السعودية تلوذ بإسرائيل بذريعة حماية أرامكو من الهجمات الفيروسية

كشف معهد واشنطن لدراسات الشرق الأدنى، عن تفاصيل التعاون «السيبراني» بين السعودية، والإمارات من جهة، وإسرائيل من جهة أخرى.

وبحسب المعهد، فإن الأسباب الرئيسية لهذا التعاون، هو محاربة التوسع الإيراني في المنطقة. وتابع المعهد أن «المغامرات الإيرانية والتطورات الأخرى في منطقة الشرق الأوسط، شكلت تقارباً تاريخياً في المصالح بين إسرائيل وبعض دول الخليج العربية، مع قيام مسؤولين إسرائيليين بارزين بزيارات دورية هناك، وتطوّر التعاون الاستخباري بين الجانبين بحيث أصبح حدثاً منتظماً، وبدء الروابط الثقافية والاقتصادية بالظهور تدريجياً إلى العلن.

ومع ذلك، يمكن القول إنه تم التدقيق في هذه العلاقات بشكل كبير في المجال السيبراني». وأضاف أنه «وفقاً للحسابات العلنية، استخدمت الحكومات العربية التكنولوجيا الإسرائيلية للدفاع عن أنظمتها ضد الهجمات الإلكترونية والقبض على الإرهابيين، ولكن أيضاً لاستهداف النقّاد المحليين، من بينهم كما يحتمل الصحفي السعودي المقتول جمال خاشقجي». ولفت المعهد في تقريره الذي أعده نيري زيلبر، إلى

التطبيع العلني بين بعض دول الخليج وإسرائيل، ابتداء من زيارة رئيس الوزراء السابق إسحاق رابين إلى مسقط عام 1994، مرورًا على التكنولوجيا الإسرائيلية في الطائرات الإماراتية.

وحول التعاون السيبراني، قال المعهد، إن ذلك بدأ للمرة الأولى في عام 2007، عندما لجأت دولة الإمارات إلى شركة «فور دي للحلول الأمنية» (4D Security Solutions) التي تعود ملكيتها لإسرائيل ومقرها في الولايات المتحدة، من أجل تحديث دفاعاتها حول منشآت الطاقة الحساسة، وإنشاء نظام مراقبة «ذكي» على مستوى المدينة في أبوظبي. ووفقاً لتقارير إعلامية متعددة، فازت شركة «آي جي تي إنترناشونال» (AGT International)، وهي شركة سويسرية منفصلة يملكها صاحب شركة «فور دي» ماتي كوخافي، بعقد قيمته 6 مليارات دولار وفقاً لبعض التقارير، مع تقديم شركة «لوجيك إندستريز» (Logic Industries) التابعة لها ومقرها في إسرائيل الخبرة الفنية الفعلية لهذا المشروع، ويُعتقد أن النظام الذي تم وضعه، والذي غالباً ما يُطلق عليه «فالكون آي» (Falcon Eye) «عين الصقر» قد اكتمل بحلول عام 2016. ويشمل هذا النظام شبكةً من الكاميرات وأجهزة استشعار ومنصات للذكاء الاصطناعي توفّر كافة أنواع البيانات، بدءًا من التحكم في حركة المرور إلى المراقبة الحميمة.

وأفادت التقارير بأنه في عام 2014 تم استخدام بعض عناصر هذا النظام للقبض على امرأة جهادية بعد هجوم بالسكين على مُدرّسة أمريكية. وقد تم السماح لاحقاً لنفس هذا الاتحاد من الشركات المملوكة لإسرائيليين، بالمشاركة في مناقصة على مشروع كان يهدف إلى المساعدة في إدارة تدفق الحجاج إلى مكة المكرمة.

وعلى الرغم من عدم نجاح المناقصة، أفادت وكالة «بلومبيرج» بأن السلطات السعودية وضعت في النهاية نظاماً إلكترونياً مماثلاً للنظام المقترح، بحسب معهد واشنطن.

وذكر المعهد أن الرياض سعت للحصول على مساعدة إسرائيلية في معالجة احتياجات سيبرانية أخرى.

ففي عام 2012، تسببت عملية ضخمة ضد شركة النفط السعودية العملاقة «أرامكو» المملوكة للدولة بمحو بيانات ثلاثة أرباع حواسيب الشركة (حوالي 30 ألف محطة عمل)، وهي حادثة تم وصفها آنذاك على أنها الهجوم السيبراني التجاري الأكبر في التاريخ.

ويعتقد مسؤولو الاستخبارات الأمريكية أن منفذي ذلك الهجوم الذين استخدموا «فيروس شمعون» كانوا ممولين من الحكومة الإيرانية.

وبعد مرور سنوات، قال رجل الأعمال الإسرائيلي المتخصص في مجال التكنولوجيا المتقدّمة والمشرّع السابق أريئيل مارغاليت إلى صحيفة «كالكاليست» إنه تم اللجوء إلى شركات متخصصة في الأمن السيبراني في بلاده من أجل مساعدة شركة «أرامكو» السعودية على إصلاح الضرر، وهي عملية استغرقت شهوراً.

وفي عام 2015، لجأت الرياض إلى الشركة الإسرائيلية «إنتو فيو» (IntuView) للمساعدة في تعقّب الجهاديين على مواقع التواصل الاجتماعي. ووفقاً لوكالة «بلومبيرج»،

لبّت الشركة ذلك الطلب باستخدامها برنامج يمكنه مراجعة 4 ملايين مشاركة على موقعَي «فيسبوك» و«تويتر» يومياً.

وعلى غرار العديد من الشركات الإسرائيلية العاملة في الخليج، أنشأت « إنتو فيو» شركةً وسيطة في أوروبا لإعطاء السعوديين القدرة على الإنكار.

ووفقاً لصحيفة «هآرتس»، حصلت البحرين على نظام مماثل لمراقبة مواقع التواصل الاجتماعي من شركة «فيرينت» (Verint) المؤسسة في إسرائيل والرائدة في مجالها، في وقت ما بعد عام 2011.

معهد واشنطن قال إن «الأمر الذي لا يبشر بالخير هو اتساع نطاق عمل شركة «إنتو فيو» مع السعوديين لاحقاً ليشمل مراقبة الآراء العامة حول العائلة المالكة، مع تسليط الضوء على الخط غير المستقر في كثير من الأحيان بين الدفاع والهجوم في المجال السيبراني».