التنصت: الأمن السيبراني في عصر غير آمن

سوزان لانداو

Listening in: Cyber security in an Insecure Age,

By: Susan Landau, Yale University Press, 240 pp., $25, 2017, ISBN: 9780300227444

عرض: علي عاطف حسان، باحث في العلوم السياسية

تصاعدت حدة تهديدات الأمن السيبراني في العالم نتيجة للتطور في تكتيكات وأدوات الاختراق وتزايد خطورة تداعياتها السياسية والاقتصادية والأمنية. وفي هذا الإطار ركزت خبيرة الأمن السيبراني الأمريكية، سوزان لانداو، في كتابها "التنصت: الأمن السيبراني في عصر غير آمن" على الارتباط الوثيق بين التطور التكنولوجي والأمن القومي، كما شددت على أهمية تأمين البيانات والشبكات لمواجهة الاختراقات المُحتملة.

تهديدات الانكشاف السيبراني

أدت الثورة التكنولوجية إلى تصاعد تهديدات الانكشاف السيبراني، خاصة بعدما وصل الأمر إلى حد اختراق شركات التكنولوجيا الكبرى، مثل الاختراق الذي قام به بعض الهاكرز الصينيين لجوجل في عام 2009، وهو ما أتاح لهم الوصول للبريد الإلكتروني لبعض المعارضين الصينيين.

كما شهد العام نفسه اختراق اثنين من أكبر الشركات العسكرية وهما: نورثرب جرومان، ولوكهيد مارتن، وتمت سرقة محتويات الأبحاث والتطوير الخاصة بطائرات "بي - 2" (B -2) و"إف- 22" (F-22) و"إف - 35"(F -35)، وأشار الكتاب إلى أن المقاتلة الصينية من طراز "شينياج جي- 31" (Shenyang J-31) التي قامت الصين بتصنيعها في عام 2010 تشابه تصميمها بشدة مع تصميم مقاتلات "إف- 35" متعددة المهام.

وامتدت تهديدات الاختراق والتجسس لتصل إلى حكومات الدول الكبرى، فمثلاً تمكنت الصين من التجسس على شبكات الاتصالات في الولايات المتحدة الأمريكية في عام 2004، كما أشارت مقالة منشورة في مجلة التايم الأمريكية في عام 2005 إلى استغلال بعض الهاكرز للثغرات الموجودة في شبكات وكالة ناسا الفضائية والبنك الدولي والجيش الأمريكي وقيامهم باختراقها، واستخدم الجيش الأمريكي سلاح الاختراق لتدمير أجهزة الطرد المركزية الإيرانية في عام 2010 فيما عرف بهجمات "ستوكسنت" (Stuxnet).

ولم يدرك الأفراد العاديون حجم هذه التهديدات بوضوح إلا بعد تسريبات سنودن في عام 2013 والتي أكدت قيام وكالة الأمن القومي بالولايات المتحدة الأمريكية بالتجسس على المكالمات الهاتفية، وعلى الخوادم الخاصة بشركات التكنولوجيا الكبرى مثل: مايكروسوفت، وياهو، وجوجل، وفيس بوك، وسكايب، وغيرها باستخدام برنامج "بريسم" (PRISM).

ودفع ذلك العديد من الشركات التكنولوجية إلى تطوير تطبيقات تقوم على فكرة التشفير الكامل (End-To-End Encryption) والتي تمنع أي شخص باستثناء المرسل والمتلقي من الوصول إلى هذه الرسائل، وهو ما استغلته لاحقاً التنظيمات الإرهابية في التواصل بعيداً عن رقابة المؤسسات الأمنية.

استراتيجيات مواجهة التهديدات

يقترح خبراء الأمن مجموعة من الاستراتيجيات لمواجهة هذه التهديدات منها مراقبة الشبكات باستمرار لإيقاف أي نشاط مريب، والاعتماد على أنظمة تشفير قوية لمنع المخترقين من سرقة الوثائق المهمة، وحماية الشركات من الاختراق بالإضافة إلى إيجاد بدائل لمنع الاتصال الدائم للأجهزة بالإنترنت، والتخزين الداخلي للبيانات والمعلومات في أجهزة مؤمنة ضد الاختراق.

وفي المقابل يتم استخدام التشفير من قبل التنظيمات الإرهابية وهو ما يمنع السلطات الأمنية من تعقبهم، فعلى سبيل المثال كان الإرهابي "سيد فاروق" والذي قام بهجوم سان برناردينو الإرهابي في عام 2015 يستخدم هاتف آيفون ويتبع هذا الهاتف خاصية التشفير، وهو ما اضطر مكتب التحقيقات الفيدرالي الأمريكي إلى مطالبة شركة "أبل" بفك التشفير عن هاتفه، إلا أنها رفضت ومن ثم تم اللجوء إلى القضاء الذي طالب "أبل" بإدخال بعض التعديلات على هاتف آيفون، إلا أنها قامت بالاستئناف على هذا الحكم، وحاولت نقل هذه القضية إلى أروقة الكونجرس الأمريكي.

ختاماً، ترى الكاتبة أن الأمن السيبراني وتأمين المعلومات ضد الاختراق يواجه تحديات متعددة يتمثل أهمها في التطور السريع في قدرات المخترقين والارتباط بين جماعات المخترقين وبعض الدول، والاتصال الدائم بالإنترنت، خاصة في ظل انتشار تقنيات "انترنت الأشياء" وتصاعد التهديدات الأمنية التي قد تترتب على تقنيات التشفير الكامل.