تعيين عمر بن سلطان العلماء كأول وزير دولة للذكاء الإصطناعي على مستوى العالم، وتأتي هذه الخطوة من جانب الإمارات في الوقت الذي تتطلع الدولة إلى تعزيز أداء كافة قطاعاتها الحكومية، بما في ذلك النقل والرعاية الصحية والفضاء والطاقة المتجددة والتعليم

لا شك أن التقدم الذي تم إحرازه في هذا المجال هو ثمرة لجهود حثيثة يبذلها الخبراء والمتخصصون في تطوير خوارزميات ذكية بوسائل ذاتية العمل، إلا أن الخطر الذي يكتنف هذه التقنيات الجديدة هو أنه في الوقت الذي قد تنطوي عليه اليوم من ميزات، فإنها يمكن أن تصبح وسيلة يستخدمها المجرمون يوماً ما في المستقبل لتنفيذ مآربهم المدمّرة، لذا فإننا نجد أنفسنا أمام تحدٍ كبير يهدد أنظمة الجيل المقبل لأمن المعلومات، فكيف السبيل إلى تحقيق التوازن السليم لجني ثمار الذكاء الاصطناعي والتهديدات المتوقعة نتيجة استخدامه؟

بكل تأكيد هي مسألة وقت قبل أن نشهد هذه تهديدات الذكاء الإصطناعي سواء كانت عبر هجمات التصيد الإلكتروني من خلال هجمات الرسائل التطفلية التلقائية الموجّهة نحو هدف محدّد، أو الأجهزة المصابة ذاتية الانتشار التي تقوم ببرمجة نفسها بنفسها أو ما يطلق عليه الطفيليات السيبرانية القادرة على شن هجمات ذاتياً دون تدخل بشري، أو البرمجيات الخبيثة متعددة الأشكال والتي لديها القدرة على الانتشار بشكل مستمر أثناء الهجمات

إن التحديات الاجتماعية والأخلاقية التي يواجهها الباحثون القائمون على حماية أنظمة المعلومات والحد من الإفراط في إساءة استخدام تقنيات الذكاء الإصطناعي اليوم لن تكون هي نفسها تحديات الغد، إذ ستختلف الأدوات التي يستخدمها القراصنة، ولا شك أن تهديدات الذكاء الإصطناعي لن تتم في إطار بيئة مُحكمة المراقبة، كما أن انتشارها لن يخضع لتشريعات بكل تأكيد، وينطوي بناء منظومة ذكاء اصطناعي أكثر فاعلية ودماراً على أولوية أكثر أهمية من مراعاة الجوانب الأخلاقية أو التطبيقات طويلة الأمد، فلا يمكن أن نتوقع أن تخضع هذه التهديدات للقوانين الثلاثة للروبوتات

ربما يظن البعض أن البرمجيات الخبيثة غير قادرة على إنتاج خوارزميات متطورة، كتلك التي تقوم عليها هجمات الذكاء الإصطناعي، إلا أن البرمجيات الحديثة وبرمجيات الفدية لم يعد يتم تطويرها على أيدي مجموعة صغيرة من القراصنة، والتي لا يتطلب الأمر سوى شخص واحد يتم تكليفه بكتابة كود كامل لبرنامج مدمّر

أما اليوم، فإن عدداً هائلاً من البرمجيات الخبيثة المتخصصة يتوفر عبر آلاف المنصات المنتشرة على المواقع الإلكترونية الخاصة ببرمجيات الاختراق، بل إن أحدث هذه البرمجيات بإمكانك شراؤها من خلال عدة مواقع، تماماً كما تشتري كتباً أو ملابس، وتتضمن البرمجيات النموذجية حالياً وحدات متنوعة من الطرف الثالث ومصادر مفتوحة، وهي متخصصة في مجالات التشفير أو فك التشفير، وأنظمة المدفوعات والبنية التحتية لمراكز التحكم والسيطرة وغيرها

إنتاج خوارزميات معقدة ليس بالأمر الهيّن هذه الأيام، إذ يتطلب مهارات برمجيات خاصة ووقتاً للقيام لكي يتمكّن المبرمج من بناء وحدة أولية يستطيع من خلالها قراصنة آخرون استخلاصها واستخدامها كبرمجية خبيثة قائمة على تقنية الذكاء الاصطناعي، وشبكات "البوتات" الخبيثة التي تضم مئات الآلاف من الأجهزة المصابة الفيروسات والأجهزة العاملة على منصات إنترنت الأشياء بإمكانها توفير طاقة الحوسبة التي تحتاجها هذا الجيل المقبل من الهجمات

إننا نتوقع تطوراً على مستوى تحسين الخوارزميات في كافة مراحل الهجمات النموذجية، سواء في مرحلة البداية، أو إصابة الهدف، أو السيطرة والتحكم، أو الانتشار، أو ابتزاز الضحية، وفي ظل التعرض للتهديد من جانب برمجية خبيثة ذكية ومجزّاة وهجمات برمجيات الفدية

الخبيثة، فإن الفرصة سانحة بالنسبة للشركات للتخلص من إجراءات التأمين الجامدة والمبادرة بتطبيق مستوى ملائماً يتألف من مجموعة أدوات أمنية، فلابد أن تتحلى الشركات بقدرات تمكّنها من تشتيت أو قطع أوصال السلسلة المدمّرة على شبكة الانترنت، وذلك عبر مراحل متعددة بقدر الإمكان

وبدلاً من أن نرى صراعاً بين قوتين كبيرتين تتقاتلان من أجل حسم معركة واحدة، سوف نرى حرباً أشبه بحرب العصابات التي تتضمن آلاف من المناوشات والمعارك المنفصلة، والتي يدور معظمها دون أي توجيه من عنصر بشري

إن الانتصار في المعارك الرقمية المستقبلية مرهون بالقدرة على التنسيق وقوة الأتمتة والقدرة على حماية كافة الموارد المرتبطة بالشبكة عبر أدوات أمنية مناسبة، حيث سيشكل الإعداد لهذه المعارك أمراً جوهرياً في هذا العصر الجديد