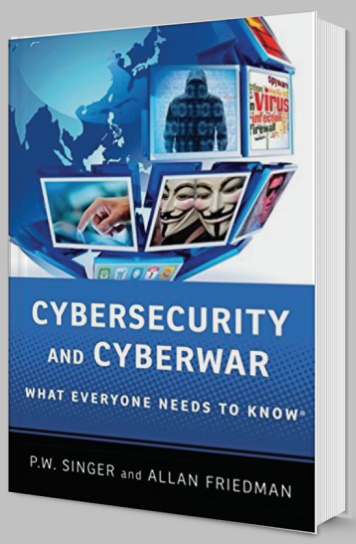
مؤسسة محمد بن راشد آل مكتوم للمعرفة
MOHAMMED BIN RASHID AL MAKTOUM KNOWLEDGE FOUNDATION

كتـــاب في دقـــائق
2017
ملخصات لكتب عالمية تصدر عن مؤسسة محمد بن راشد آل مكتوم للمعرفة

الأمن الإلكتروني والحروب الإلكترونيَّة

دليلٌ أساسيٌّ لما عليك معرفته



تأليف
بي دبليو سينجر
ألان فريدمان

138

في ثوانٍ...

يسرُّني أن أعودَ إليكم مع أعدادِ هذا الشهر؛ شهر الوحدة والإنجازات، مع الذكرى السادسة والأربعين على وحدة الوطن وتلاحم الشعب مع قيادته، ومع تقدُّم دولتنا الذكية في مراتب التنافسية العالمية، واحتلال المراكز الأولى في مجالات التميز الحكومي والمؤسسي ومؤشرات التنمية والسَّعادة، ونحن نقدِّمُ إليكم ملخصات أفضل الكتب العالمية الرائدة.

في ملخَّص كتاب: «اسلُك الطريق الصحيح: كيف نأخذ بالأسباب المدهشة التي تقودنا إلى النجاح» يؤكِّدُ المؤلف «إريك باركر» أنَّ القادة نوعان: عاديون واستثنائيون،حيث يسلك القادة العاديون القنوات الرسميَّة ويحصلون على الترقيات ويلتزمون بالقواعد ويُلبُّون التوقُّعات. أمَّا القادة الاستثنائيون فهم الذين يسلكون طرقاً غير مألوفة، ويستثمرون الفرص، ويفاجئون العالم بإنجازات غير مسبوقة، ويتخذون قرارات غير متوقَّعة، ولذلك فهم الذين يصنعون الفارق من خلال أفكارهم المتحرِّرة، فيقودون مجتمعاتهم ومؤسَّساتهم إلى آفاق أوسع من الفرص، ولا سيِّما في ظلِّ اقتصاد العولمة شديد التنافسيَّة. وهؤلاء هم القادة المبادِرون والإيجابيُّون والمؤثِّرون.

وفي ملخَّص كتاب: «أموال وأحوال: كيف يتعلَّم الاقتصاد من العلوم الإنسانيَّة» يُسبغ المؤلفان «جاري ساول مورسون، ومورتون شابيرو» نظرةً إنسانية جديدة على علم الاقتصاد؛ لأنَّ غرسَ المنهج الإنساني في الاقتصاد يجعلُ نماذجَه أكثرَ واقعيَّة، وتوقُّعاته أكثرَ دقَّة، وسياساته أكثر فاعليَّة وعدلاً. وهذا يعني أنه يمكن للاقتصاد أن يستفيدَ من فهم سلوك الناس واحترام فلسفاتهم الأخلاقية، ومن الفهم العميق لمعنى ودور الثقافة. ولكي نكونَ عمليين وعلميين أيضاً، فالمطلوب هو أن يستفيدَ الاقتصاديُّون من هاتين الفكرتين من دون أن يتخلَّى الاقتصاد عن إنجازاته العظيمة، وعبر علم اقتصاد إنساني؛ يسمح لكلِّ مجال بالحفاظ على سماته المميَّزة. ويدير حواراً بين علمين اجتماعيين ومجالين كنَّا نعتبرهما نهجين مختلفين للمعرفة. ومع بدء مثل هذا الحوار الأخلاقي والخلَّاق، فإنَّ المزيد من الأفكار الجديدة والإبداعات المفيدة ستفاجئنا وتُلهمنا في رحلتنا لمواكبة المستقبل واستشرافه.

وفي ملخَّص كتاب: «الأمن الإلكتروني والحروب الإلكترونيَّة: دليلٌ أساسيٌّ لما عليك معرفته» يؤكِّدُ المؤلفان «بي دبليو سينجر، وألان فريدمان» أنَّ مشكلات الحروب الإلكترونية وأمن المعلومات ليست فنيَّة وتقنيَّة فقط، بل هي في منشئها مشكلاتٌ تنظيميَّةٌ وقانونيَّةٌ واقتصاديَّةٌ واجتماعيَّةٌ، ولكنَّ المهمَّ أنَّنا عندما نفكِّر في الأمن المعلوماتيِّ، يجب أن نعرفَ شروطَه ونفهمَ حدودَه؛ لأنه يُكلِّف مالاً ووقتاً وإمكانات وحريَّات كذلك. ولهذا فإننا نحتاجُ إلى استجابات مرنة ومتنوعة لنواجهَ المخاطرَ التي تتهدَّدُ السِّريَّة والإتاحة والمرونة والسلامة، ولا سيما أنَّ الأمنَ المُطلقَ ليس له وجودٌ، فلا يوجدُ حلٌّ سحريٌّ يقي من جميع المخاطر. وهنا يبرزُ دورُنا وتتجلَّى مسؤوليَّتُنا كمواطنين مبادرين في العالم الافتراضي، والعالم الواقعي على حدٍّ سواء.

جمال بن حويرب
المدير التنفيذي لمؤسسة محمد بن راشد آل مكتوم للمعرفة

جميعنا يعاني وكلُّنا مسؤول

لو عُدنا بالذاكرة إلى الوراء جيلاً واحداً، لتذكَّرنا أنَّ مصطلح «الفضاء الإلكتروني» كان مجرَّد خيال علمي، إذ كان يُستخدَم في وصف شبكة ناشئة من أجهزة الكمبيوتر المنتشرة في بعض الجامعات، أمَّا اليوم فقد صارت حياتنا؛ بدءاً من التواصل ومروراً بالتجارة ووصولاً إلى الصراع، تعتمد بصورة جوهريَّة على الإنترنت، حتَّى صارت القضايا الأمنيَّة تمثِّل تحدِّياً للجميع: فالساسة يُواجهون الجرائم الإلكترونيَّة وقضايا الحريَّة على شبكة الإنترنت، وصار المهندسون يدافعون عن بلادهم ضد أشكال جديدة من الهجمات من دون أن يرتدوا ملابس الجنرالات، وقادة الأعمال يَدفعون عن مؤسَّساتهم مخاطر لم يكن أحد يتخيَّلها في وقت من الأوقات؛ والمحامون وفلاسفة الأخلاق يضعون أطراً جديدة لما يعتبرونه صواباً أو خطأً. ونحن أيضاً نواجه أسئلة جديدة في كلِّ شيء؛ بدءاً من حقوقنا ومسؤوليَّاتنا كمواطنين في العالم الافتراضي، والعالم الواقعي على حدٍّ سواء.

بعد أن صار «الفضاء الإلكتروني» أمراً واقعاً، نما حجم المخاطر نمواً هائلاً، إذ تعرَّض 97 في المائة من المؤسَّسات المُدرجة على قائمة مجلة «فورتشن 500» للقرصنة، وأعدَّت أكثر من مائة حكومة العدَّة لخوض معارك في النطاق الإلكتروني. وبسبب هذه المخاوف، ظهر ما يسمَّى «الأمن الإلكتروني»، فصار من أسرع المجالات نمواً وتشابكاً، وبدأت الحكومات بابتكار إدارات جديدة للدفاع عن فضائها وأسرارها. ويرى الدكتور «جو ناي» صاحب نظريَّة «القوة الناعمة» والعميد السابق لكليَّة كينيدي الحكوميَّة في «جامعة هارفارد» أنَّه إذا بدأ المستخدمون يفقدون الثقة بسلامة وأمن الإنترنت والمعلومات، فإنَّهم سينسحبون من الفضاء الإلكتروني مقايضين الرفاهية بالأمن على حدِّ تعبيره، وهذا يعني أنَّ المخاوف بشأن الأمن الإلكتروني تؤثِّر في أفكارنا المتعلِّقة بالخصوصيَّة، ولهذا سمحنا بمراقبة المحتوى في المؤسَّسات الحكوميَّة والخاصَّة، وفي منازلنا أيضاً، الأمر الذي من شأنه أن ينتهك الحقوق الاقتصاديَّة والاجتماعيَّة وحقوق الإنسان، بسبب التواصل المفرط بين شبكات المعلومات حول العالم.

تعريف الفضاء الإلكتروني

الفضاء الإلكتروني هو عالم مستخدمي الشبكات الإلكترونيَّة المُحوسَبة الذي نُخزِّن فيه المعلومات ونتبادلها على شبكة الإنترنت، وبدلاً من البحث عن التعريف الأمثل والأدقِّ للفضاء الإلكتروني، من المفيد تحليل ما تسعى التعريفات إلى توضيحه، فهناك سمات لا تُشكِّل الفضاء الإلكتروني فحسب، بل تجعله فريداً أيضاً، فالفضاء الإلكتروني هو بيئة معلوماتيَّة تتشكَّل من البيانات الرقميَّة التي تُنتَج وتُخزَّن وتُرسَل وتُستقبَل. فهو ليس مكاناً مادياً فقط، ولذا فهو يتحدَّى التأطير بأيِّ بعد ومقياس مادي وأحادي أياً كان نوعه. والفضاء الإلكتروني ليس افتراضياً على نحو خالص، فهو يشمل أجهزة حاسوب تُخزِّن البيانات، إضافة إلى نُظم وبنية أساسيَّة تسمح له بالتدفُّق، وهذا يشمل الأجهزة المتصلة بشبكات الإنترنت المغلقة، والأجهزة المتنقِّلة، والألياف البصريَّة أو الضوئيَّة، والاتصالات الفضائيَّة اللاسلكيَّة، وكلِّ النظم الرقميَّة الذكيَّة.

العالم الرقمي

نحن نستخدم مصطلح «الإنترنت» لنصف العالم الرقمي، بما في ذلك الأشخاص الذين يجلسون خلف أجهزة الحاسوب ويعيشون في عالم لا ينقطع من التواصل بكلِّ اللغات ولمختلف الغايات. ومن أهمِّ خصائصه أنَّ أنظمته وتقنياته من صنع البشر. ويمكن من هنا تعريف الفضاء الإلكتروني استناداً إلى العالم المعرفي والعالم المادي والرقمي معاً، كما أنَّ التصوُّرات والمفاهيم مهمَّة، حيث تستند إليها الهياكل الداخليَّة للفضاء الإلكتروني في كلِّ شيء، بدءاً من الطريقة التي تُخصَّص بها الأسماء ضمن الفضاء الإلكتروني، ووصولاً إلى الأشخاص والجهات التي تدير البنية الأساسيَّة وتضع تشريعاتها وقوانينها.

السيادة والملكيَّة والجنسيَّة

هناك نقطة مهمَّة كثيراً ما نُسيء فهمَها، وهي أنَّ الفضاء الإلكتروني الذي نعتبره عالمياً، ليس «مُنعدِم الجنسيَّة»، أو «مشاعاً»، بل يُستخدم كلا المصطلحين كثيراً من جانب الحكومات ووسائل الإعلام، فقد تمَّ تقسيم الكرة الأرضيَّة إلى نطاقات وأقاليم نُطلق عليها «أمماً» أو «دولاً»، ثمَّ قسَّمنا الجنس البشري إلى مجموعات يُطلق عليها «جنسيَّات» أو «قوميَّات». ونفس هذا التقسيم يسري على الفضاء الإلكتروني، فهو يعتمد على بنية ماديَّة ومستخدمين يرتبطون جغرافياً، ومن هنا فهو يخضع لمفاهيمنا البشريَّة مثل السيادة والجنسيَّة والملكيَّة. ورغمَّ أنَّ أقسام الفضاء الإلكتروني واقعيَّة وذات أهمِّية، فإنَّها أيضاً خطوط وهميَّة وتخيُّليَّة مثل الحدود التي تفصل الولايات المتحدة عن كندا، أو كارولاينا الشماليَّة عن كارولاينا الجنوبيَّة، والهند عن

الصين، وهكذا. فالجمع بين التكنولوجيا والبشر الذين يستخدمونها يتغيَّر على نحو دائم ويتغيَّر معه حجم الفضاء الإلكتروني ونطاقه، وصولاً إلى القواعد الفنيَّة والسياسات التي تسعى لتوجيهه. ويرى الخبراء أنَّ جغرافيَّة الفضاء الإلكتروني أكثر قابليَّة للتغيُّر من البيئات الأخرى. فمن الصعب أن تتحرَّك الجبال والمحيطات من أماكنها، لكنَّ بعض مكوِّنات وأجزاء الفضاء الإلكتروني يمكن تشغيلها أو إيقافها بضغطة زر. وتبقى الخصائص الأساسيَّة كما هي، لكنَّ الطبوغرافيَّة في تدفُّق مستمر. فالفضاء الإلكتروني اليوم، هو نفسه الفضاء الإلكتروني الذي عرفناه في عام 1982، وهو يختلف فقط من حيث سعة التخزين وسرعة التبادل، وسيولة التدفُّق، وسهولة الاستخدام.

وفي حين كان الفضاء الإلكتروني في وقت من الأوقات مجرَّد عالم للاتصال ثمَّ للتجارة الإلكترونيَّة التي تقترب مبيعاتها من عشرة تريليونات دولار في هذا العام، فقد اتسع هذا الفضاء ليشمل ما نُطلق عليه «البنية الأساسيَّة الحيويَّة»، ويُقصد بها القطاعات الأساسيَّة التي تستند إليها حضارتنا الحديثة، بدءاً من الزراعة وتوزيع الغذاء، ووصولاً إلى النشاط المصرفي والرعاية الصحيَّة والنقل والماء والطاقة. كلُّ هذه القطاعات التي كانت في وقت من الأوقات مستقلَّة ومنفصل بعضها عن بعض، أصبحت مرتبطة ومتصلة بالفضاء الإلكتروني عن طريق ما يسمَّى تكنولوجيا المعلومات، ويحدث ذلك غالباً من خلال ما يُعرف باسم «سكادا» ومعناه «نظام التحكُّم الإشرافي وتحصيل البيانات». فهناك أنظمة حاسوبيَّة ترصد عمليَّات البنية الأساسيَّة الحيويَّة الأخرى وتضبط ما يحدث لها من تغيير وتتحكَّم فيها. ويتحكَّم القطاع الخاص بنحو 90% تقريباً من البنية الأساسيَّة الحيويَّة الأمريكيَّة، وتستخدم المؤسَّسات التي تعتمد على الفضاء الإلكتروني من أجل تحقيق التوازن في كلِّ شيء؛ بدءاً من مراقبة وتحديد مواصفات ونسب تنقية المياه في مدينتك، والتحكُّم في تدفُّق الغاز اللازم لتدفئة منزلك، وليس انتهاءً بالمعاملات الماليَّة التي تحافظ على استقرار أسعار العملات في مختلف دول العالم. ورغم كلِّ هذه الأهمية، فإنَّ الإنسان الذي اخترع وطوَّر وأطلق العنان للإنترنت، لم يحترم هذه القيمة الحضاريَّة، حتَّى صار الإنترنت مصدراً للحبِّ والحرب، والربح والخسارة، والإعمار والدمار.

الهويَّة والتوثيق

الكيفيَّة التي نستطيع بها تحديد وتوثيق أنشطة مباشرة على شبكة الإنترنت، تختلف عن الكيفيَّة التي تقودنا إليها فطرتنا الإنسانيَّة، فترانا متحفِّظين ومحافظين وميَّالين إلى السريَّة، وترك جزء من هويَّاتنا غامضاً وملتبساً. فنحن نقدِّم بياناتنا لبعض المؤسَّسات، ونحجبها عن أخرى؛ ونتعامل مع جهات بثقة، وننظر إلى جهات أخرى بشيء من الريبة. ففي حين نسوِّق لمواقعنا وندفع مقابل إشهار ماركاتنا، نرقِّي أرقام حساباتنا، وأحياناً بأسماء سريَّة، حتَّى نثق بمن نتواصل معه، أو نثق بالنظام الذي يربطنا معاً.

فيما يتعلَّق بالأمن الإلكتروني، فإنَّ الهويَّة الرقميَّة هي توازن بين حماية المعلومات ومشاركتها. فالحدُّ من المعلومات التي تُفصح عنها لا يمثِّل أهمية بالنسبة إلى الخصوصيَّة فحسب، بل يمنع الآخرين كذلك من الحصول على معلومات يمكن أن يستخدموها في عمليَّات تدليس أو غشٍّ ممنهَجة يُحتال فيها على التوثيق بطرق شديدة التعقيد. وفي نفس الوقت، يتضمَّن كلُّ نظام عدداً من المُحفِّزات والإغراءات لزيادة مقدار البيانات التي يجمعها بهدف استخدام تلك البيانات لخدمة أهدافه الخاصَّة.

ما الأمن؟

لا يقتصر الأمن في معناه الأشمل على فكرة عدم التعرُّض للخطر كما نتصوَّر، لأنَّه يرتبط دائماً بوجود خصم أو غريم. بهذا، يبدو الأمر أشبه ما يكون بالحرب أو التجارة؛ فأنت بحاجة إلى طرفين على الأقلِّ كي يصبح الأمر حقيقياً. قد تتعرَّض الأشياء للكسر وقد تُرتكب الأخطاء لكنَّ المشكلة الإلكترونيَّة لا تصبح مشكلة أمن إلكتروني إلا إذا سعى الخصم لتحقيق مكاسب من هذا النشاط، وقد يتمثَّل هذا المكسب في الحصول على معلومات خاصَّة أو تدمير النظام أو منع استخدامه من قبل أصحابه وعملائه وشركائه، أو تدميره نهائياً وإزالته من الوجود.

ليست كلُّ مشكلات الأمن فنيَّة أو تقنيَّة، بل هي مشكلات تنظيميَّة وقانونيَّة واقتصاديَّة واجتماعيَّة أيضاً، لكنَّ الأهم أنَّنا عندما نفكِّر في الأمن، نحتاج إلى وضع شروطه وتعريف حدوده. فأي مكسب أمني يتضمَّن نوعاً من المقايضة، فالأمن يُكلِّف مالاً ووقتاً وإمكانات وحريَّات وغير ذلك، وبالمثل تتطلَّب المخاطر المختلفة التي تهدِّد السريَّة والإتاحة والمرونة والسلامة استجابات مختلفة، فالأمن المُطلق ليس له وجود، فلا يوجد حلٌّ سحري يقي من جميع المخاطر.

ما المخاطر؟

عند مناقشة الحوادث الإلكترونيَّة أو المخاوف من وقوع هجمات محتملة، من المهمِّ أن نفصل بين فكرة الانكشاف والتسريب، وفكرة التهديد. فالباب المفتوح يمثِّل ثغرة أو انكشافاً على خطر ما، لكنَّه لا يمثِّل تهديداً ما دام لا أحد يريد الدخول. والعكس صحيح، فإنَّه يمكن أن تتمخَّض عن ثغرة واحدة تهديدات عديدة: فالباب المفتوح يمكن أن يمنح الإرهابيِّين فرصة وضع قنبلة، وقد يسرق منافسوك أسرارك التجاريَّة، وقد يستولي اللصوص على سلع قيِّمة، أو يدمِّر المخرِّبون ممتلكاتك، وقد يتسرَّب أو يُهرَّب فيروس إلى نظام معلوماتك ويشوِّش على أداء شبكات العمل، ويربك المؤسَّسة كلَّها بلمح البصر.

العنصران الحاسمان في تعريف التهديدات والمخاطر هما الفاعل والنتيجة. الاعتراف بالفاعل يدفعنا إلى التفكير بطريقة استراتيجيَّة بشأن التهديدات أو المخاطر. ويمكن أن يلتقط الخصم ويختار ثغرة يستغلُّها من أجل تحقيق مأرب ما، وهذا يعني ضمنياً أنَّه لا يكفي سدُّ مجموعة الثغرات المعرَّضة لتهديد معيَّن، ولكن ينبغي علينا إدراك أنَّ التهديد قد ينشأ بسبب أفعالنا الدفاعيَّة.

هناك أنواع الهجمات الخطرة، ومن السهل أن تنساق وراء مانشيتات وسائل الإعلام كي تجمع كلَّ التهديدات في كلمة واحدة مثل مصطلح «قراصنة» مثلاً، إذ يعتبر هدف المهاجم نقطة الانطلاق عند تعريف وتصنيف المخاطر.

الحالات

في بعض الحالات يأتي الخطر من الداخل، فحالات مثل «برادلي مانينج» و«ويكيليكس» و«إدوارد سنودن» وفضيحة وكالة الأمن القومي الأمريكي تسلِّط الضوء على «الخطر الداخلي» الذي يُعدُّ عظيماً في تأثيره، لأنَّ الفاعل يعرف ثغرات النظم، ويعرف أسرار وشيفرات الحماية، وقد يكون أحد المشاركين في تصميمها. فالمطَّلعون على بواطن الأمور يمكن أن يمتلكوا رؤى أفضل بكثير بشأن ما هو ذو قيمة، وما هي أفضل طريقة لتعزيز هذه القيمة سواء أكانوا يحاولون سرقة أسرار أم تخريب أم تعطيل تنفيذ عمليَّة إلكترونيَّة مهمَّة.

ومن المهمِّ التفكير فيما إذا كان الفاعل أو مصدر التهديد يريد مهاجمتك أنت بالذات، أم إنه يهاجم الجميع، أم إنه يمارس لعبة إلكترونيَّة ويراهن أصدقاءه على اختراق نظامك الإلكتروني من أجل التسلية، فبعض الهجمات تستهدف نظماً بعينها لأسباب معيَّنة، في حين قد يسعى خصوم آخرون لتحقيق هدف معيَّن بصرف النظر عمَّن يتحكَّم فيه. فالبرمجيَّات الخبيثة غير الموجَّهة يمكن أن تضرب جهازاً حيوياً من خلال البريد الإلكتروني، وأن تبحث عن بيانات بطاقة ائتمانيَّة مخزَّنة، مع حفظ تلك البيانات لصاحبها من دون تدخُّل العنصر البشري في العمليَّة. الاختلاف الجوهري في تلك الهجمات الرقميَّة الذكيَّة يتعلَّق بالتكلفة من وجهة نظر المهاجم والمدافع، فمن منظور المهاجم، تقلِّل الأتمتة التكلفة فلا يضطرُّ القائمون على حماية النمو إلى الاستثمار في جميع المهام المطلوبة بدءاً من اختيار الضحيَّة، ومروراً بتحديد الهدف، ووصولاً إلى تنسيق وتنفيذ الهجوم. وفي حالة كهذه لا تزيد تكلفة المهاجم بصرف النظر على عدد الضحايا الذين يستهدفهم. أمَّا الهجوم الموجَّه فإنَّه، على الجانب الآخر، يمكن أن يؤدِّي إلى زيادة كبيرة في التكاليف مع ارتفاع عدد الضحايا. فحتَّى يكون المهاجم على استعداد للاستثمار في هجمات موجَّهة، يجب أن يحقِّق عائداً متوقَّعاً من كلِّ ضحيَّة. وعلى النقيض من ذلك، يمكن أن تحقِّق الهجمات الذكيَّة والتلقائيَّة هوامش ربح أقلَّ بكثير.

الاحتمالات

هناك ثلاثة احتمالات فقط لما يمكن فعله بأيِّ نظام إلكتروني محوسب: إمَّا سرقة بياناته، وإمَّا إساءة استخدام وتشويش بيانات التوثيق والتحقُّق من الهويَّة، أو السيطرة عليه بالكامل. وبسبب اعتمادنا الكلِّي على نظم المعلومات، فإنَّ الفاعل يمكن أن يُلحِق الكثير من الضرر عن طريق ارتكاب أيِّ فعل من الأفعال الثلاثة المذكورة، فسرقة البيانات يمكن أن تكشف عن خطط استراتيجيَّة لدولة من الدول، أو تدمِّر قدرة قطاع بأكمله وتحرمه من المنافسة. وسرقة بيانات التوثيق يمكن أن يمنح الفاعل إمكانيَّة تغيير أو تدمير البرمجيَّات والبيانات ما يؤدِّي إلى تبديل في كشوف الرواتب أو طمس أدلَّة أو تدليس وقائع. والاستيلاء على الموارد يمكن أن يمنع مؤسَّسة ما من الوصول إلى العملاء أو أن يحرم جيشاً من الجيوش القدرة على التواصل. ومثلما تتطوَّر التهديدات، يجب أن تتطوَّر استجاباتنا لها، إذ يمكن التخفيف من آثار بعضها باتخاذ إجراءات بسيطة وتغيير السلوك أو بتكرار تعديل معطيات النظام لمواصلة إخفاء تعديلات الثغرات أو الحيلولة دون ظهورها من خلال ابتكار وتطبيق تقنيات جديدة. وهناك ثغرات عديدة يمكن طمسها وإلغاؤها بمجرَّد إعادة هيكلة النظام ككل، أو تغيير الطريقة التي نستخدمها بها، فكيف يمكن أن يتمَّ ذلك؟

أساليب الدفاع والحماية

إذا كان تأمين نظام تشغيل حديث أمراً صعباً، فإنَّ ثمَّة اتجاهاً بديلاً يحاول منع البرمجيَّات الخبيثة من الوصول إلى حاسوبك عبر الشبكة. وأبسط شكل من أشكال الدفاع الإلكتروني هو «الجدار الناري»، وهو نظامٌ يوفِّر حمايةً للشبكة عبر ترشيح البيانات المُرسَلة والمُستقبَلة بناءً على قواعد حدَّدها المستخدم. الهدف من بناء وتشغيل الجدار الناري هو تقليل أو إزالة الاتصالات الشبكيَّة غير المرغوب فيها، والسماح في الوقت نفسه للاتصالات «الشرعيَّة» أن تُرسَل وتُستقبَل بحريَّة.

الجدار الناري عبارة عن مرشِّحات تسمح بالنشاط المصرَّح له على الشبكة؛ والطبقة التالية من الدفاع هي مجموعة من المجسَّات التي تبحث عن السلوكيَّات المخالفة، فأنظمة كشف التسلُّل توجد على المستوى الحاسوبي أو على الشبكة، وهذه الأنظمة عبارة عن برامج أو أجهزة مصمَّمة للكشف عن محاولات الوصول إلى نظام الحاسب الآلي غير المرغوب بها، أو محاولة تعطيل النظام بوجه عام والتلاعب به، وذلك من خلال شبكة الإنترنت. ويمكن لهذه المحاولات أن تَستخدِم أشكالاً عدَّة للهجمات، مثل: اختراق الحماية التي تتعلَّق بحقوق النسخ أو الطبع، أو استخدام برامج ضارَّة وما شابه ذلك. نظام كشف التسلُّل وحده، لا يمكنه كشف الهجمات ضمن حركة مرور مُشفَّرة، فهذا النظام يستخدم للكشف عن أنواع عدَّة من التصرُّفات المريبة التي يمكن أن تنتهك نظام الحماية الأمني وتُفقده موثوقيَّته. وهذا يتضمَّن هجمات الشبكة الموجَّهة إلى الخدمات الضعيفة، والبيانات التي تدفع الهجمات على التطبيقات، والدخول غير المصرَّح به، والوصول إلى الملفَّات الحسَّاسة، والبرامج الضارَّة. ومثل البرامج المضادَّة للفيروسات فإنَّ لكلٍّ من هذه الأنظمة ثمنها. فإضافة إلى تكلفتها الماديَّة، فإنَّها تكلِّف وقتاً وموارد أداء داخل منظومة العمل، فضلاً عن تركيبها وتفعيلها على كلِّ جهة، لا سيَّما إذا كان يتعيَّن على النظام تقييم جميع حالات المرور الواردة على شبكة ضخمة على نحو فوري.

ما الهجوم الإلكتروني؟

لتعرف ما يعنيه الهجوم الإلكتروني، عليك أولاً أن تعرف أنواع الهجمات التقليديَّة. تستخدم الهجمات الإلكترونيَّة وسائل مختلفة. فعوضاً عن استخدام قوَّة حركيَّة (كاستخدام قبضة اليد أو السيف أو البندقيَّة) تستخدم الهجمات الإلكترونيَّة وسائل رقميَّة، أو إجراءات وعمليَّات حاسوبيَّة من نوع ما، فالهجوم الإلكتروني ليس مقيَّداً بالجوانب الماديَّة المعتادة في حالة الهجمات التقليديَّة. ففي الفضاء الإلكتروني، يمكن أن يتحرَّك الهجوم حرفياً بسرعة الضوء دون أن تقيِّده الحدود الجغرافيَّة أو الحواجز السياسيَّة. كما أنَّ خروجه عن قيود القوانين الماديَّة يعني أنَّه يمكن أن يوجد في أماكن متعدِّدة في الوقت ذاته، وهذا يعني أنَّ الهجوم سيصيب أهدافاً متعدِّدة، في أماكن مختلفة، في الوقت ذاته.

ويمثِّل الهدف نقطة الاختلاف الثانية بين الهجوم الإلكتروني والهجمات التقليديَّة. فعوضاً عن التسبُّب في ضرر مادي مباشر، يستهدف الهجوم الإلكتروني حاسوباً آخر إضافة إلى المعلومات التي يحتويها. والنتائج المبتغاة من وراء هذا الهجوم قد تكون إلحاق الضرر بشيء مادي، لكنَّ الضرر ينجم أولاً عن حادث ما في العالم الرقمي.

انطلاقاً من هذين الاختلافين الجوهريَّين، تنبثق جميع الطرق الأخرى التي يبدو بها الهجوم الإلكتروني مختلفاً عن الهجوم المادي، فعادةً ما تكون الهجمات الإلكترونيَّة أكثر صعوبة في معرفة مصدرها. وأحياناً يُطلق القنَّاصة الرصاص من بنادقهم المصمَّمة بدقَّة

بحيث لا تُكتشف، في حين يوقِّع بعض منفذي الهجمات الإلكترونية بأسمائهم في برمجيَّاتهم الخبيثة كي يتمكَّنوا من شنِّ هجومهم، وبالمثل يكون تأثير الهجوم المادي أسهل في التنبُّؤ به من الهجوم الإلكتروني. فمن الممكن أن يُطلِق أحدهم قنبلةً موجَّهةً بالليزر بشكل دقيق وهو يعرف مدى الدمار الذي سيحدثه الانفجار. أمَّا في حالة الفيروس الحاسوبي، فمن الصعب أن نعرف أيَّ جهازٍ حاسوبي سيصيبه الفيروس قبل غيره، وإذ قد تؤدِّي القنبلة الحقيقية دون قصد إلى تفجير خطوط الغاز والكهرباء الممتدَّة وغير المرئيَّة وانهيار المبنى، فإن الهجمات الفيروسية؛ مثل فيروس «ستكسنت»، مصمَّمة لإصابة أهدافها بدقة لا تخطئ أبداً.

علاوة على ذلك، ترتبط تكاليف شنِّ هجوم مادي بشراء أسلحة ومواد فعليَّة وتخزينها ثم نشرها وإطلاقها، في حين تترتَّب تكاليف الهجمات الإلكترونيَّة على عمليَّات البحث والتطوير. وهي في هذا تشبه مشروعات تطوير الأسلحة النووية التي تقوم على البحث والتطوير المستمر أكثر من اعتمادها الأسلحة التقليدية. ولهذا فإن الفارق الوحيد بين الهجمات الإلكترونيَّة وغيرها من الهجمات هو وسائلها الرقميَّة وأهدافها الإلكترونيَّة.

فكيف يمكننا التمييز بين الهجمات الإلكترونيَّة؟ لقد تطوَّرت تلك الهجمات بدايةً من تعطيل الخدمة، حيث يتمُّ إغراق وشلُّ النظام المُستهدف بكمٍّ هائل من الطلبات من شبكات أخرى، إلى «ستكسنت» حيث يمكن أن يسبِّب مثل هذا البرنامج الخبيث تعطيل الأجهزة في مختبر نووي وخروجه عن السيطرة، فالأمر أشبه ما يكون بتصنيف كلِّ شيء في قوائم بدءاً من مجموعة من أطفال الجيران الذين يقرعون جرس الباب ويهربون، وصولاً إلى تدمير المقاومة النرويجيَّة للأبحاث النوويَّة النازيَّة إبَّان الحرب العالميَّة الثانية.

ويمكن تقسيم الهجمات الإلكترونيَّة كما يلي:

هجمات الإتاحة: وهي الهجمات التي تمنع الوصول إلى شبكة من الشبكات، سواءً عن طريق غمرها بالزيارات الوهميَّة، أو حرمانها من الخدمة وفصلها عن شبكة الإنترنت وتعطيل منظومتها الهندسيَّة والافتراضيَّة.

الهجمات السريَّة: وهي المحاولات التي يبذلها المهاجمون للتمكُّن من دخول الشبكات الرقميَّة ورصد أنشطة واستخلاص معلومات المستخدمين. ويعتمد تقدير مثل هذا النوع من الاختراقات على قيمة المعلومات المستخلصة والجهد المبذول في سحبها.

هجمات تكامليَّة: وتتمُّ بدخول النظام لتغيير المعلومات بدلاً من استخلاصها أو الاستيلاء عليها، وهي تستغلُّ البيانات في العالم الافتراضي إضافة إلى الأنظمة والأشخاص الذين يعتمدون على تلك البيانات في الواقع. وفي أغلب الأحيان، تهدف تلك الهجمات إمَّا إلى تغيير تصوُّر المستخدِم أو وعيه بالموقف، أو تتسبَّب في تدمير أجهزة ماديَّة وعمليَّات توجِّهها وتُفعِّلها أنظمة معلوماتيَّة. ومثل هذه الهجمات التكامليَّة تكون مراوغة حيث نعتمد على أنظمة حاسوبيَّة تستطيع فهم ما يجري داخل المنظَّمات المستهدفة.

الجرائم الإلكترونيَّة ضد المؤسَّسات

تتعرَّض المؤسَّسات لأضرار مباشرة نتيجة هجمات الابتزاز، وهي هجمات تستخدم برامج وتطبيقات الفدية. ويطلب من الضحيَّة أن تختار إمَّا تحمُّل التكلفة المحتملة لصدِّ الهجوم المنظَّم تنظيماً جيداً، وإمَّا الإذعان لطلبات المهاجم. المواقع الإلكترونيَّة التي تمتلك نظم عمل تعتمد على برمجة الوقت والتشغيل والتوريد في مواعيد مبرمجة؛ مثل المبيعات الموسميَّة تكون أكثر عرضة لهجمات من هذا النوع. فما حجم مثل هذه الجرائم الإلكترونيَّة؟

تسلِّط الأنواع المختلفة من الهجمات الضوء على مدى صعوبة تحديد حجم المشكلة، لا سيَّما أنَّ هناك شحاً في البيانات الموثوق بها، فالمجرمون لا يتشاركون معلوماتهم أو إحصائيَّاتهم مع الأكاديميِّين في أغلب الأحيان. يقول «روس أندرسون» الأستاذ في جامعة كامبريدج: «هناك أكثر من مائة مصدر للبيانات المتعلِّقة بالجريمة الإلكترونيَّة، ومع ذلك لا تزال الإحصاءات المتوافرة متناثرة وغير كافية، فهذه البيانات تفتقر إلى الدقَّة والموثوقيَّة، وهي إمَّا أقل من الحقيقة الواقعة وإمَّا تتجاوزها، وهذا يتوقَّف على الشخص الذي جمعها والأخطاء المقصودة مثل مؤسَّسات الحماية والوكالات الأمنيَّة التي تختلق التهديدات لترويج وبيع حلولها.

وحتَّى إن كانت البيانات متوافرة، فإنَّ تحديد تكاليف الجريمة الإلكترونيَّة ليس أمراً سهلاً. فالتكاليف المباشرة لا تطال الضحايا المباشرين وحسب، بل تطال أيضاً الوسطاء مثل البنوك ومزوِّدي خدمة الإنترنت الذين يتعيَّن عليهم التعامل مع الكمِّ الهائل من البريد الإلكتروني المزعج «الاسبام». تلك التكاليف غير المباشرة يمكن أن تُحدث فارقاً كبيراً في التكلفة النهائيَّة في واقع الأمر. فبحلول عام 2013، كان متوسِّط إنفاق المؤسَّسات التي تضم 1000 موظَّف أو أكثر، نحو 9 ملايين دولار سنوياً، سواءً أكانت تلك المؤسَّسة بنكاً أم مؤسَّسة صناعيَّة مثلاً. وعند النظر إلى المسألة بطريقة شاملة، تفرض الجريمة الإلكترونيَّة تكلفة كبيرة على المجتمع بأسره، ولهذا ينبغي اكتشاف طرق وأساليب أكثر تعقيداً وذكاءً في مواجهتها.

كما يمكن النظر إلى الجريمة الإلكترونيَّة من منظور آخر غير التكلفة، وهو حجم ما تدرُّه من ربح لمرتكبيها. فمن بين طرق بحث الجريمة الإلكترونيَّة من هذه الزاوية أن نفحص الدخل الذي تحقِّقه. وفي هذه الحالة يصبح الأمر معقَّداً، حيث لا يتوافر الكثير من التقارير عن تلك الإيرادات. ويشير «جيم لويس» أحد الخبراء البارزين في مجال الأمن الإلكتروني إلى أنَّ الأرباح التي تدرُّها

الجريمة الإلكترونيَّة جيِّدة، ويضيف قائلاً: «عائد الجريمة الإلكترونيَّة جيِّد، فقد حقَّق اثنان من مرتكبي الجرائم الإلكترونيَّة دخلاً يُقدَّر بنحو مليوني دولار أمريكي خلال عام واحد من التفاعل الوهمي والاحتيال على موقع فيسبوك»، والنقر الاحتيالي نوع من جرائم الإنترنت يحدث في نموذج الدفع وفقاً للنقرات في الإعلان على الإنترنت، عندما يقوم شخص ما أو برنامج إلكتروني صغير بتقليد المستخدم الشرعي والضغط على أحد الإعلانات، بغرض تحميل تكلفة النقرات للمنافسين من دون تحقيق فائدة فعليَّة من الإعلان. ويضرب لويس مثالاً آخر على الربح الكبير الذي يحقِّقه مقترفو الجرائم الإلكترونيَّة فيقول: «ابتكر اثنان من مرتكبي الجرائم الإلكترونيَّة تحذيرات من البرمجيَّات الخبيثة التي تومض على شاشات الحواسيب، وأكَّد مكتب التحقيقات الفيدرالي الأمريكي «إف بي آي» أنَّ المجرمين حقَّقوا أرباحاً بلغت 72 مليون دولار من أناس دفعوا لهم كي يمكِّنوهم من إزالة تلك التهديدات الزائفة.

الإرهاب الإلكتروني

يرى واضعو السياسات الحكوميَّة وخبراء الإعلام أنَّ الإرهاب الإلكتروني ليس مخيفاً أو محتمل الحدوث بدرجة كبيرة، لكنَّ هذا لا يعني أنَّ الإرهابيين متخلِّفون ولا يواكبون التكنولوجيا، فالإنترنت توفِّر وسائل يمكن التواصل من خلالها مع جماعات كبيرة من الناس واختراق القيود والحدود الجغرافيَّة التقليديَّة، فهي تربط الناس ذوي الاهتمامات والمعتقدات المتشابهة الذين ما كانوا ليلتقوا لولا الشبكة العنكبوتيَّة، فالإنترنت تتيح للمهاجمين مثلما تتيح للمستخدمين العاديِّين توصيل أصواتهم وبلوغ المزيد من الجماهير.

ومع توسُّع العالم الافتراضي، تطوَّر استخدام الجماعات الإرهابيَّة له، لا سيَّما في مجال عمليَّات معالجة واستخدام المعلومات. ومثلما هو الحال في كلِّ نشاطات الفضاء الإلكتروني، كلَّما كان المحتوى جاذباً للاهتمام، زادت احتمالات متابعته، وهو ما يُكافئ الاتجاهات والسلوكيَّات البغيضة بمزيد من الأنشطة الإلكترونيَّة على مواقع الإنترنت. فقد أتاح العالم الإلكتروني للجماعات المتطرِّفة الوصول إلى كلِّ الناس والتشويش على الأصوات المسالمة والمحترمة والأكثر اعتدالاً.

لقد أتاحت ثورة الإنترنت للجريمة المنظَّمة إخفاء عمليَّاتها بطرق جديدة أكثر تعقيداً من الخوارزميَّات المصمَّمة للعمل والاتصال والحماية وردِّ الهجمات، فالمهاجمون يعرفون قيمة الإنترنت ويستثمرون فيها وكأنَّها مؤسَّسات تجاريَّة مشروعة، ويضعون خططاً طويلة المدى، وهم يستطيعون بعد كلِّ هذا إخفاء عمليَّاته، وسلب هويَّات الآخرين واستخدامها في الهجوم على مواقع كنَّا نظنها آمنة، ولهذا يتزايد القلق من أن تستغلَّ هذه الجماعات شبكات التواصل الاجتماعي للوصول إلى معلومات وأهداف مؤسَّسيَّة أو شخصيَّة. فبعد أحداث الحادي عشر من سبتمبر عام 2011، تساءل أحد المحلِّلين العاملين في مجال الأمن الإلكتروني عمَّا يمكن معرفته عن منفِّذي الهجوم، ثمَّ أعلن أنَّه استطاع أن يعثر على أسماء اثني عشر عضواً سابقين وأسماء أسرهم وعناوين منازلهم. لم يكن هذا مسألة تسريبات للصحافة، بل تمَّ من خلال مجموعة من حيل التواصل الاجتماعي، حتَّى إنَّه تمكَّن من تعقُّبهم عبر الإنترنت. وباستخدام تكتيكات كهذه، استطاع التوصُّل إلى أسماء عملاء سرِّيين تابعين لمكتب التحقيقات الفيدرالي الأمريكي «إف بي آي» كانوا يرتادون أحد المواقع المحظورة، ويُعرِّضون أنفسهم للابتزاز. وقد نفَّذ كلَّ هذه العمليَّات لتحذير المستهدفين من توافر معلومات عنهم على شبكة الإنترنت أكثر ممَّا يعتقدون، ولعلَّ في هذا تذكرة لنا أيضاً.

ما الحل؟

نرى أنَّ الدعوة إلى إنشاء إنترنت جديدة تشبه محاولة مؤسَّسة «جوجل» منافسة «فيسبوك» من خلال نظام «جوجل بلاس»، ومنافسة «واتساب» من خلال نظام تبادل الرسائل «هانج آوت». فما يعتاده الناس يدمنونه، والتحوُّل من إنترنت إلى آخر ليس حلاً عملياً، لكنَّ هذا لا يعني إلغاء فكرة بناء إنترنت أقلَّ خطورة. فمن حقِّ المخترع المبتكر أن يتخيَّل، ومن حق المستخدم أن يختار ويجرِّب ويتأمَّل، مع التركيز على التحليل الواعي والدقيق للأفكار المقترحة ومقارنة تكاليفها بإمكاناتها، مع وضع مسائل الحماية والأمن الإلكتروني على قمَّة الخيارات.

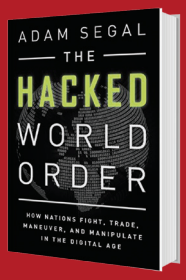
في عالم يعتمد اعتماداً هائلاً على الإنترنت، ثمَّة مخاوف واقعيَّة من فقدان هذ العالم الافتراضي العظيم. والأمر لا يتعلَّق بمجرَّد فقدان التواصل الاجتماعي عبر مواقع مثل فيسبوك وتويتر وغيرهما، وإنَّما يتعلَّق بالتأثير السياسي والاقتصادي الذي يمكن أن يترتَّب على ذلك، وبناءً عليه فإنَّ الحاجة إلى توفير «المرونة» والبدائل ضد صدمات كهذه أصبحت واحداً من المتطلَّبات الأساسيَّة للأمن الإلكتروني. والمرونة من المفاهيم التي نُفرِط في استخدامها ولا تنال القدر المناسب من البحث والتدقيق. والفكرة العامَّة من المرونة هي التكيُّف مع الظروف غير المواتية والتعافي من الأزمات بسرعة.

المرونة ميزة تنافسيَّة تحتاج إليها كلُّ النظم والمؤسَّسات، فالشبكات والمؤسَّسات المرنة تكون متأهِّبة وجاهزة لصدِّ الهجمات، مع الاحتفاظ بقدر كبير من التحكُّم مع مواصلة أداء وظيفتها حتَّى أثناء تعرُّضها للهجوم. يقول الخبير الأمني «دان جير»: «ينبغي أن نُسلِّم بحقيقة أنَّ عمليَّات التسلُّل حدثت وستحدث. وينبغي أن نفكِّر باحتمال أن نصبح قادرين على تقبُّل التأثير المباشر لتلك الهجمات، فمهما بلغ الضرر الذي يتسبَّب فيه المهاجم، يمكن أن يستمرَّ النظام في أداء مهمَّته بأقصى قدرٍ ممكنٍ من المرونة والفاعليَّة».

تحويل الداء إلى دواء

بدلاً من التركيز على تطوير حلول لمشكلات تتعلَّق بالأمن الإلكتروني بطريقة عشوائيَّة، ينبغي التركيز على بناء نظم مرنة وقادرة على مقاومة مختلف أنواع التهديدات. وبعبارة أخرى: لا يوجد حلٌّ سحريٌّ واحدٌ لمشكلة الأمن الإلكتروني، ولكنَّ هناك أطراً للتفكير من شأنها أن تساعد على تطوير منهجيَّات أكثر فاعليَّة في تحقيق الأمن الإلكتروني في مختلف المجالات. مثل هذه المنهجيَّات والبرمجيَّات تشمل: مقاييس التعقُّب اللازمة لتوجيه عمليَّات التخطيط والاستثمار المؤسَّسي طويلة المدى؛ إضافة إلى التدريب على المضاهاة والمحاكاة وتخيُّل السيناريوهات التي يمكن أن يفكِّر فيها ويطوِّرها المهاجمون، مع استخدام أدوات التحليل النفسي وفرز نقاط التهديد وتعقُّبها، وتوطيد العلاقات مع المبدعين من المخترقين الإلكترونيِّين وتوظيف خبراتهم في وضع سياسات وإجراءات افتراضيَّة غير قابلة للاختراق.

كتب مشابهة:

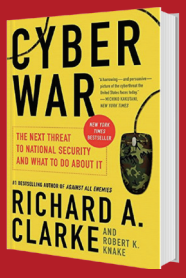


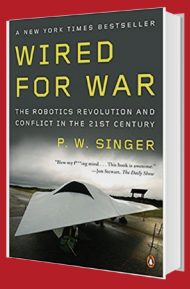
The Hacked World Order
How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age,

By Adam Segal. 2016.

Cyber War
The Next Threat to National Security and What To Do About It.

By Richard A. Clarke. 2012.





Wired for War
The Robotics Revolution and Conflict in the 21st Century.

By P. W. Singer. 2009.

قراءة ممتعة

ص.ب: 214444
دبي، الإمارات العربية المتحدة
هاتف: 3444 423 04
نستقبل آراءكم على pr@mbrf.ae

تواصلوا معنا على

MBRF_News
MBRF_News
mbrf.ae
www.mbrf.ae

qindeel_uae
qindeel_uae
qindeel.uae
qindeel.ae

Qindeel | قنديل
للطباعة والنشر والتوزيع
Printing, Publishing, and Distribution

مبادرات محمد بن راشد آل مكتوم العالمية
Mohammed Bin Rashid
Al Maktoum Global Initiatives

مؤسسة محمد بن راشد آل مكتوم للمعرفة
MOHAMMED BIN RASHID AL MAKTOUM
KNOWLEDGE FOUNDATION

بالعربي

إحدى مبادرات مؤسسة
محمد بن راشد آل مكتوم للمعرفة

تتشرف مؤسَّسة محمد بن راشد آل مكتوم للمعرفة بدعوتكم إلى المشاركة في فعاليات مبادرة #بالعربي2017 في دورتها الخامسة

من 14 إلى 18 ديسمبر 2017

تزامنًا مع الاحتفال باليوم العالمي للغة العربية 18 ديسمبر، حيث تحتفي مبادرة #بالعربي باللغة العربية من خلال دعم ونشر محتواها، وتشجيع استخدامها على شبكات التواصل الاجتماعي. وتقام فعاليات المبادرة في الأماكن التالية:

أبوظبي - ياس مول | العين - العين مول | دبي - مردف ستي سنتر - إمارات مول - ديرة ستي سنتر - العربي سنتر

الشارقة - صحارى سنتر | عجمان - عجمان ستي سنتر | رأس الخيمة - الحمرا مول | الفجيرة - ستي سنتر الفجيرة

شاركونا الاحتفال بلغتنا الأصيلة وتواصلوا #بالعربي

bilarabi.mbrf | bilarabi_mbrf | bilarabi_mbrf | bilarabi_mbrf

bilarabi-mbrf | bilarabi_mbrf | bilarabi.mbrf