اختراق: قصة كفاح أمريكا لتأمين المجال السيبراني

تشارلي ميتشل

Hacked: The Inside Story of America's Struggle to Secure Cyberspace

By: Charlie Mitchell Rowman & Littlefield Publishing Group, 301pp., $18.77, 2016, 1442255218

عرض: إيهاب خليفة، رئيس وحدة التطورات التكنولوجية - مركز المستقبل للأبحاث والدراسات المتقدمة

بعد عملية القرصنة الشهيرة التي تعرضت لها شركة سوني لإنتاج الأفلام في الولايات المتحدة من كوريا الشمالية، أثار تشارلي ميتشيل في كتابه أن التخوف الرئيسي الذي يهدد الأمن القومي الأمريكي يتمثل في الهجمات الإلكترونية والتي يمكن أن تستهدف البنية التحتية الصناعية والخدمية وشبكات الكمبيوتر ومحطات الطاقة وأنظمة الاتصالات والمواصلات، فكل شيء في الولايات المتحدة، بل والاقتصاد العالمي مرتبط بشبكات الكمبيوتر.

حروب المستقبل ضد الولايات المتحدة

يثير الكاتب إشكالية الأمن الإلكتروني في الولايات المتحدة، ويلقي بالمسؤولية على الحكومة والشركات الخاصة، ففي الوقت الذي كان يستعد فيه الكونجرس لإعلان خطوات تاريخية للأمن الإلكتروني الأمريكي، قام أحد المراهقين باختراق الإيميل الشخصي لمدير وكالة الاستخبارات المركزية أن يطلع على العديد من الوثائق والرسائل، سواء أكانت متعلقة بالأمن القومي الأمريكية أو حتى شخصية.

وفي أبريل 2009 نشرت صحيفة الوول ستريت جورنال خبراً عن اكتشاف فيروسات في شبكات الكمبيوتر تستهدف شبكة الطاقة الكهربائية في الولايات المتحدة، وأشارت إلى أن مصدر الهجمة يأتي من روسيا والصين وأماكن أخرى، وأنها "حرب المستقبل" ضد الولايات المتحدة كما سماها تشارلي ميتشيل.

كما أنه أعاد إثارة تخوف وزير الدفاع السابق "ليون بانيتا" من احتمالية تعرض الولايات المتحدة لبيل هاربر إلكتروني، يتسبب في تدمير البنية التحتية للدولة والاقتصاد، فإذا كانت الهجمات التي شنتها كوريا الشمالية استهدفت شركة سوني، فإنها يمكن أن تستهدف أيضاً القطاعات الحيوية والحرجة في الولايات المتحدة، وهو ما دفع الحكومة الأمريكية لأول مرة لمشاركة مؤشرات التعرض لهجمات إلكترونية بين المؤسسات الحكومية والخاصة في الولايات المتحدة. وعلى الرغم من الإجراءات التي اتخذها الكونجرس والحكومة الأمريكية لتدعيم الأمن الإلكتروني، يرى الكاتب أنها مازالت غير كافية، فالتهديدات الإلكترونية مازالت تأتي للولايات المتحدة بصورة أكثر شراسة من روسيا والصين وإيران وكوريا الشمالية والشرق الأوسط ومناطق أخرى غير معلومة حول العالم.

ويستعرض ميتشيل بعض البيانات المهمة المتعلقة بالأمن الإلكتروني، منها أن الشركات الخاصة تمتلك 85% مما يجب حمايته من الهجمات الإلكترونية في الولايات المتحدة، وأن عدد الشكاوى التي تلقاها مكتب التحقيقات الفيدرالية عام 2014 بلغ 269.422 شكوى، وأن الجرائم الإلكترونية تبلغ تكلفتها الاقتصادية حوالي 800 مليون دولار أمريكي. ويتساءل: هل الهجمات الإلكترونية أمر أكبر من قدرة الحكومة الأمريكية والقادة السياسيين والشركات الخاصة والمخترعين في مجال التكنولوجية على مواجهته؟

استراتيجية الأمن السيبراني

يستعرض الكاتب الجهود الأمريكية لتدعيم الأمن الإلكتروني في الولايات المتحدة، بداية من الرئيس بيل كلينتون الذي يعتبر أول رئيس يهتم بمسألة الأمن الإلكتروني، ثم جورج بوش الذي وضع أول مبادرة قومية خاصة بالأمن الإلكتروني، ثم يلقي مزيد من الضوء على جهود إدارة الرئيس أوباما في مجال الأمن الإلكتروني، والتي وضعت العديد من الخطط والاستراتيجيات الخاصة بمجال الأمن الإلكتروني، وتعاملت معه بنفس أهمية القضايا التقليدية كالهجرة مثلاً، في إطار من الشركات بين الحكومة والقطاع الخاص والمجتمع المدني.

ويثير الكاتب قضية غاية في الأهمية حول العلاقة الجدلية بين التشفير والأمن القومي، حيث طالب البعض بوضع إجراءات قانونية تسمح للحكومة الأمريكية بالحصول على الشيفرات من الشركات العاملة في مجال صناعة تكنولوجية المعلومات لتدعيم إجراءات الأمن القومي، ولكن يرى الكاتب أنه بفضل التشفير القوي للتعاملات الإلكترونية، وثقة المستخدمين في الحفاظ على خصوصياتهم، تطورت الأسواق الافتراضية الأمريكية على الإنترنت، وساهمت في تدعيم الاقتصاد الأمريكي، ومع ذلك تبقى تكلفة التشفير الجيد متمثلة في إمكانية استخدام بعض الإرهابيين للمواقع والخدمات المشفرة لتنفيذ مخططاتهم.

ويؤخذ على الكاتب هنا أنه ركز على الإجراءات والجهود القانونية التي اتخذتها الحكومات الأمريكية لتحقيق الأمن الإلكتروني الأمريكي، غافلاً الانتهاكات التي قامت بها هذه الحكومات سواء ضد الشعب الأمريكي أو ضد مستخدمي الإنترنت في العالم بصورة عامة، وهو ما كشفه إدوارد سنودن المتعاقد السابق مع وكالة الأمن القومي الأمريكي.