

الأمن الغذائي والقرصنة الإلكترونية

أمن وأفكار

حذر الخبراء من أن الآلات الزراعية «الذكية» الحديثة عرضة للقرصنة، ما قد يعرض سلاسل توريد الغذاء العالمية للخطر. ويُخشى أن يتمكن القراصنة من استغلال الخلل ونقاط الضعف في المعدات الزراعية المستخدمة في زراعة المحاصيل وحصادها.

وتقول عملاقة صناعة الآلات الزراعية «جون دير»، إنها تعمل الآن على إصلاح أي نقاط ضعف في البرامج الإلكترونية التي تدير آلاتها الزراعية.

وقال تقرير حديث لجامعة كامبريدج، إن أجهزة رش المحاصيل الآلية والطائرات من دون طيار والحاصدات الآلية يمكن قرصنتها. وحذرت حكومة المملكة المتحدة ومكتب التحقيقات الفيدرالي من تزايد خطر الهجمات الإلكترونية.

«وقالت «جون دير» إن حماية العملاء وآلاتهم وبياناتهم هي «أولوية قصوى

وباتت التكنولوجيا الذكية تستخدم بشكل متزايد لجعل المزارع أكثر كفاءة وإنتاجية، فعلى سبيل المثال كان الحصاد

الذي يتطلب عمالة مكثفة للمحاصيل الغذائية الحساسة، مثل قطاف الهليون، بعيداً عن متناول الآلات

ويستخدم أحدث جيل من الروبوتات الزراعية الذكاء الاصطناعي، ما يقلل دور العامل البشري. وقد تساعد الروبوتات في سد النقص في اليد العاملة، أو زيادة الإنتاجية، لكن المخاطر الأمنية التي ترافق ذلك في تزايد، ما يزيد من القلق بشأن سلاسل الإمداد الغذائي التي تأثرت كثيراً بالحرب في أوكرانيا، وجائحة كورونا

وقال كريس تشافاس، أحد مؤسسي شركة «مادي ماشينز» التي تختبر روبوتاً آلياً لحصاد الهليون يسمى «سبراوت»: «هناك خطر حقيقي من أن يحاول شخص ما، في أي مكان في العالم السيطرة على هذه الآلات، وجعلها تفعل ما يريد».

وحتى أن أكبر الشركات ليست في مأمن من عمليات العصابات الإلكترونية، حيث يستخدم البعض برامج الفدية التي تعتمد على تشفير البيانات وقفل الأنظمة

وفي العام الماضي، دفعت شركة «جيه بي إس»، إحدى أكبر شركات تصنيع اللحوم في العالم 11 مليون دولار كفدية لهجوم فدية، «AGCO» لقراصنة إلكترونيين كي تعود إلى العمل. وفي هذا الشهر، تعرضت أكبر شركة زراعية أمريكية ما أثر في إنتاجها

وفي إبريل/ نيسان حذرت مجموعة من هيئات الأمن السيبراني الحكومية، بينها المملكة المتحدة والولايات المتحدة وأستراليا، من أن القراصنة الروس الذين ترعاهم الدولة يمكن أن يستهدفوا سلاسل التوريد كجزء حيوي من البنية التحتية في الدول الغربية

(بي بي سي)