أرض الظلام: التاريخ السري للحرب السيبرانية

فريد كابلن

Dark Territory: The Secret History of Cyber War

By: Fred Kaplan

Simon & Schuster, 352 pp., $28.00, 2016, 9781476763255

عرض: سلمى العليمي، باحث بالمركز الإقليمي للدراسات الاستراتيجية

لا تعد الهجمات السيبرانية بالأمر الجديد، وهذا ما حاول الكاتب فريد كابلان التطرق له في كتابه "أرض الظلام: التاريخ السري للحرب السيبرانية" من خلال تسليطه الضوء على تاريخ الولايات المتحدة في تناول قضية الأمن السيبراني وجهود الحكومات الأمريكية المتعاقبة بداية من إدارة رونالد ريجان حتى إدارة أوباما في مواجهة التحديات الأمنية والثغرات التي عانتها لتأمين شبكاتها الإلكترونية ومؤسساتها الحيوية ضد الهجمات السيبرانية المتطورة.

ويعد هذا الكتاب من الكتب المهمة في تاريخ الأمن السيبراني لأن كابلن استند فيه إلى مقابلات مع أكثر من 100 شخصية قيادية أمريكية من أمناء مجلس الوزراء وصانعي القرار داخل البيت الأبيض ووزارة الدفاع الأمريكية ووكالة الأمن القومي وخبراء ومحللين.

بداية الاهتمام بالأمن السيبراني

أشار الكاتب إلى أن الاهتمامات الأولى بهذا الأمر قد بدأ في عام 1967، وذلك عندما قام المهندس ويليس وار (Willis Ware) بإعداد ورقة بحثية بعنوان: "الأمن والخصوصية في نظم الكمبيوتر"، والتي أشار فيها إلى خطورة مشاركة الملفات، وشبكات الكمبيوتر المتصلة بالإنترنت، وقد أعقب ذلك مشاهدة الرئيس الأمريكي رونالد ريغان لفيلم الخيال العلمي الأمريكي "ألعاب الحرب" (War Games) عام 1983، والذي تدور قصته حول شاب تمكن من اختراق الشيفرة الأمنية لقيادة الدفاع الجوي الأمريكية، فقد أثار هذا الفيلم فضول الرئيس الأمريكي، ودفع إلى تبني أول استراتيجية وطنية لتقليل أجهزة الكمبيوتر.

وبداية من عام 2009 تم إنشاء وحدة تتعلق بالأمن السيبراني داخل وزارة الدفاع الأمريكية وخصص لها 7 مليارات دولار سنوياً، ومن المتوقع أن يصل عدد أعضاء تلك الوحدة بنهاية عام 2016 إلى 14 ألف فرد.

اكتشاف الثغرات الأمنية

في يونيو 1997 أطلقت وكالة الأمن القومي الأمريكية تدريباً باسم "المتلقي المؤهل" (Eligible Receiver)، والذي يستهدف اختراق شبكات الكمبيوتر التابعة لوزارة الدفاع باستخدام معدات وبرمجيات متاحة تجارياً، ويعد ذلك أول اختبار لقياس مدى استعداد الجيش الأمريكي للتصدي لهجوم إلكتروني، وهو ما كشف عن وجود ثغرات لدى أنظمة الدفاع الإلكترونية.

فبعد عام من تطبيق ذلك التدريب وقع اختراق حقيقي لشبكات قاعدة أندروز الجوية على يد مجموعة من طلاب ولاية سان فرانسيسكو الأمريكية، حيث تم اختراق موقع الإدارة والاستحواذ على كافة أسماء المستخدمين وكلمات المرور، وذلك بسبب استغلال عيب شهير في أنظمة يونكس (UNIX) المستخدمة في القاعدة.

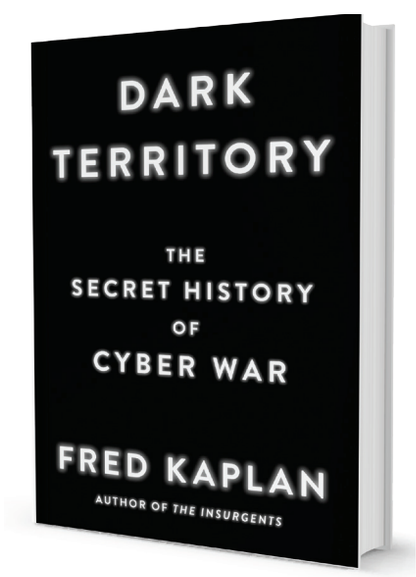
بداية الحروب الإلكترونية

أشار كابلن إلى أن الغزو الأمريكي للعراق 1991 في عهد إدارة بوش كان النواة الأولى في استخدام التقنيات الإلكترونية عندما تم تعطيل شبكة الاتصالات للجيش العراقي، وبداية من عام 2007 دخلت الحروب الإلكترونية حقبة جديدة بزغت باختراق الجيش الأمريكي حسابات البريد الإلكتروني للمتمردين في العراق والوصول إلى حسابات قيادات من تنظيم القاعدة، وقيام روسيا بشن هجوم إلكتروني على الموقع الإلكتروني لحكومة إستونيا وتكبدها خسائر مالية عديدة.

ومؤخراً، هاجمت كوريا الشمالية شبكة شركة سوني في 2015، الأمر الذي طرح تساؤلات عدة حول مدى إمكانية توظيف الهجمات الإلكترونية لإلحاق الضرر بمؤسسات البنية التحتية، نظراً لاعتمادها على شبكات الكمبيوتر في تشغيلها.

الخصوصية والأمن القومي

اعتبر كابلن أن على الولايات المتحدة التعامل مع إشكالية المحافظة على حريات وحقوق الشعب الأمريكي في ضوء قيام الأجهزة الأمنية بالتجسس على رسائل البريد الإلكتروني والسجلات الهاتفية لمواطنين أمريكيين دون الحصول على إذن قضائي، التي كشف عنها إدوارد سنودن في تسريباته، ولذلك يطالب كابلن بأهمية إشراك الرأي العام الأمريكي واطلاعه على الأنشطة المخابراتية للدولة مع الحفاظ على الحريات الشخصية للأفراد.

ختاماً، يشير كابلن إلى أن الحروب الإلكترونية تختلف عن الحروب التقليدية المعلوم أطرافها والتي يمكن التنبؤ بنتائجها، بينما الحروب الإلكترونية استطاعت خلق ساحة جديدة من المواجهات الافتراضية بين الدول لا يمكن التنبؤ بحجم أضرارها.

وعلى الرغم من أهمية الكتاب، فإنه أغفل تناول مخاطر الإرهاب الإلكتروني على الرغم من تعرض حساب توتير الخاص بالقيادة العسكرية الأمريكية في 2015 إلى اختراق لمدة 30 دقيقة من جانب مجموعة أطلقت على نفسها الخلافة الإلكترونية.