المستقبل
للأبحاث والدراسات المتقدمة

اسم الموضوع : مجتمع ما بعد المعلومات

عنوان الموضوع : الثورة الصناعية الرابعة تغير المنظور المعرفي للبشر.. إيهاب خليفة يستشرف المستقبل في كتابه الجديد "مجتمع ما بعد المعلومات

تاريخ النشر : 20/03/2019

اسم الكاتب : محمد الحمامصي

الموضوع :

تشهد السنوات القليلة المقبلة تغيُّرًا جذريًّا في أنماط حياة الأفراد، وطرق إدارة الدول والمؤسسات، وأشكال الحروب والصراعات، مدفوعة في ذلك بتقنيات أكثر ذكاءً ودقَّة وكفاءةً في مجملها من قدرات الإنسان، تتمثل في نظم الذَّكاء الاصطناعي، والطابعات ثُلاثيَّة، ورُباعية الأبعاد، وتقنيات إنترنت الأشياء، والسيارات ذاتية القيادة، والدرونز، والحاسبات الكمومية، ونظم "البلوك تشين" القادرة على إدارة جميع المعاملات البشرية، وبذلك تدخل البشرية على مرحلة جديدة من التاريخ الإنساني. هذا ما يؤكد عليه الكاتب د. إيهاب خليفة رئيس وحدة التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات المتقدمة، ويحاول استشرافه في كتابه الجديد "مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي"، الصادرة عن مركز المستقبل للأبحاث والدراسات المتقدمة بأبوظبي بالتعاون مع دار العربي للنشر.وأشار الكاتب إلى أن الثورة الصناعية الرابعة من شأنها أن تغير ليس فقط من هياكل الإنتاج وخصائص المجتمعات وموازين القوة، بل تغير أيضاً من المنظور المعرفي للبشر تجاه الأشياء بصورة عامة؛ فالبشرية أصبحت على وشك التحول نحو جيل جديد من المجتمعات، حيث ينذر هذا التحول بظهور مجتمع فائق الذكاء تكون فيه اليد العليا للآلة على الإنسان، وتتحقق فيه نبوءات أفلام الخيال العلمي بتآكل المجتمع من داخله عبر إزالة الخطوط الفاصلة بين ما هو إنساني وما هو مادي، ويتعدى ما تم تسميته بمجتمع المعلومات ليظهر "مجتمع ما بعد المعلومات".هذا المجتمع الجديد الذي سماه د. خليفة بـ "مجتمع ما بعد المعلومات"، يأتي بعد أربعة أجيال رئيسية مرت بها الإنسانية، وهي: مجتمعات الصيد والزراعة والصناعة والمعلومات، وأخيراً المجتمع أو "مجتمع ما بعد المعلومات" على حد قول الكاتب، ذلك المجتمع الذي تندمج فيه المعلومة والآلة مع عقل الإنسان فتتحول المعلومة لوظيفة.وأوضح إيهاب خليفة ذلك بقوله إنه بدلاً من أن يستخدم الفرد خرائط جوجل مثلاً للذهاب إلى مقصده كما هو الحال في مجتمع المعلومات، ستقوم السيارة ذاتية القيادة أو الطائرات المسيرة بدون طيار بذلك في مجتمع ما بعد المعلومات، وبدلاً من إعطاء أوامر للروبوتات للقيام ببعض الوظائف والمهام، فإنها سوف تقوم بصورة منفردة بتحليل المعلومات من المجسّات وأجهزة الاستشعارات الموجودة في كل مكان وتتخذ القرار بصورة ذاتية، وستقدم تقنيات إنترنت الأشياء خدمات للبشر تسبق احتياجاتهم وتوقعاتهم، ومن هنا تتحول المعلومة لوظيفة تقوم بها الآلة عوضاً عن الإنسان. وقد حاول هذا الكتاب من خلال أربعة فصول تقديم القوى التكنولوجية المُحرّكة للثورة الذَّكيَّة التي سوف تؤثر على حياة البشرية في المستقبل القريب، لتنقلها إلى مرحلة "مُجتمع ما بعد المعلومات" لينهي بذلك مرحلة من الحياة الإنسانية، ويعلن تدشين مرحلة جديدة، قد تهيمن فيها العقول الصِّناعيَّة على العقول البشرية، وتتحكَّم في حياة الأفراد مجموعة خوارزميات تُرتِّب لهم أولوياتهم، وأفكارهم، واحتياجاتهم، وتتَّخذ بدلاً منهم قراراتهم، وتُدير شؤون حياتهم اليومية، مثل المساعدات الصوتية الذَّكيَّة، وتقنيات الواقع المُعزَّز، وإنترنت الأشياء، وتتولَّى المركبات ذاتية التحكُّم شؤون تحرُّكاتهم وتنقُّلاتهم، وتقوم الطابعات ثُلاثيَّة الأبعاد بطباعة أطعمتهم الغذائية، وأعضائهم البشرية، ومتطلبات حياتهم اليومية، لتصبح حياة الأفراد عبارة عن مشاهدة أحد أفلام الخيال العلمي.عرف خليفة الدفاع الإلكتروني الوقائي بأنه "وسيلة لتحقيق الأمن الإلكتروني من خلال استخدام آليات رصد الهجمات السيبرانية وتحليلها وتحديد مصدرها والتخفيف من حدة آثارها على نظم الاتصالات والشبكات والبنية التحتية، وذلك في وقتها الحقيقي، مع توافر القدرات الهجومية لتعقب الكيانات وتدمير الشبكات، التي انطلق منها هذا التهديد". وقال إن الدفاع الوقائي يختلف عن نظيره التقليدي في عنصرين رئيسيين، هما الاكتشاف المبكر للهجمات الإلكترونية، والتعامل معها في حالة حدوثها؛ فبينما يعمل الدفاع التقليدي كدرع داخلية للتخفيف من حدة الهجمات والتعافي السريع منها، يعمل الدفاع الوقائي كرمح استباقي لإعاقة الخصم عن تنفيذ الهجمة الإلكترونية. ويتحقق الدفاع الإلكتروني الوقائي من خلال ثلاثة أساليب رئيسية، وهي:أولا: الكشف المبكر للهجمات في وقتها الحقيقي: يتم تحقيق هذا الأمر من خلال استخدام مجسَّات على الشبكات والبرامج والتَّطبيقات، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يُصنف على أنه هجمة إلكترونية، وبداية مواجهتها واحتوائها قبل أن تبدأ نشاطها في الشبكة أو النظم المستهدفة.ثانيا: الهجوم الإلكتروني الاستباقي: يتم ذلك من خلال استخدام ونشر الديدان البيضاء، وهي برامج قادرة على اكتشاف التَّطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمة إلكترونية محتملة. كما تقوم أيضًا بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمة نفسها، وليس التصدي لها فحسب، كما يشمل أيضًا مهاجمة الخصم، فما أن يتم تحديد هوية ومصدر الهجمة، حتى يمكن إطلاق هجمة إلكترونية مضادة فيما يعرف بالاختراق العكسي.ثالثا: التضليل والإخفاء والخداع: يتم عن طريق إخفاء هويات الأهداف الاستراتيجية للدولة على الإنترنت، وتضليل الخصم أثناء محاولة الوصول إليها أو اختراقها، من خلال أدوات التمويه والخداع وتغيير ملامح الأهداف الاستراتيجية للدولة، بما يساعد على تضليل الخصم وتشتيت الانتباه عن الهدف الرئيسي.وأكد أن أهداف الدفاع الإلكتروني تتمحور في الحفاظ على مقدرات الأمن القومي التكنولوجي للدولة، من خطوط اتصالات، وشبكات كمبيوتر، وبنية تحتية، سواء مدنية، أو عسكرية، فضلاً عن تأمين البيانات الحيوية، بما يساهم في النهاية في تحقيق الأمن الإلكتروني للدولة والدفاع عن مصالحها في الفضاء الإلكتروني وتدعيم قدراتها في مجال الحروب الإلكترونية، وردع أي محاولة لزعزعة استقرارها عبر الإنترنت.وحدد د. خليفة أهداف الدفاع الإلكتروني في التالي: 1 - حماية الأهداف العسكرية: تشمل هذه الأهداف نظم الإدارة والمراقبة ونظم التحكم والسيطرة ونظم توجيه الأسلحة وقطاع الاتصالات الحربية والأسلحة آلية القيادة، مثل الطائرات من دون طيار، فضلاً عن تأمين المنشآت العسكرية، مثل محطات الطاقة النووية من أي اختراق إلكتروني.2 - حماية البيانات العسكرية: تشمل المعلومات حول أفراد القوات المسلحة كالأسماء، والرتب، والمرتبات، والوظائف داخل الجيش، وأماكن الإقامة الشخصية، فضلاً عن خطط التسليح وتصميمات الأسلحة، وخرائط انتشار القوات وتوزيع الأسلحة وغيرها من المعلومات السرية.3 - حماية البنية التحتية الحرجة: تشمل على سبيل المثال قطاعات الاتصالات والمواصلات، ومحطات الطاقة، ونظم إدارة المرور، وقواعد البيانات الحكومية، وخدمات الحكومات الذَّكيَّة، والبنوك والمؤسسات المالية والمصرفية.4 - دعم وحدات الحرب السيبرانية: هي تلك الوحدات الخاصة بإدارة الحروب السيبرانية للدولة، حيث تكون مهمة الدفاع الإلكتروني تأمين الخطوط خلف هذه الوحدات، بما يحمي أهداف الدولة الاستراتيجية في حالة شنّ هجوم إلكتروني مضاد عليها، وتوفير غطاء إلكتروني للوحدات المقاتلة بهدف التمويه والخداع وصعوبة تعقب مصدر الهجمة. يتم ذلك من خلال رفع تكلفة الهجوم الإلكتروني على الدولة المُعادية، عبر إنشاء نظم دفاع إلكترونية صعبة الاختراق تحتاج إلى وقت وجهد كبير لاختراقها، مع تطوير قدرات تتبع الهجمات السيبرانية واكتشاف مصدرها، بما يؤدي في النهاية إلى التأثير على قرارات الخصم وردعه من شنّ هجمات إلكترونية على الدولة في النهاية.6 - تحقيق الأمن الإلكتروني: إن الهدف الرئيسي من الدفاع الإلكتروني، هو تحقيق الأمن الإلكتروني داخل الدولة بصفة عامة، أي ضمان سلامة واستقرار الشبكات والأجهزة، واستمرار تقديم الخدمات الإلكترونية.ورأى د. خليفة أنه مع توجُّه الدول لتبنِّي نماذج ذَكيَّة تعتمد بصورة رئيسية على تكنولوجيا المعلومات والاتصالات لإدارة جميع متطلبات الحياة اليومية فيها، واعتماد النظم المالية والمصرفية والإدارية على الانترنت، وانتشار أجهزة انترنت الأشياء والذَّكاء الاصطناعي في كل مكان، تُصبح الدول والأفراد أكثر عُرضة للاختراق، وتُصبح جميع الخدمات الحكومية أكثر عُرضة للتوقف المفاجئ من خلال هجمات القراصنة، وتصبح قواعد البيانات والخطط والاستراتيجيات والوثائق والمعلومات السرية عُرضة للتلاعب بها وتسريبها، وتُصبح الأسلحة والأدوات العسكرية قليلة التكلفة وسهلة التصنيع وشديدة التدمير، وهي عبارة عن فيروسات كمبيوتر، وتزداد احتمالية نشوب صراعات سيبرانية بين الدول لا يمكن احتواؤها، حتى تتطوَّر وتصل إلى مرحلة الحرب السيبرانية الشاملة.*المصدر: ميدل إيست أون لاين