بسم الله الرحمن الرحيم

جامعة السودان للعلوم والتكنولوجيا

كلية الدراسات العليا

ترجمة الصفحات (1-66) من كتاب الأمن الإلكتروني والحرب الإلكترونية - ما ينبغي ان يعرفه كل شخص

لمؤلفيه: بيتر وارن سينغر و ألن أ. فريدمان

بحث تكميلي لنيل درجة الماجستير في الترجمة

A Translation of the Pages (1-66) from the Book:

Cybersecurity and Cyberwar

What Everyone Needs To Know®

By: Peter Warren Singer and Allan A. Friedman

A Thesis Submitted in Fulfillment of the Requirements for

M.A in Translation

إعداد:

مجاهد فخرالدين قاسم أحمد

إشراف:

د. أريج عثمان أحمد محمد

إهداء

إلى من تعهداني بالتربية في الصغر

وكانا لي نبراساً يضيء فكري بالنصح والتوجيه في الكبر

أمي وأبي حفظهما الله.

إلى من شملوني بالعطف، وأمدوني بالعون، وحفزوني للتقدم،

إخوتي وأخواتي رعاهم الله.

إلى كل من علمني حرفاً، وأخذ بيدي في سبيل تحصيل العلم والمعرفة.

إلى روح صديقي الغالي

مجاهد أمين (رحمه الله).

إليهم جميعاً أهدي ثمرة جهدي، ونتاج بحثي المتواضع.

شكر وتقدير

الحمد لله رب العالمين والصلاة والسلام على معلم البشرية وهادي الإنسانية وعلى آله وصحبه وسلم. الشكر لله عز وجل الذي أنار لي الدرب، وفتح لي أبواب العلم وأمدني بالصبر والإرادة. ثم الشكر للأستاذة الدكتورة أريج عثمان على توجيهاتها ونصحها السديد. والشكر لصديقي الغالي مجاهد أمين (رحمه الله وطيب ثراه وأسكنه فسيح جناته). والشكر والامتنان لكل الذين قدموا لي يد العون. جزاكم الله عني كل خير.

مستخلص البحث

تناول كتاب الأمن الإلكتروني والحرب الإلكترونية موضوع تكنولوجيا الحاسوب والانترنت بلغة سهلة، يسهل على من يقرأه فهمة واستيعابه. يتكون الكتاب من ثلاثة اجزاء شملت المعلومات الضرورية التي يحتاجها كل شخص من وجهة نظر الكاتبين. ترجم الباحث مستهل الكتاب من مقدمة وكامل الجزء الأول. احتوى الجزء الأول على نبذة تاريخية عن مسيرة تطور الانترنت، والعلماء الذين تركوا بصمة في ذاك المجال. ثم واصل الكتاب شرح كيفية عمل الإنترنت، من أساليب وبرامج وأجهزة، وعن الإدارات المختلفة العاملة عليه. وتطرق الكاتبان ايضاً لذكر بعض الحوادث التي تركت اثراً واضحا في تاريخ الإنترنت، والتي أدت لتغيرات جذرية في المعتقدات والمفاهيم. وكما ورد في عنوان الكتاب، فالكتاب في مجمله يتناول الأمن المتعلق بالحاسوب والمخاطر المحدقة بنا في عصر أصبح فيه كل شيء متصلا بالإنترنت. فمنذ جيل مضى، لم يكن مصطلح "الفضاء الإلكتروني" إلا مصطلحاً في قصص الخيال العلمي، والذي استخدم ليصف شبكة من الحواسيب تربط معامل جامعات قليلة. اما اليوم، أسلوب حياتنا العصري من الاتصالات إلى الصراعات كله يعتمد على الإنترنت. للبعض منا، قد يكون الإنترنت عبارة عن شبكات التواصل الاجتماعي فقط، او ربما حيث تجد المساعدة لبحث أكاديمي. ولكنه أكبر من ذلك بكثير، فهو عالم مليء بالعجائب. علاوة على ذلك، نجد أن قضايا الأمن الإلكتروني تهديداً يمسنا كأفراد، فإننا نواجه تساؤلات في كل شيء، بدأ من حقوقنا ومسؤولياتنا كمواطنين في العالمين الرقمي والحقيقي. إلى كيفية حماية أنفسنا واهلينا من نوع جديد من الأخطار. في النهاية، ليست هناك قضية تفاقم الاهتمام بها بهذه السرعة ومست الكثيرين منا، وظلت غير مفهومة ومبهمة كقضية الأمن الإلكتروني. وقد اعتلت الباحث الدهشة عندما اطلع على حقائق الإنترنت وما احتواه الكتاب من حقائق ومعلومات جديرة بالاطلاع. ولذا وجد من الجدير ترجمة كتاب مثل هذا ليفتح أبواب المعرفة للجميع.

Abstract

Cybersecurity and Cyberwar is a book about computer technology and the Internet, written in an easy language, which makes it easier for everyone to read, follow up and understand. The book comes in three parts, which contain what the writers think is essential for everyone to know. The researcher translated the introduction and the first part completely. The first part includes a brief historical introduction about the Internet revolution, and the scientists who contributed and left their marks on it. Then the book continues to show how the Internet all works, its architecture, programs, machines, and its authorities. The writers also mentioned some of the incidents that changed the course of the Internet. As the title reads, it is all about security and the danger around us in an era everything connected to the Internet. A generation ago, “cyberspace” was just a term from science fiction, used to describe the nascent network of computers linking a few university labs. Today, our entire modern way of life, from communication to conflicts, fundamentally depends on the Internet. For some of us, the internet is just about social media networks, or perhaps a place where you would find help in your academic researches. However, it is a whole world of wonders. Moreover, cyber security issues affect us as individuals. We face new questions in everything from our rights and responsibilities as citizens of both the online and real world. To simply how to protect ourselves, and our families from a new type of danger. Moreover, there perhaps no issue that has grown so important, so quickly, and that touches so many and remains so poorly understood. The researcher stunned by the facts of the internet, and the knowledge the book holds between its covers, this why such a book should be translated to make this knowledge available to everyone.

مقدمة المترجم

تعثر الباحث في فهم بعض المصطلحات والمفاهيم التي جعلته في حيرة من امره. فالكتاب يندرج تحت طائلة الكتب العلمية، واللغة المستخدمة متعلقة بالحاسوب والانترنت، ونسبة لحداثة النشر فكان لابد من وجود مصطلحات ومفاهيم لم ترد في القواميس الموجودة. لجأ الباحث في الترجمة بشكل كبير إلى المعاجم الموجودة على الإنترنت من المعاجم أحاديه اللغة وثنائية اللغة، ليتبين ويتفحص المعاني بصورة أدق.

إن أولى الكلمات التي أوقفت الباحث وهي أكثر المصلحات وروداً في هذا الكتاب، هي كلمة Cyber والتي كان معناها شاملاً لدرجة كبيرة. حسب ما ورد في القاموس فهي "كل ما تعلق او اتصف بصفات ثقافة الحواسيب وتقنية المعلومات والواقع الافتراضي" فكان من الصعب اختيار المعني "المناسب" فقد ترجمتها اولاً "الحاسوبي" وبعد مشورة وبحث وجد الباحث ان الترجمة الأكثر شيوعاً هي "إلكتروني"، وكِلاَ الكلمتين تحملان نفس المعني.

من الكلمات أيضاً، كلمة Router والتي تعنى "جهاز لتوجيه البيانات الى اماكن محددة في شبكة الحاسوب"، فقد أصبح متداولاً بين العامة ما انحدر من تعريب الكلمة لتصبح "راوتر" مع ان لها ترجمة محفوظة وهي "مُوجِه" او "جهاز توجيه". استخدمت في هذه الترجمة كلمة "المُوجِّه".

قد تطول القائمة بالمعاني والكلمات ولكنها كلها تشترك في كونها مصطلحات جديدة وكلمات مستحدثة في عالم الاتصالات والحاسوب، في كثير من الأحيان لم يكن لها معني مترجم واضح فلجأ الباحث إلى تعابير ضمنية احتوت على المعني، وهذا يأتي في المثال الأخير في كلمة Botnet والتي ورد معناها انها "شبكة

من الحواسيب الخاصة المصابة ببرنامج ضار يتحكم فيها كمجموعة بدون علم اصحابها"، قام الباحث بترجمتها على انها "حواسيب مصابة خارجة عن السيطرة"، أتت كلمة "مصابة" هنا نكرة لأنه تم شرحها مسبقاً في النص الذي وردت فيه اولاً، وفيما تلت وردت نكرة.

المحتويات

الملاحق

بسم الله الرحمن الرحيم

مقدمة

لماذا يجب تأليف كتاب عن الأمن الإلكتروني والحرب الإلكترونية؟

"كل هذه الأشياء الإلكترونية."

دارت الأحداث في غرفة المؤتمرات في العاصمة واشنطن، وكان المتحدث قائد كبير في وزارة الدفاع الأمريكية، وكان الموضوع عن لماذا اعتقد بأن الأمن الإلكتروني والحرب الإلكترونية مهمة جداً. ولكن عندما لم يستطع أن يصف المشكلة إلا بـ "كل هذه الأشياء الإلكترونية" وبغير قصد منه أقنعنا بكتابة هذ الكتاب.

كلانا في عقده الثلاثين، وما زلنا نذكر أول اجهزة حاسوب استخدمناها. بالنسبة لألن، كان أول جهاز له من أوائل أجهزة أبل ماكنتوش في بيته في بتسبيرغ، عندما كان في الخامسة من عمره. كانت سعة تخزينه محدودة جداً، لدرجة أنها ما كانت لتسع هذا الكتاب. أما بيتر، في عمر السبع سنوات كان أول جهاز استخدمه من طراز كوماندر معروضا في متحف العلوم في شمال كارولينا. وقد أخذ دروسا عن كيفية "البرمجة" تعلم فيها لغة جديدة كلياً لغرض وحيد وهو صناعة واحد من أهم الاختراعات في تاريخ البشرية وهو طباعة وجه مبتسم، كان يطبع على ورق مثقوب الجوانب يخرج من طابعة فيها لفافة دائرية من الورق.

وبعد ثلاثة عقود، أصبح من المستحيل تفهم كيف تمركزت الحواسيب في حياتنا. في الحقيقة، صارت الحواسيب محيطة بنا لدرجة اننا لم نعد نفكر فيها "كحواسيب" بعد الآن. نصحوا باكراً بفضل ساعات محوسبة، ونستحم بمياه تم تسخينها بحاسوب، ونشرب قهوتنا وقد أُعدّت أيضاً بحاسوب، ونأكل حبوب دقيق الشوفان في فطورنا وتم تسخينها عن طريق حاسوب، ثم نقود سياراتنا إلى أعمالنا وقد تحكمت فيها مئات من الحواسيب،

ومن ثم نختلس النظر على نتائج مباريات البارحة أيضاً عن طريق جهاز حاسوب، وفي أماكن عملنا نمضي معظم يومنا ونحن نضغط على أزرار حاسوب. تجربةٌ كان تعد مستقبليةً أيام آباءنا، حيث كان ضغط الأزرار على جهاز حاسوب هي من أفعال "آل جتسن" (كانت وظيفة جورج جستن الذي كان يعمل "مشغلاً للمؤشر الرقمي"). لعل أفضل طريقة لإدراك ولو الشيء القليل عن الوجود العصري للحواسيب في كل مكان، هي أن تستلقي على فراشك ليلاً وتطفئ الأنوار وتبدأ بعد الأنوار الصغيرة الحمراء التي تحدق فيك!

ليس فقط أن كل هذه الماكينات لها وجود مطلق في أي مكان، بل هي متصلة مع بعضها. أما الحاسوب الذي استخدمناه في صغرنا لم يكن متصل بشيء غير مقبس الكهرباء، وربما طابعةٌ ذاتُ الورق مثقوبِ الجوانب. منذ جيل مضى كان الإنترنت مجرد ربط بين قله من الباحثين الجامعيين. تم إرسال أول بريد إلكتروني في عام 1971، يعيش أبناء هؤلاء العلماء اليوم في عالم يرسل فيه ما يقارب الأربعين ترليون بريد إلكتروني في السنة. تم إنشاء أول موقع على الإنترنت في العام 1991، بحلول عام 2013 كان هناك ما يزيد عن ثلاثين ترليون صفحة على الإنترنت.

علاوة على ذلك، لم يعد الإنترنت يقتصر فقط على إرسال بريد إلكتروني أو جمع معلومات. بل أصبح يتعامل مع كل شيء من ربط محطات الكهرباء إلى تتبع طرد لعبة باربي كنت قد اشتريتها. قدرت سيسكو التي هي إحدى الشركات التي تساهم في تشغيل العمود الفقري للإنترنت، أن بنهاية عام 2012 كان هناك 8.7 بليون جهاز متصل بالإنترنت، هذا التقدير يُعتقد أنه سيزيد إلى أربعين بليوناً بحلول عام 2020. كما هي حال السيارات والثلاجات والأجهزة الطبية والأجهزة التي لم يُفكّر فيها أو تُخترع بعد، كلها مرتبطةٌ بالإنترنت. باختصار فإن المجالات التي تشمل ما بين التجارة إلى الاتصالات إلى البنية التحتية الحيوية والتي تشكل تحضرنا العصري في شكله اليومي كلها تدار بما أصبح شبكة عالمية من الشبكات.

ولكن مع تصاعد "كل هذه الأشياء الإلكترونية" والذي هو مهم للغاية، فإن التاريخ القصير بشكل لا يصدق للحواسيب والإنترنت وصل إلى نقطة حاسمة، وكما هو حال الجانب الإيجابي للنطاق الإلكتروني وهو يمتد ليصل إلى نطاق العالم الحقيقي، مع عواقب سريعة وغالباً غير متوقعه. فإن ذاك ينطبق على جانبه السلبي أيضاً.

كلما استطلعنا أكثر تبين أن تلك الأرقام الصاعقة خلف " كل هذه الأشياء الإلكترونية" تقود إلى نطاق من التهديدات: سبعة وتسعون بالمئة من الشركات الخمسمائة الأولى في الولايات المتحدة حسب تقيم مجلة "فورشن" Fortune تم اختراقها (ومن المرجح أن الثلاثة بالمئة قد تم أيضاً اختراقها لكنهم لم يدركوا ذلك بعد). أكثر من مائة حكومة يعدون العتاد لخوض المعارك على نطاق الإنترنت. بشكل أخر، يمكن تصور المشكلة عن طريق النظر إلى القضايا السياسية المعقدة التي قد احدثتها هذه "الأشياء": مثل الفضائح من "وكيليكس" WikiLeaks ومراقبات وكالة الأمن القومي، واسلحة حاسوبية جديدة مثل "ستكسنت" Stuxnet. والدور الذي تلعبه شبكات التواصل الاجتماعي في كل شيء، بداءً من ثورات الربيع العربي وصولاً إلى اهتمامك بخصوصيتك الشخصية. في الواقع، فإن الرئيس باراك أوباما كان قد صرح بأن" مخاطر الأمن الإلكتروني تشكل جزءً من أخطر تحديات القرن الواحد والعشرين التي تهدد الاقتصاد والأمن القومي "وهذا موقف تكرر من قادةٍ في دول من بريطانيا إلى الصين.

مع كل الوعود والآمال التي يحملها لنا عصر المعلوماتية، فإنه الوقت "للقلق التكنلوجي". في استبان عن إلى اين يتجه العالم في المستقبل؟، وصفت مجلة "فورن بولسي" Foreign Policy عصر تقنية المعلومات بأنه "أحد أكبر التهديدات الناشئة"، بينما ادعت صحيفة "بوسطن قلوب" Boston Globe أن المستقبل هنا بالفعل: فإن هناك "حرب عالمية إلكترونية" جاريةٌ الآن، تبلغ ذروتها على خنادق حرب رقمية دموية.

كل هذه المخاوف قد انصهرت لتفجر تجارة الأمن الإلكتروني، واحدة من أسرع الصناعات نمواً في العالم. وأيضاً أدت إلى خلق العديد من الإدارات والمكاتب الحكومية (تتضاعف وزارة الأمن القومي الأمريكية في حجمها مرتين أو ثلاثة كل سنة منذ نشأتها)، مثل ما هو حال القوات المسلحة حول العالم كالقيادة الإلكترونية للولايات المتحدة و "قاعدة سرية المعلومات" الصينية وأيضاً وحدات حربية مهمتها الوحيدة هي خوض الحروب والنصر في الفضاء الإلكتروني.

كما نسرى لاحقاً إن مفاهيم " الأشياء الإلكترونية" تشكل مخاطر حقيقية ولكن طريقة إدراكنا وتعاملنا مع هذه المخاطر قد تكون ذات أثر كبير على المستقبل وليس فقط على الإنترنت. أوضح العميد السابق لكلية هارفرد كنيدي للإدارة الحكومية أن متى ما بدء المستخدمون في فقدان الثقة في أمن وسلامة الإنترنت فسينسحبون من الفضاء الإلكتروني بتبديل "الرفاهية بحثاً عن الأمن".

زيادة المخاوف بصدد الأمن الإلكتروني أدت إلى هتك مفاهيمنا للخصوصية مما سمحت للمراقبة وترشيح الإنترنت بأن يصبح مقبولاً في اماكن العمل والمدارس وحتى على المستوى الحكومي. أيضاً هناك دول بأكملها تنسحب مما سيودي لتدهور فوائد الاقتصاد وحقوق الإنسان التي رأيناها من التواصل العالمي. تُطور الصين شبكتها الخاصة بالشركات فيما أسمته بـ "جدار النار العظيم" ليمكنها من عرض الرسائل الواردة وفصل الاتصال بالشبكة العالمية للإنترنت إذا ما دعت الضرورة. كما جاء في مقال لكلية يال للقانون أن كل هذه النزاعات "تتجمع لتُكوّن عاصفة عارمة تهدد بعصف القيم التقليدية للإنترنت من انفتاح وتعاون وابتكار وسلطة محدودة وتبادلٍ حرٍ للأفكار".

هذه القضايا ستشكل عواقب أبعد من الإنترنت، هناك حس متنامي للتعرض للإصابة في عالمنا الواقعي عن طريق نواقل الهجمات الإلكترونية من العالم الافتراضي. وصف تقريرٌ عنوانه "السباق الجديد للتسلح

التكنلوجي": لن تخاض الحروب في المستقبل بالجنود المسلحين ورمي القنابل من الطائرات فقط، ولكن ستخاض أيضاً بضغطة فارةٍ حاسوب من النصف الأخر للكوكب لتطلق بحذر سلاحاً حاسوبياً مبرمجاً يؤدي إلى خلل أو تدمير للبنية الأساسية كالمرافق العامة والموصلات والاتصالات والطاقة. هجمات مثل تلك قد تؤدي إلى تعطيل شبكات الجيش التي تتحكم بتحركات الكتائب ومسار الطائرات المقاتلة والتحكم وإدارة السفن الحربية".

تلك الرؤية لحرب بلا ثمن أو هزيمةٍ فورية قد تشعرنا إما بالخوف أو بالرضا، ذاك يعتمد كلياً في أي جانب كنت من الهجوم الإلكتروني، كلما استطلعنا أكثر في الكتاب أدركنا أن الحقيقة أكثرُ تعقيداً مما تبدو. تلك الرؤى لا تسبب الجزع أو تسير الميزانيات وحسب، بل يحتمل أنها ستقود لتغير الفضاء الإلكتروني إلى منطقة عسكرية. كما أن هذه الرؤى تهدد نطاقاً يوفر كميه كبيرة وهائلةً من المعلومات والابتكارات والرفاهية لكوكب أكبر، وتزيد حدة التوتر بين الدول. وكما كشف عنوان التقرير السابق لربما أدت فعلاً إلى سباق تسلحٍ عالميٍ جديد.

في النهاية، ليست هناك قضية تفاقم الاهتمام بها بصورة سريعة كقضية الأمن الإلكتروني، كما أنه ليست هناك قضية كثر فيها الجهل كـ "هذه الأشياء الإلكترونية".

لماذا هناك فجوة معرفية بصدد الأمن الإلكتروني، ولما المعرفة مهمة؟:

"من النادر أن تجد أمراً مهماً مبهماً وقل فيه الفهم وشائعاً جداً بين الناس... كنت جالسا في اجتماع صغيرٍ في واشنطن غير قادرٍ – أنا وزملائي – لاتخاذ أي قرارٍ لأنا كنا نفتقر لصورةٍ واضحةٍ للمدى البعيد للأثارِ السياسيةِ والقانونيةِ المترتبة على أي قرار قد نتخذه".

هكذا وصف الرئيس السابق لوكالة المخابرات المركزية الجنرال مايكل هيدن الفجوة المعرفية المتعلقة بالأمن الإلكتروني والخطر الذي تُلوّح به. سبب أساسي لعدم الترابط هذا يُعتبرُ نتيجةَ التجاربِ الأولى مع الحواسيب، أو بالأحرى انعدامها وسط كثير من القادة. شباب اليوم يُعتبرون مواطنين أصليين للعالم الرقمي، فقد نشؤا في عالم أصبح وجود الحاسوب فيه امراً طبيعيا. لكن ما زال العالم يُقاد بواسطة من يُعتبرون مهاجرين في العالم الرقمي، ذاك الجيل الذي تظل له الحواسيب ومخاطر الإنترنت لغزاً محيراً وأمراً غير مألوف.

بطريقة أخرى فإن قلةً مِن مَنهُم أكبر من عمر الخمسين قد قضوا تدريبهم الجامعي باستخدام حاسوب، وعلى الأرجح فإن هؤلاء القلة استخدموا حاسوباً قائماً بذاته غير متصل بالعالم. إن أغلب كبار قادتنا في عمر الستين والسبعين في الغالب لم يعتادوا استخدام الحواسيب حتى فترة متأخرة من حياتهم المهنية، وإن مِنهُم مَن لا يملك إلا الخبرة القليلة جداً حتى يومنا هذا. حتى عام 2001 لم يكن هناك جهاز حاسوب في مكتب رئيس التحقيقات الفدرالية بينما كان يطلب وزير الدفاع الأمريكي من مساعده أن يطبع له البريد الإلكتروني يقرئه ثم يكتب رده بالقلم ويطلب من مساعده طباعة ما كتب على الحاسوب. كم كان ذلك غريبا! ولكن بعد عقد كامل من الزمن قالت وزيرة الأمن القومي التي هي مسؤولة عن حماية أُمتنا من التهديدات الإلكترونية في مؤتمر عام 2012 "لا تضحكوا... لكني لا أستخدم البريد الإلكتروني إطلاقاً"، وذلك لم يكن خوفاً من الأمان بل اعتقاداً منها أنه بلا فائدة. وفي عام 2013 كشفت القاضية إلين كأغن أن ثمانيةً من أصل تسعة من قضاة المحكمة العليا في الولايات المتحدة ذو تجربة محدودة في التعامل مع الحاسوب وهم الأشخاص الذي بيدهم القرار المطلق عما يكون شرعيا أو غير شرعي.

لا يتعلق الامر كلياً بالعمر، ولو كان كذلك لكان الحل أن ننتظر حتى يفنى كبار السن فتُحل كل المشاكل. وأيضاً هذا لا يعني أن الشباب يدركون تلك القضايا الرئيسية بالفطرة. إن الأمن الإلكتروني واحد من

المجالات التي تُرِكت لمن هم ميالون للتكنلوجيا للقلق بشأنها. كل ما هو متعلق بالعالم الرقمي ذو الأصفار والأحاد كان فقط مشكلةً يحُلّها علماء الحاسوب وأنظمة المعلومات، والذين إذا تكلموا ظلت الأغلبية يومؤون برؤوسهم صامتين، مشكلين ما اسماه الكاتب مارك بودن بـ "الاندهاش" تلك "نظرة لا يمكن تفسيرها إلا بالتشوش الشديد واللامبالاة، متي ما تغير الموضوع إلى ما يتعلق بالحاسوب" الاندهاش تعبير يظهر في وجهك عندما لا تسطع وصف شيء ما إلاَّ بعبارة "أشياء". بالمقابل فإن مَن هُم ميالون للتكنلوجيا غالبا ما يديرون أعينهم غير مهتمين للمنطق الغريب في عوالم السياسة والأعمال، ساخرين من "الطريقة التقليدية" للقيام بالأعمال بغير فهم للتداخل بين الناس والتكنولوجيا.

والنتيجة أن الأمن الإلكتروني لا يقع في أي أرض يملكها إنسان، صار الميدان منطقة حاسمة لمجالات حساسة كخصوصيتك وخطيرة كمستقبل السياسات العالمية. ولكنه نطاق معروف جداً في وسط "حشد تقنيون المعلومات"، ويهم جانبا كبيراً من القطاعين الخاص والعام، ولكن فقط الشباب ومَن هُم ذو دراية واسعة بالحاسوب يتعاملون معه. بالمقابل فهؤلاء التقنيون غالبا ما ينظرون إلى العالم بطريقة معينةٍ تفتقر إلى تقدير الصورة العامة للعالم أو المجالات غير التقنية. لذا كان هناك قضايا حرجة تركت غير مفهومة وغالباً لا تناقش.

تعدُدُ المخاطر قادنا لكتابة هذا الكتاب، أيا كان الدور الذي نلعبه في هذه الحياة فإن كلانا عليه اتخاذ قرارات بشأن الأمن الإلكتروني والتي ستشكل المستقبل ما وراء عالم الحواسيب. ولكن غالبا ما نقوم بذلك بدون الأدوات المناسبة، فإن المفاهيم الضرورية والمصطلحات الأساسية التي كانت لتُبين ما يكون ممكنا ومناسبا مفقودة، أو حُرِفت علي أسوء الفروض. ما كان مجهولا في الماضي وما يروّج عنه في المستقبل أمران ينسجمان في الغالب معا، متجاهلين ما حدث بالفعل وأين نحن حقاً الآن. بعض المخاطر يزداد الاهتمام بها ويُرد عليها بنوع من المبالغةِ، وبعضها يتم تجاهله.

هذه الفجوة لها أثارٌ واسعة. وصف جنرال أمريكي لنا أن "فهم كل ما يتعلق بالحاسوب أصبح الآن مسؤولية القيادة" لتأثيرها على كل جزء من الحرب العصرية. هكذا وقد أوضح جنرال أخر وبكل وضوح "هناك نقص حقيقي في المفاهيم والسياسة في عالم الفضاء الإلكتروني". كما سنرى لاحقا فإن مخاوفه لم تكن فقط بأن لا يؤدي الجانب العسكري مهمته في "الحسابات الإلكترونية" بالصورة المطلوبة، بل أيضاً عدم توفير التعاون الازم والإرشاد من الجانب المدني. حال اليوم كما كان أيام الحرب العالمية الأولى عندما أرادت الجيوش في اروبا استخدام تكنلوجيا جديدة مثل السكك الحديدية، عندها كانت المشكلة أنهم والقادة المدنيين والمواطنين من خلفهم لم يفهموا تلك التكنولوجيا ولا أثارها وبذاك الجهل اتخذوا قرارات أدت وبدون قصد لإشعال الحرب بين تلك الدول. قام اخرون برسم أوجه الشبه بينها وبين السنوات الأولى للحرب الباردة، مثل الأسلحة النووية والتفاعل الساسي الذي جلبته لم يكن مفهوما، وأسوء من ذلك فقد تُرك أغلبه للمتخصصين. والنتيجة أن تلك الأفكار التي نضحك عليها الآن مثل ما فعل د.سترينجلوفيان* كانت تؤخذ على محمل الجد فقد قاربوا أن يجعلوا من الكوكب كتلة ضخمة مشعة.

إن العلاقات الدولية أصبحت مسمومة بهذا الفصل ما بين ما هو معروف وما هو مفهوم. نحن الاثنان امريكيان ولذلك فإن كثير من الأمثلة والدروس المدرجة في هذا الكتاب تنعكس من تلك الخلفية، إن مشكلة "هذه الأشياء الإلكترونية" لا تهم أمريكا وحسب فقد أخبرنا موظفون ومختصون من دول مختلفة أنهم مهتمون بها أيضاً، دول مثل الصين وابوظبي وبريطانيا وفرنسا. في مثال أخر لتوضيح الفجوة العالمية فإن المسؤولة

* المترجم: Dr.Stranglovian د.سترينجلوفيان عبارة عن فلم كوميدي ساخر تم انتاجه عام 1964، يجسد المخاوف من صراع نووي أيام الحرب الباردة بين الولايات المتحدة والاتحاد السوفيتي.

عن الأمن الإلكتروني في استراليا لم تسمع قط عن "تور" Tor الذي هو واحد من أهم التكنولوجيات في مجال الإنترنت ومستقبله. (سيتم التوضيح لك أكثر في الجزء الثاني ونأمل أن يتضح لها هي الأخرى).

إن هذا القلق ليس بسبب "سذاجة" هؤلاء المسؤولين الحكوميين ولكن بسبب أنه فعلاً صارت له ردة فعل خطيرة على النظام العالمي. على سبيل المثال فإنه في الغالب ليست هناك علاقة مهمة جداً لمستقبل الاستقرار العالمي كما هي العلاقة بين القوى العظمى للولايات المتحدة والصين. وحتى الآن يتنازع الطرفان من واضعي السياسات العليا وعامة الشعب في فهم التحركات الأساسية للنظام الإلكتروني والأثار المترتبة منه. إن قضية الأمن الإلكتروني هذه أكبر بكثير من تلك العلاقة بين الولايات المتحدة والصين. إن الأكاديمية الصينية للعلوم العسكرية أصدرت في الواقع تقريراً ما بين سطوره تلاحظ بوضوح كيف أن الشك والجهل والتوتر والغلو في الترويج قد اختلطت في تشكيل خطير. "اجتاح إعصار الإنترنت العالم في الآونة الأخيرة مخلفاً تأثيراً على نطاق واسعٍ وترك العالم مصدوماً، واجهته الاستعدادات لحرب الإنترنت، فإن كل دولة وكل جيش ليس باستطاعتهم تجاهل الأمر لكنهم يستعدون لمجابه حرب الإنترنت".

هذه النبرة التعبيرية ـ والتي تنعكس في الولايات المتحدة ـ لا تمد للتوتر الإلكتروني العالمي بصلة، وتوضح كيف أن هذا الخوف كان نتيجة المعلومات المضللة والخلط في اساسيات الموضوع. كما سنرى لاحقا فإن الطرفين فعّالين في الدفاع والهجوم باستخدام الحاسوب، مع حداثة القضية فقد أثبتت كم هي صعبة. تحدث معنا كبار القادة الحكوميين من الصين والولايات المتحدة كيف أنهم يجدون الأمن الإلكتروني يشكل تهديداً بعيداً مقارنة بالتوترات القديمة بين البلدين. فعلى الأقل هم يفهمون وقد لا يختلفون في قضايا مثل التجارة وحقوق الإنسان ونزاعات الحدود، على عكس ما يتعلق بالحاسوب والإنترنت فهم يظلون على حال يرثى لها حتى في الحديث عما تفعله دولهم، ناهيك عن الطرف الأخر. على سبيل المثال في مرة شارك قيادي بارز في

الولايات المتحدة في حوار مع الصين في قضايا متعلقة بالحاسوب والإنترنت وكان قد سألنا ماذا تعني "أي إس بي" ISP (مرة أُخرى، لا تستاء إن لم تكن تعلم معناها، سنشرحه قريباً) إذا كان هذا الموقف أيام الحرب الباردة فذاك السؤال يكون أقرب لعدم معرفة معنى "الصاروخ العابر للقارات" في وسط مفاوضات مع السوفيتيين حول قضايا نووية.

مسائل مثل تلك ليست قضايا للجنرالات والدبلوماسيين فقط، ولكنها تُهِم كل المواطنين. إن النقص العام في فهم هذا الموضوع أصبح أيضاً مشكلة ديموقراطية. بينما نحن نكتب كتابنا هذا، وجدنا أنه جارى النظر من قِبل الهيئة التشريعية للولايات المتحدة فيما يقارب خمسين مشروع قانون متعلق بالأمن الإلكتروني. ولكن تم تصنيف القضية بأنها معقدة جداً لتهم الناخبين. والنتيجة أنه يكون هناك ممثلين مختارين سيفصلون في القضايا نيابة عنهم. هذا واحد من الأسباب، والتي بغض النظر عن مشاريع القوانين تلك لم يتم اصدار أي تشريع حقيقي بخصوص الأمن الإلكتروني في الفترة ما بين عام 2002 وحتى كتابة هذا الكتاب بعد مضي عشر سنوات.

تطورت التكنولوجيا مرة أخرى بصورة سريعة لذا ليس من العجيب أن أغلب الناخبين والقادة الذين انتخبوهم ليسوا متفاعلين بشكل كبير مع مخاوف الأمن الإلكتروني، ولكن يجدر بهم أن يولوها الاهتمام. يربط هذا المجال مجموعة من الجوانب تبدأ بأمن حساباتك البنكية وهويتك على الإنترنت وقضايا حدودية عمن واي من الحكومات يمكنها الوصول إلى اسرارك الشخصية وأيضاً متي وأين لدولتك أن تخوض حروبا. كلنا نحن مستخدمون لهذا النظام ومتكيفين عليه، ومع ذلك نفتقر إلى حوارٍ عامٍ لائقٍ حوله. وكما أوضح أستاذ بجامعة الولايات المتحدة للدفاع الوطني "نحن لا نملك أي حوار مستنير حول الموضوع، وبالتالي إما تجاهلنا المشكلة وتركناها لغيرنا ليحلها أو لمن هم جالسين في الغرف المظلمة يضعون السياسات المهمة" وحتى ذلك لن يجدي

نفعا بالنظر لهؤلاء الأشخاص الجالسين اليوم في الغرف المظلمة فهم لم يدخلوا أي غرفة دردشة على الإنترنت قط.

كيف تمت كتابة الكتاب، وماذا يرتجى منه أن يحقق؟

مع كل هذه القضايا في الساحة فإن توقيت وقيمة كتاب يحاول معالجة القضايا الأساسية حول الأمن الإلكتروني والحرب الإلكترونية التي يجدر بكل شخص أن يلم بها، أمر لابد منه. طريقة التصميم المتبعة في هذه السلسلة لأكسفورد حيث كل الكتب صممت على نهج "سؤال واجابة" يبدوا أنها قد أدت المهمة بإيصال المعلومة.

عندما بدأنا في بحثنا لكتابة هذا الكتاب تقيد نهجنا بأسلوب السؤال والإجابة، بطريقة أخرى فإنك إذا تقيدت بنسق سؤال وإجابة فيتوجب عليك أولاً طرح الأسئلة الصحيحة. حاولنا جمع الأسئلة الأساسية التي طرحها الناس حول الموضوع ليس فقط من السياسيين أو ممن يشتغلون بالتكنولوجيا، ولكن أيضاً ابعد من ذلك من تفاعلاتنا ولقاءاتنا. دُعِمت مجموعة الأسئلة هذه بما كان يعرف قديما (قبل عصر الإنترنت) بـ "الدراسة الاستقصائية" والذي كان يتوجب عليك الذهاب إلى المكتبة واخذ كل الكتب المتعلقة بنظام ديوي العشري من على الرف في ذاك القسم. أما اليوم، وفي هذه الموضوع بالتحديد فإن المصادر تتراوح ما بين الكتب إلى الصحائف على الإنترنت إلى صغائر المدونات. ساعدتنا أيضاً مجموعة من الورش والندوات في مركز بروكنجز Brookings للفكر، الذي عملنا به في واشنطن. هذا التجمع لخبراء القطاع العام والخاص لمناقشة أسئلة تتباين ما بين فعالية الدفاعات الإلكترونية إلى ما يمكن فعله بشأن الحواسيب المصابة الخارجة عن السيطرة (سوف نتطرق لكل هذه الأسئلة لحقا في الكتاب) لقد أقمنا سلسلة من الاجتماعات و اللقاءات مع كبار القادة و الخبراء في الولايات المتحدة، ضمت هذه اللقاءات قيادات عليا كرئيس هيئة الأركان المشتركة وأعلى الرتب

العسكرية في الجيش الأمريكي ورئيس وكالة الأمن القومي نزولا للإدارات الأقل درجة، من الولاة المدنيين وأُمناء مجلس الوزراء وكبار المديرين التنفيذين إلى أصحاب الاعمال الصغيرة و بعض المخترقين المراهقين. كان نطاق بحثنا عالميا لذا تضمنت اجتماعاتنا قادة وخبراء من الصين (كان من بينهم وزير الخارجية وجنرالات من جيش التحرير الشعبي)، كما كان هناك من هم من المملكة المتحدة وكندا وألمانيا وفرنسا وأستراليا واستونيا والامارات العربية المتحدة وسنغافورا. وفي النهاية وبما أنه عالم افتراضي فقد زرنا أيضاً اهم المرافق وعدة مراكز للأمن الإلكتروني في مواقع تتجسد ما بين العاصمة واشنطن إلى سيلكون فإلى إلى باريس إلى ابوظبي.

لاحظنا في رحلتنا هذه نمطا معين، فإن اغلبية الأسئلة (والقضايا التي تمثلها) تصنف في ثلاثة اقسام. الفئة الأولي كانت لأسئلة عن السمات الأساسية وديناميكية الفضاء الإلكتروني والأمن المتعلق بالحاسوب والإنترنت، كلها أسئلة عن "كيفية عمله". فكر في هذا الجزء كمُعينَاتٍ السائق، والتي تُعطي اللبِنَات الأساسية لعالم الإنترنت. القسم الثاني كان لأسئلة حول الأمن الإلكتروني واثاره الواسعة خارج الفضاء الإلكتروني، هذه قسم الاسئلة عن "لما هو مهم هذا الامر؟". ثم كانت الأسئلة حول الردود المحتملة في اخر قسم عن "ما الذي نستطيع فعله؟". ما يلي من اقسام في الكتاب اتبعت نفس الترتيب السابق.

بطرح تلك الأسئلة تأتي مهمة الرد عليهم، هذه الكتاب هو النتيجة. مع هذا التنوع في الأسئلة ستلاحظ اثناء الإجابة عليهم تتداخلا في بعض المواضيع التي سيجرى ذكرها في الكتاب:

قضايا المعرفة: من المهم إزالة الغموض عن ذا المجال إذا أردنا ابدا ان نحصل على ما هو فعال لتأمينه.

قضايا الناس: ان مشكلة الأمن المتعلق بالحاسوب والإنترنت واحدة من المجالات "الخادعة" التي تتفشى مع التعقيدات والمقايضات. والجزء الكبير من هذا ليس بسبب التقنيين في المجال بل بسبب الناس، ان الناس خلف الآلات هم في جوهر أي مشكلة أو حل.

أهمية الحافز: إذا اردت ان تدرك سبب حدوث شيء أو عدم حدوثه في الفضاء الإلكتروني عليك بالنظر في الدوافع والتكلفة والجهد المبذول لأداء المهمة، في هذا المجال أي شخص يعتزم حل جذريا اما أنه إنسان جاهل أو أنه لا ينوي على خير.

أهمية التعاون: هذا نظام لا تملك الحكومة فيه كل الإجابات فالأمن المتعلق بالحاسوب والإنترنت يعتمد علينا كلنا.

قضايا الدول: وهذا يوضح جوهرية دور الحكومات، خصوصا الولايات المتحدة والصين. ليس السبب فقط أن هذين الدولتين ذو نفوذ وقوة كبيرين، ولكن رؤاهم المختلفة للأمن المتعلق بالحاسوب والإنترنت خطر يهدد مستقبل الإنترنت والسياسات العالمية.

أهمية القطط: في النهاية، إننا مَن نجعل مِن الإنترنت ما هو عليه، وهذا يعني أنه ومع كل ما يدور من أمور جدية في الفضاء الإلكتروني فإن هناك ما هو ممتع ومبهج، فإنه عالم غريب الاطوار مع كل الأطفال الرقاصين والقطط التي تعزف على البيانو! لذا أي معالجة لذاك العالم يجب أن تهم بتلك الغرابة.

بطريقة أخرى، فإن هدفنا هو الصراع المباشر مع مشكلة "الأشياء الإلكترونية" التي كانت السبب وراء رحلتنا هذه. هذا كتاب تمت كتابته بواسطة باحثين اتبعا المناهج الأكاديمية بصرامة، وتم نشرة بواسطة دور نشر جامعية مرموقة. ولكن هدفنا لم يكن كتابا للدارسين فقط، فإن أفضل بحثٍ في العالم يصبح بلا قيمة إن

لم يجد من يستفيد منه. في الواقع فإن البحوث الأكاديمية في الأمن المتعلق بالحاسوب والإنترنت تزايدت بمعدل عشرون بالمئة سنويا خلال العشر سنوات المنصرمة. ومع ذلك لا يستطيع أحد الجزم أن الأغلبية من سكان الكوكب باتو مستنيرين في هذا الموضوع.

عوضا عن ذلك، فقد تبنينا الفكرة الأساسية لهذه السلسلة وهي "ما الذي يحتاج معرفته أي شخص". ليس بالضرورة أن يعرف كل شخص الاسرار البرمجية لفايروس "ستكسنت" أو ديناميكية قوانين التأمين للشركات التي تقدم خدمات الإنترنت. ولكن كلما كثر تعاملنا وزاد اعتماداتنا على الأمن الإلكتروني، فإن هناك مفاهيم مبدئية يجب على كل واحد منا التحلي بها. إن الجهل ليس نعمة عندما يتعلق الامر بالأمن الإلكتروني، فإن القضايا المتعلقة بالحاسوب تؤثر حرفيا على كل شخص، فالسياسيون في صراع مع كل شيء من الحرية في الإنترنت إلى الجرائم الإلكترونية، والجنرالات يحمون أُمتنا من اشكال جديدة من الهجمات وفي نفس الوقت يخططون لحروب الإلكترونية. مدراء الأعمال يدافعون عن شركاتهم من تهديدات لم تكن إلا في الخيال وفي نفس الوقت يبحثون عن طرق لجنى المال من تلك الفرص. المحامون والأخلاقيون يضعون أُطراً جديدة للصواب والخطاء. والأهم أن قضايا الأمن الإلكتروني تمسنا كأفراد، نواجه تساؤلات في كل شيء بدء من حقوقنا ومسؤولياتنا كمواطنين في العالمين الواقعي والافتراضي إلى كيف نحمي أنفسنا وعائلاتنا من خطر بشكل جديد.

لذا ليس هذا الكتاب للمختصين فقط، ولكنه كتاب القصد منه سبر اغوار ذاك المجال ورفع مستوى الوعي العام لدفع عجلة الحوار والنقاش للأمام.

نأمل أن تجدو الرحلة مفيدة وممتعة مثل كلمة "الأشياء الإلكترونية" نفسها.

بيتر وارن سينغر والن أ فريدمان

Peter Warren Singer and Allan A. Friedman

أغسطس 2013، العاصمة واشنطن

الجزء الأول

كيفية عمل الإنترنت

ما النطاق العالمي؟ تعريف الفضاء الإلكتروني:

"إنه ليس بناقل، بل مجموعة من القنوات."

هكذا وبهذه الطريقة الشهيرة عرف عضو مجلس الشيوخ السابق في الاسكا تد ستيفنس الفضاء الإلكتروني أثناء اجتماع للمجلس عام 2006. وكما أشار جون استورت الساخر، في برنامجه الليلي "يبدو أن من ليس لدية خبرة في الحواسيب والإنترنت هو نفسه المسؤول عنها" والذي يوضح أن السياسيين في واشنطن بعيدين كل البعد عن الواقع التكنلوجي.

نجد أن من السهل السخرية من فكرة كبير مجلس الشيوخ. عن أن الرسائل الإلكترونية ترسل عبر القنوات، لكن في الحقيقة إن تعريف الأفكار والمصطلحات في القضايا الإلكترونية قد يكون أمراً معقداً. إن كلمة "قنوات" كما استخدمها ستيفنس، هي في الواقع مستوحاةٌ من كلمة "أنابيب" والتي بدورها تستخدم من قبل المختصين في المجال لوصف اتصالات البيانات.

إذا أراد ستيفنس أن يكون دقيقاً في وصفه، كان ليستخدم المفهوم الأساسي لكاتب القصص العلمية وليم قبسن عن الفضاء الإلكتروني. فقد استخدم قبسن المصطلح أولاً، وهو عبارة عن خلط ما بين الدراسة العلمية المختصة بالتحكم والاتصالات وبين الفضاء، والتي ظهرت في قصة قصيرة للكاتب عام 1982. وبعد سنتين في روايته "نيورومانسر" Neuromancer التي أحدثت طفرة نوعية، عرف المصطلح بأنه "هذيان

جماعي حُرّ يمر به بلايين من المستخدمين المسموح لهم من كل دولة يوميا... وصف تصوري للبيانات المستخلصة من خزانات كل حاسوب في النظام البشري والتي تمثل تعقيداً يفوت حد الوصف. خطوط من الضوء ممتدة في الفضاء غير الحسي والمعنوي للعقل وتكتلات ومجموعات من البيانات". بالطبع لو كان استخدم عضو مجلس الشيوخ هذا الوصف ليصف الفضاء الإلكتروني، ما كان اعتبره الكثيرون انه بعيد عن المجال ولكنه قد فقد عقله.

جزء من صعوبة تعريف الفضاء الإلكتروني لا ترجع فقط إلى توسعه وطبيعته العالمية، ولكن أيضاً إلى حقيقة أن الفضاء الإلكتروني اليوم بالكاد يمكن تميزه، مقارنة بما كان عليه في بداياته المتواضعة. تُعتبر وزارة الدفاع الامريكية الأب الروحي للفضاء الإلكتروني، والذي يرجع إلى دعمها المادي لبدايات الحاسوب وأولى الشبكات مثل شبكة وكالة مشاريع البحوث المتقدمة "اربانت" (Advanced Research Projects ARPANET (Agency Network (سنستعرضها قريباً). حتى أن وزارة الدفاع الامريكية واجهة صعوبات في التأقلم مع السرعة المتزايدة للتطور واتساع ما أنتجته. مع مرور السنوات، فقد أصدرت ما لا يقل عن اثني عشر تعريفا مختلفا لما اعتقدت أنه فضاء حاسوبي. والتي تراوحت ما بين "بيئة قومية يتم فيها إرسال البيانات الرقمية على شبكات من الحواسيب"، والذي تم رفضه لما فيه من مفهوم ضمني بأن الفضاء الإلكتروني؛ فقط للاتصال وأنه تخيلي إلى حد كبير، إلى تعريف أخر بأنه "مجال يتميز باستخدام الإلكترونيات والمجال الكهرومغناطيسي"، والذي تم رفضه أيضاً، لشموله على كل شيء بدءاً من الحواسيب إلى الصواريخ وحتى ضوء الشمس.

في محاولة أخيرة عام 2008، جمعت وزارة الدفاع الأمريكية فريقا من المختصين، استغرقوا أكثر من عامٍ للاتفاق على تعريف أخر للفضاء الإلكتروني. هذه المرة عرفوه بأنه " المجال العالمي الذي فيه بيئة من

المعلومات تتألف من ترابط شبكة البنى التحتية للمعلومات، التي تتضمن الإنترنت وشبكات الاتصالات السلكية واللاسلكية وأنظمة الحواسيب وما ضم معالجات وأجهزة تحكم ". هذا تعريف أكثرٌ تفصيلاً بالتأكيد، ولكنه كثير لدرجة أنه يجعلنا نتمنى أن نرجع إلى تعريفه "بالقنوات" فقط.

لخدمة أغراض هذا الكتاب، فكرنا أنه من الأفضل تبسيط الأمر. فطبيعة الفضاء الإلكتروني أنه نطاق من شبكات الحواسيب (ومستخدميها)، تخزن فيه المعلومات وتشارك وترسل على الإنترنت. بدلاً من محاولة إيجاد الكلمات المناسبة لصياغة تعريف أمثل، فإنه من الأفضل استخلاص المفيد مما تتضمنه هذه التعريفات. فماهي السمات الأساسية التي لا تعرف الفضاء الإلكتروني فقط، بل وتجعله مميزاً أيضاً؟

إن الفضاء الإلكتروني أولاً وقبل كل شيء، بيئة للمعلومات. فهو مكون من بيانات رقمية تم إنشاءُها وتخزينُها والأهم أنها تمت مشاركتُها. وهذا يعني أنه ليس بالمكان المحسوس بتاتاً، بالتالي يتحدى أي نوع من قياسات البعد الحسي.

ولكن الفضاء الإلكتروني ليس افتراضياً بحتاً، فإنه يشمل الحواسيب التي تخزن البيانات وأنظمة التشغيل والبنية التحتية التي تتيح له الانسياب، هذا يتضمن الإنترنت للحواسيب المتصلة والشبكات الداخلية المغلقة، وتقنيات الاتصالات الخلوية وكابلات الألياف الضوئية والاتصالات عبر المحطات الفضائية.

غالباً ما نستخدم كلمة "الإنترنت" كاختصار للعالم الرقمي، فالفضاء الإلكتروني أيضاً قد اشتمل الأشخاص خلف هذه الحواسيب، وكيف أن تواصلهم فيما بينهم قد غير مجتمعهم. إذاً فإن واحدة من السمات الأساسية للفضاء الإلكتروني؛ هي أن التكنولوجيا والأنظمة التي تُستخدم هي من صنع الإنسان. لذا فالفضاء الإلكتروني يُعرف إلى حد ما بالنطاق المعرفي كما بالحسي أو الرقمي. التصورات مهمة، فهي تُبلغ الهياكل

الداخلية للفضاء الإلكتروني بكل شيء، بدء من كيف يتم اختيار الأسماء في الفضاء الإلكتروني إلى من يملك أجزاء من البنية التحتية التي يقوم عليها الفضاء الإلكتروني ويستخدمها.

هذا يقود إلى نقطة مهمة غالباً ما يساء فهمها، فالفضاء الإلكتروني ربما يكون عالمياً، ولكنه ليس "بلا وطن" أو أنه "تراث عالمي مشترك"، كِلاَ التعبيرين يُستخدمان بتكرارٍ من قِّبلِ الحكومة والإعلام. كما قسمنا نحن البشر عالمنا بطريقة مصطنعة، إلى مستعمرات نُطلق عليها "دول"، وبالتالي فصائلنا البشرية لعدة مجموعات تمثلت في "الجنسيات"، إذاً نفس الشيء يمكن أن يتم في الفضاء الإلكتروني. فهو يعتمد على البنية التحتية المحسوسة والناس المستخدمين المقيدين بالموقع الجغرافي، بالتالي فهو أيضاً يخضع لمفاهيمنا البشرية كالسيادة والجنسية والملكية. يمكن التعبير عن ذلك بطريقة أخرى، إن اقسام الفضاء الإلكتروني حقيقية بكل معنى الكلمة، ولكنها وهمية، كما هي الخطوط التي تفصل الولايات المتحدة عن كندا أو شمال كارولينا عن جنوبها.

لكن الفضاء الإلكتروني، كما هي الحياة، في تطور مستمر. فإن التركيبة الهجينة بين التكنولوجيا والبشر المستخدمين لها في تغير دائم، وأنها لا محالة تُغيّر كل شيء بدءًا من حجم ونطاق الفضاء الإلكتروني، إلى القوانين التقنية والسياسية التي تسعى لتوجيهها. كما أوضح مختص ذات مرة أن "جغرافيا الفضاء الإلكتروني أكثر عرضة للتغير من بيئات اخرى. فمن الصعب تحريك الجبال والمحيطات، ولكن اقسام الفضاء الإلكتروني يمكن أن تظهر أو تختفي بضغطة زر". السمات الأساسية تظل كما هي، ولكن التضاريس في تَغيرٍ مستمر. إن الفضاء الإلكتروني اليوم هو أيضاً نفسه كما كان في عام 1982، ولكنه أيضاً مختلف تماماً عما كان في ذلك الوقت.

على سبيل المثال، فإن البرامج والأجهزة التي تُكوّن الفضاء الإلكتروني، قد صممت في الأصل للحواسيب التي تعمل بالأسلاك الثابتة وخطوط الهاتف. كان أول ظهور للأجهزة النقالة في ستار ترك (Star Track)، ومن ثم عند تجار المخدرات في سلسلة ميامي فايس الذين كان باستطاعتهم اقتناء شيء غريب ومدهش كـ "هاتف السيارة". أما اليوم فإن نسبة متزايدة من الحوسبة متجهة نحو الأجهزة النقالة، لدرجة أننا رأينا أطفال يضربون شاشات حواسيب مكتبية كما لو كانت أجهزة أي باد (iPads) معطلة.

تتطور توقعاتنا كلما تطورت تكنلوجيا الفضاء الإلكتروني. هذا يولد نظم جديدة للسلوك، تبدأ من كيف "يلعب" الأطفال، إلى مفهوم أقوى بكثيرٍ يتوجب فيه علينا كلنا أن نحظى بالوصول إلى الفضاء الإلكتروني، وأن نعبر عن آرائنا الشخصية. آرائنا في كل شيء بدءًا من قَصّةِ الشّعَرِ الجديدة لنجم في هوليود، إلى رأيك في حاكم مستبد.

إن ما يكون الإنترنت نفسه في تطور أمام أعيننا، وبطريقة أكثر حيوية. فإنه يتضخم بشكل هائل (حيث أن حوالي 2,500,000,000,000,000,000 بايت تضاف يومياً إلى المخزون العالمي للمعلومات الرقمية) ليصبح أكثر خصوصية، وذلك في آن واحد. بدلا من تلقي هذا الكم الهائل من المعلومات بطريقة لا تكشف عن هوياتهم، فإن الأفراد ينسِجُون ويصنعون صفحات على الشبكة لاستخدامهم الشخصي، مما يؤدي في نهاية المطاف إلى كشف المزيد عن هوياتهم على الإنترنت. تتراوح هذه الصفحات ما بين شبكات التواصل الاجتماعي، مثل فيس بوك في الولايات المتحدة، ورين رين RenRen في الصين، إلى صغار المدونات مثل توتير ومقابله في الصين تن سنت وسينا. في الواقع فإن موقع مدونات صغيرة في الصين (يسمى ويبو Weibo) قد بدء بحوالي 550 مليون مشترك قد سجلوا في عام 2012.

فالفضاء الإلكتروني كان مجرد نطاق للتواصل، ثم للتجارة الإلكترونية (يصل في مبيعاته إلى 10 تريليون دولار سنوياً)، وقد اتسع ليشمل ما نسميه بـ "البنية التحتية الحيوية". هذه هي العوامل الكامنة التي تُسير تحضرنا العصري في شكله اليومي، تتباين ما بين الزراعة وتوزيع الطعام إلى المعاملات المصرفية والرعاية الصحية والموصلات والمياه والطاقة. في زمن كانت كل واحدة قائمة بذاتها، أما الآن فكلها ترتبط مع بعضها البعض وتتصل بالفضاء الإلكتروني عن طريق تكنلوجيا المعلومات، عادة من خلال ما يعرف بـ "التحكم الإشرافي وجمع المعلومات" أو أنظمة سكادا SCADA (Supervisory Control And Data Acquisition). هذه هي أنظمة الحواسيب التي تراقب وتتحكم في الإغلاق وعمليات أخرى تتبع للبنية التحتية الحيوية. ومن الملاحظ أن القطاع الخاص يتحكم فيما لا يقل عن تسعين بالمئة من البنية التحتية الحيوية للولايات المتحدة، وتلك الشركات تستخدم الفضاء الإلكتروني لأغراض من بينها –وليس كلها–الحفاظ على مستوى الكلور في مياه مدينتك والتحكم في انسياب الغاز الذي يدفئ منزلك وتسير المعاملات المالية التي تحافظ على سعر العملة.

وبالتالي فإن الفضاء الإلكتروني يتطور من "النظام العصبي ـ نظام التحكم في اقتصادنا"، إلى شيء أخر. كما قال مره الرئيس جورج بوش. وكما وصفه رئيس تحرير مجلة وايرد (Wired) بن همرسلي، فإن الفضاء الإلكتروني يتجه ليصبح "النظام الأساسي المسيطر على الحياة في القرن الواحد والعشرين".

يمكننا الاحتجاج، ولكن فيس بوك وتوتير وقوقل وما شابههم، يعتبرون وبطرق شتى، التعريف الأنسب للحياة العصرية في الغرب الديمقراطي. يعتبر الكثيرون أن الإنترنت المتصل مع حرية التعبير والاتصال الجيد بما نختاره من شبكات التواصل الاجتماعي، هو دليل ليس فقط على العصرية بل على الحضارة نفسها. ليس هذا بسبب أن الناس صاروا "مدمنين على شاشات الفيديو"، أو أنه يتم تصنيفهم بحالة من حالات مرض نفسي؛

ولكن بسبب أن الإنترنت أصبح المكان الذي نعيش فيه، إنه المكان الذي نؤدي فيه أعمالنا والمكان الذي نلتقي فيه والمكان الذي نحب فيه. إنه المنصة المركزية لإدارة الأعمال والثقافة والعلاقات الاجتماعية، وبهذا لم يبقى الكثير في حياتنا لم يكن الإنترنت جزءًا منه. إساءة فهم مركزية هذه الخدمات في المجتمع الحالي هو بمثابة ارتكاب خطأٍ فادح. فإن الإنترنت ليس رفاهية في الحياة؛ فهو يعد لأغلب الناس سواءً أدركوا ذلك أم لا، هو الحياة.

ولكن كما في الحياة، ليس الكل يتعامل بلطف. فالإنترنت الذي نشأنا على حبه وحاجته، أصبح الآن وبطريقة متسارعة مكاناً محفوفاً بالمخاطر.

من أين أتت هذه "الأشياء الإلكترونية" على كل حال؟

نبذة تاريخية قصيرة عن الإنترنت

"Lo."

كانت هذه أول كلمة حقيقة تم إرسالها عبر شبكة حاسوب، والتي ستتطور لاحقا لتصبح الإنترنت. ولكن بدلاً من أن تكون بداية كلام بليغ مثل "Lo وبعد، ..." عوضاً عن ذلك كانت "Lo فقط" نتيجة خطأ في النظام. في عام 1969، كان الباحثون في جامعة كاليفورنيا في لوس انجلس، يحاولون الدخول إلى حاسوب في معهد ستانفورد للبحوث. ولكن قبل طباعتهم للحرف "g" من كلمة "Log"، تعطل الحاسوب في الطرف الأخر من الشبكة في ستانفورد. على كل حال فإن مشروع "اربانت"، سمي كذلك لأن وكالة مشاريع البحوث المتقدمة "اربا" اسسته(ARPA (Advanced Research Projects Agency، والتي في النهاية ستغير طريقة مشاركة البيانات بين الحواسيب وطبقاً لذلك كل شيء أخر سيتغير.

ظلت شبكات الاتصالات الإلكترونية تشكل طريقة مشاركتنا للمعلومات منذ اختراع التلغراف، الجهاز الذي يتذكره البعض فيتذكرون كتاب فكتورين إنترنت "Victorian Internet". كانت الضجة حول تلك التكنولوجيا عالية كما لهذه الان، صرح المعاصرون بأن مع التلغراف "من المستحيل أن تتواجد تلك العداوات والانحيازيات بعد الآن".

ما يجعل الإنترنت متميزاً عما سواه من تقنيات الاتصالات السابقة كالتلغراف ومن ثم شبكات الهواتف، هو أنه حزمة متنقلة بدلا عن دائرة كهربائية متنقلة. الحزم هي ظروف رقمية صغيرة من البيانات. في بداية كل حزمة فإن احتواء الظرف على عنوان أمرٌ أساسي، والذي يحتوي تفاصيل عن مصدر الشبكة والوجه المقصودة وبعض المعلومات الأساسية عن محتويات الحزمة. بعد تفكيك البيانات المنسابة إلى أجزاء أصغر، كل منها يمكن إيصاله بطريقة منفصلة وغير مجتمعة، ومن ثم إعادة تجميعها عند نقطة النهاية. توجه الشبكة كل حزمة منذ وصولها، هندسة معمارية حركية تخلق ليناً ومرونةً معاً.

وعلى عكس الأسطورة الشائعة، فإن تحويل الحزم لم يُطوّر من قِبلِ حكومة الولايات المتحدة للحفاظ على الاتصالات في حال هجوم نووي. ولكن في الحقيقة تم تطويره ليعزز فعالية وكفاءة الاتصال بين الحواسيب. قبل ظهوره في السبعينيات، فإن الاتصال بين حاسوبين كان يتطلب دائرة الإلكترونية مخصصة، أو نطاقاً ترددياً مسبق التعين. هذا الربط المباشر يعني أن المصدرين لا يمكن لأي أحد أخر استخدمهما، حتى عندما لا تكون هناك بيانات مرسلة. بتفكيك هذه الحوارات إلى أجزاء أصغر، فإن حزماً مختلفة من حوارات متعددة يمكنها مشاركة نفس روابط الشبكة. وهذا أيضاً يعني أنه إذا انقطعت الروابط في الشبكة بين جهازين فأصبح الاتصال من جهة واحدة، يتم تلقائياً إعادة توجيه الاتصال بدون أي خسارة قد تظهر في الاتصال (بما أنه لم يكن هناك اتصال للبداية منه اصلاً).

شُيدت منظمة "اربا" (تحولت لتصبح "داربا" بعد إضافة "د" من كلمة دفاع Defense) من قِبلِ وزارة الدفاع الأمريكية، لتتجنب المفاجئات التقنية مع التقدم السريع في البحوث. إن الحواسيب باتت منتشرة في أواخر الستينيات، ومع ذلك ما كانت تلبي حاجة الكثيرين من الباحثين. حاولت "اربا" إيجاد طرق للسماح للناس في مؤسسات مختلفة من اغتنام الزمن الذي لا تُستخدم فيه الحواسيب في البلد.

بدلا من جعل اتصالات مخصصة وباهظة التكلفة بين الجامعات، فإن الرؤية كانت شبكة من روابط مشاركة البيانات، مشاركة للمصادر الإلكترونية. كل الأجهزة على حد سواء ستربط بـ واجهة معالج الرسائل الذي بدوره يتعامل مع الاتصال الفعلي من الشبكة. هذه الشبكة كانت "اربانت" هي نفسها الأولى التي أُرسلت فيها "Lo" والتي كانت بداية العصر الإلكتروني. توسع ذاك الرابط الذي كان عام 1969 بين جامعة كاليفورنيا في لوس انجلس وستانفورد ليشمل أربعين نقطة التقاء بحلول عام 1972. بعدها بقليل انضمت المزيد من الجامعات ومراكز البحوث حول العالم لهذه الشبكة الأولى، أو صنعوا شبكاتهم الخاصة، بدلا من ذلك.

لخدمة اغراض الإنترنت الحديث، فإن مجموعة من الحزم مرسلة بين أجهزة في شبكة واحدة، لا يُعد هذا "إنترنت". ان الإنترنت يعني توصيل العديد من الشبكات المختلفة، في هذه الحالة تلك الشبكات المختلفة سرعان ما نشأت وتفوقت "اربانت" ولكنها ظلت غير متصلة.

كان التحدي يكمن في أن تلك الشبكات المختلفة تستخدم تقنيات مختلفة تماماً. أصبحت المشكلة الفنية هي محاولة صهر تلك الفروقات والسماح بتواصل فعال. تم إيجاد الحل في عام 1973، حيث قام فينت كيرف الذي لاحقاً أصبح استاذ في ستانفورد مع روبرت خان من "اربا" بإعادة تحسين برتوكول اتصال الحاسوب. أرسى ذاك "البرتوكول" التوقعات التي توجب على نهاية كل رابط اتصال أن يتصل بأخر. يتطلب الاتصال في

البداية ثلاثة حواسيب متصلين معا، ومن ثم كيف أن كل طرف يفكك الرسائل ليمكن جمعها، وكيفية التحكم بالسرعة لتحديد السعات العريضة المتاحة، تلقائيا.

تكمن العبقرية خلف هذا النموذج في كيفية تفكيك الاتصال إلى "طبقات" والسماح لكل طبقة بالعمل بطريقة مستقلة. بالمقابل فإن تلك الحزم يمكن إرسالها على أي شبكة كانت، بدءًا من الموجات الصوتية إلى ترددات الراديو إلى نبضات الضوء في ألياف زجاجية. تلك البرتوكولات المتحكمة في الاتصال أو تي سي بي TCPs، يمكن تطبيقها على كل أنواع برتوكولات الحزم، ولكننا حاليا نستخدم نوع يدعي برتوكول الإنترنت أو أي بي IP، وبشكل حصري في الإنترنت الحديث.

مكن هذا البروتوكول من خلق شبكة من كل الشبكات. ولكن بالطبع لم يتوقف الإنترنت هنا. فالروابط بين الأجهزة كانت ممتازة، ولكن البشر يتفوقون في تسخير التكنولوجيا لأهوائهم الشخصية. في أثناء استخدام الأجهزة لمشاركة البحوث بدء الناس بترك رسائل لبعضهم البعض، عن طريق ملفات بسيطة يمكن تعديلها لصياغة حوار. صار الأمر شاقاً، فكتب ري توملنسون من شركة بي بي إن BBN للاستشارات التقنية عام 1972 برنامجاً أساسياً لقرائه وإنشاء وإرسال الرسائل. كان هذا هو البريد الإلكتروني: أول "برنامج رائع" للإنترنت. خلال عام، أصبحت اغلبية حركة البيانات في الشبكة اتجاه البريد الإلكتروني، في شبكة تم إنشاءها في الأصل للبحوث. صارت الآن الاتصالات الشبكية عن الناس.

كانت الخطوة الأخيرة لخلق الإنترنت الحديث هي إزالة حواجز الدخول. كان الاستخدام في أوله محصورا على من لهم صلاحيات للدخول في شبكة الحواسيب المتصلة، في مؤسسات البحوث ووزارة الدفاع. تواصلت هذه المنظمات عن طريق روابط مخصصة. بتجلي قيمة الاتصال الشبكي، وبانخفاض أسعار

الحواسيب، سعت مزيد من المنظمات للانضمام. أتاح المودم والذي يحول البيانات إلى موجات صوتية والعكس، لخطوط الهاتف الأساسية العمل كروابط للحواسيب الأخرى.

سرعان ما أراد باحثون خارج علوم الحاسوب الدخول، ليس فقط للاستفادة من المصادر الإلكترونية المشاركة، ولكن أيضاً لدراسة تكنلوجيا الاتصالات الجديدة نفسها. أوصلت مؤسسة العلوم الوطنية في الولايات المتحدة، مراكز الحواسيب العملاقة في ارجاء البلاد، فيما صار يعرف بـ "إن إس إف نت" NSFnet (National Science Foundation network)، والتي نمت بسرعة هائلة لدرجة أن توسعها تطلب إدارة تجارية. فإن كل تحديث كان يقابله طلب أكبر والحاجة لقدرة أكبر وبنية تحتية منظمة ومستقلة. فإن تصميم "عمودٍ فقري" يدير الحركة بين الشبكات المحلية المختلفة، بدت تظهر كحل فعال.

شهدت هذه الفترة أيضاً بداية الدافع الربحي في توسع الإنترنت. على سبيل المثال، في هذا الوقت انضم فينت كيرف لشركة ام سي أي MCI للاتصالات. ففي عام 1983، قاد الجهود لبداية بريد ام سي أي، أول خدمة بريد الإلكتروني تجاري على الإنترنت. في أواخر الثمانينيات، أصبح من الواضح ان إدارة الإنترنت الوليد ليست من شأن المجتمع البحثي. فالقائمين بالأعمال التجارية يمكنهم توفير الخدمات الضرورية لشبكة الإنترنت، ويصبحوا مستهلكين شرهين أيضاً. لذا طور مكتب البيت الأبيض للعلوم والتكنولوجيا خطة لتوسعة وتسويق خدمات العمود الفقري، خطة ترى فيها الحل الوحيد للنهوض بالإنترنت الجديد.

تصور المخططون خطة تستغرق عشر سنوات، لذا، لن تكتمل المرحلة الأخيرة التي تقتضي التسليم التجاري، حتى أواخر التسعينيات. لحسن الحظ، فإن العضو الشاب في مجلس الشيوخ من مدينة تينسي، كان مقتنعا بتسريع العملية. ففي عام 1989 قدم آل قور مذكرة تناشد بتسريع تخصيص الشبكة. والذي سيبالغ لاحقا بقوله انه هو من " قدم المبادرة لخلق الإنترنت"، حركة مجلس الشيوخ هذه لتسريع الامور كانت في غاية الأهمية

لتوسع الإنترنت. في الوقت الذي صار فيه قور نائب الرئيس في عام 1994، كانت المؤسسة الوطنية للعلوم تسلم التحكم في العمود الفقري للاتصالات المحلية بصورة رسمية للقطاع الخاص.

تزامن التخصيص مع عدة اختراعات جديدة وتحسينات، التي سرعان ما جعلت من الإنترنت مكاناً دمقراطياً وشعبياً. في عام 1990 قام باحث في مركز البحوث الأوربية "سي إي ار ان" CERN (European Organization for Nuclear Research) في سويسرا بأخذ الشكل الغامض نسبيا من عرض المعلومات علي شكل مجموعة من المستندات الإلكترونية المترابطة، وصنع لها واجهة شبكية جديدة. مع برتوكول نقل النصوص التشعبي "إتش تي تي بي" HTTP (Hypertext Transfer Protocol)، ونظام مرفق للتعرف على المستندات المترابطة URLs (Uniform–or Universal–Resource Locator)، "اخترع" تيم بارنرز لي شبكة الإنترنت التي نراها اليوم. والمثير للعجب أنه عندما حاول بارنرز لي تقديمه في مؤتمر أكاديمي، فإن طفرته العلمية لم تعد ذات نفع كبير، ولو حتى لعرض رسمي. بالمقابل فقد تم منعه من وضع ملصق اعلاني لها في المدخل. وبعد عدة سنوات، قدم باحثون بجامعة إيلينوي متصفح الإنترنت "موسايك" Mosaic، الذي سهل التصميم والتصفح للشبكة معا، وقدم تجربة جديدة في "تصفح الإنترنت" للجمهور العام.

وسواء احببنا أن تعترف بذلك ام لا؛ فهذه هي الفترة التي باتت فيها صناعة المواد الإباحية جزءًا لا يتجزأ من تاريخ الإنترنت. قدر البعض، ان ذاك النطاق القاتم يستحوذ على نسبة تصل حتى خمس وعشرون بالمئة من جملة البحث في الإنترنت، جذبت تلك الصناعة القذرة المستخدمين الجدد للإنترنت، والاستخدامات الجديدة للإنترنت على حد سواء؛ مثل الرسائل الفورية وغرف الدردشة والتسوق على الإنترنت وبث الفيديو وتبادل الملفات والمحدثات المرئية على الإنترنت (زيادة الطلب على كل من تلك الخدمات، يقع على كاهل موجات التردد العريضة، مما يقود إلى المزيد من الأعمال الأساسية).

وسرعان ما افاقت وسائل الاعلام الرئيسية، على أن هناك أمراً كبير يحصل في الإنترنت. كما ذكرت صحيفة نيويورك تايمس عام 1994 (كانت صحيفة مطبوعة علي ورق بالطبع!)، "ستقود زيادة الإتجار في الإنترنت إلى تسريع عملية تحوله؛ من نظام اتصالات مقصور على علماء الحاسوب الأمريكيين، إلى نظام عالمي لسير البيانات والنصوص والصور والصوت والفيديو وسط الشركات وزبائنهم ومموليهم"

فياله من مستهل...Lo

ما كيفية عمل الإنترنت في واقع الأمر؟

لعدة ساعات في فبراير من عام 2008، احتفظت باكستان بكل فيديوهات العالم للقطط الظريفة كرهينة.

بدء الموقف عندما قررت الحكومة الباكستانية، في محاولة منها لمنع مواطنيها من الدخول إلى ما قررت أنه محتوى غير لائق، فأمرت شركة الاتصالات باكستان تيلكوم بحظر الدخول إلى موقع مشاركة الفيديو يوتيوب YouTube. للقيام بذلك، قامت باكستان تيلكوم بتضليل حواسيب زبائنها بأن أقصر طريق للوصل ليوتيوب هو عن طريق باكستان تيلكوم، ومن ثم منع المستخدمين الباكستان من الوصل إلى موقع يوتيوب الأصلي. ولسوء الحظ فإن الشركة كانت قد شاركت الهوية المزيفة خارج نطاق شبكتها، فانتشرت الأخبار عبر الآليات الكامنة للإنترنت، عن أقصر طريق للوصل لموقع يوتيوب. وسرعان ما تم تضليل ثلثي مستخدمين الإنترنت في العالم إلى موقع يوتيوب المزيف، مما أدى في المقابل إلى ازدحام مفرط في شبكة باكستان تيلكوم الخاصة.

كان الأثر مؤقتا، ولكن الحادثة أكدت على أهمية معرفة طريقة عمل الإنترنت. الطريقة الافضل لاكتساب تلك المعرفة هي فهم كيفه وصول المعلومات من مكان لأخر في العالم الافتراضي. الأمر معقد قليلاً، ولكن سنبذل قصارى جهدنا لتبسيطه.

لنفترض أنك تريد زيارة الموقع الاخباري –ولنتجرأ ونقول– الموقع الترفيهي لمؤسسة بروكنجز، مركز الأبحاث الذي عملنا به. في الواقع، فقد طلبت من جهازك بأن يتحدث مع حاسوب يتحكم فيه بروكنجز في العاصمة واشنطن. على جهازك معرفة أين يقع ذاك الحاسوب ومن ثم بدء اتصال ليتمكن من التواصل.

يحتاج حاسوبك أولاً إلى معرفة طريقة إيجاد الخوادم التي تستضيف صفحة الإنترنت التابعة لبروكنجز. للقيام بذلك عليه استخدام رقم بروتوكول الإنترنت "أي بي" الذي يخدم كعنوان للنقطة الأخيرة على الإنترنت. في الغالب فإن جهازك عُين له رقم أي بي بطريقةِ أتوماتيكية من قِبلِ مُقدِم خدمة الإنترنت أو أيا كانت الشبكة التي تستخدمها. وأيضاً يدرك عنوان مُوجِّههُ، أو الطريق إلى الإنترنت. في النهاية فإن حاسوبك يدرك عنوان مزود خدمة نظام أسماء النطاقات.

نظام أسماء النطاقات أو دي إن إس DNS (Domain Name Server)، هو بنية تحتية والبروتوكول الذي من خلاله تربط الحواسيب أسماء النطاقات (أسماء يمكن للبشر تذكرها مثل Brookings.edu) بما يقبلها من عنوان أي بي (الذي يكون في شكل بيانات آلة مثل 192.245.194.172). إن نظام أسماء النطاقات عالمي ولا مركزي. فإن أسلوب بنائه يمكن تصوره كأنه شجرة. فجذر الشجرة يعمل كنقطة توجيه لنظام أسماء النطاقات. فوق ذلك هناك النطاقات من الدرجة الأولى، وتلك هي رموز الدول مثل uk.، وكما هو الحال للنطاقات مثل com. و net. كل من تلك النطاقات العليا يمكن تقسيمه. كثير من الدول لها نطاقات

مخصصة من الدرجة الثانية، مثل co.uk و ac.uk، وذلك لتميز المؤسسات التجارية من الاكاديمية، على التوالي.

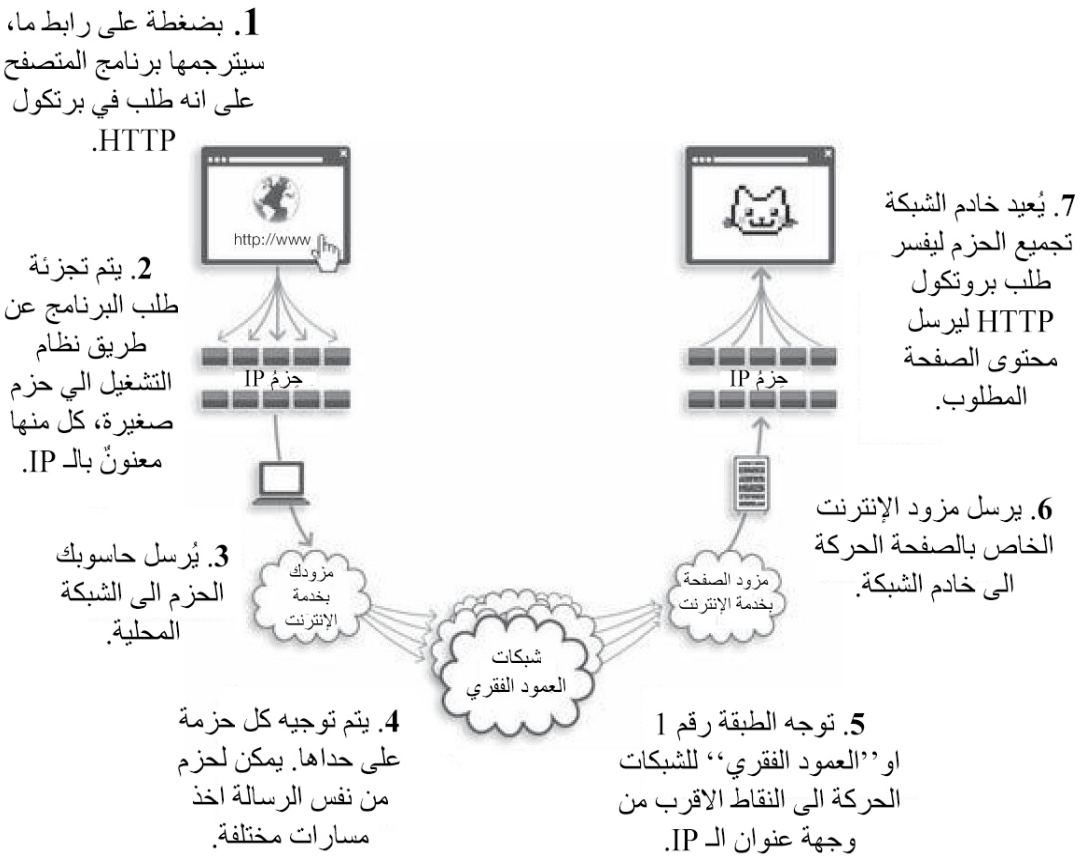
يتم التحكم عالميا في الدخول إلى نادي نطاقات الدرجة الأولى، بواسطة مؤسسة الإنترنت لإسناد الأسماء والأرقام ICANN (Internet Corporation for Assigned Names and Numbers) "أي سي اى إن إن" هي منظمة غير ربحية خاصة، تم تأسيسها عام 1998 لتشغيل ادارت الإنترنت المختلفة ومهام العمليات، التي كانت سابقا تنفذ بواسطة المنظمات الحكومية.

إن كل نطاق من الدرجة الأولى يدار بواسطة مسجل، له سياساته الداخلية الخاصة للنطاقات. تحصل كل من المنظمات مثل بروكنجز أو أبل أو وزارة الخارجية الامريكية، على أسماء نطاقاتهم عن طريق وسطاء يدعون بالمسجلين. يتعاون هؤلاء المسجلون مع بعضهم، لضمان عدم تشابه أسماء النطاقات، وأن يبقى كل نطاق متفرداً. وبالمقابل فإن كل نطاق، يدير ما تحته من النطاقات المتفرعة، مثل mail.yahoo.com.

للوصول إلى نطاق بروكنجز، فعلى حاسوبك الاستعلام من نظام دي إن اس DNS عن طريق سلسلة من المُحلِلات. إن أساس الفكرة هو الصعود لأعلى الشجرة. حيث تبدء من الجذر، الذي سيوجهك إلى سجلات edu. و التي تدار بواسطة إيديوكوز Educause. إن إيديوكوز هي المنظمة التي تضم كل نطاق مسجل ينتهي بـ edu. وهي حوالي الفان مؤسسة تعليمية. سيعلم حاسوبك من هذه القائمة ال أي بي IP المخصص للخادم الداخلي لبروكنجز من تلك القائمة، والذي يتيح له الاستعلام عن محتوى أو برامج معينه داخل نطاق بروكنجز. وبعدها سيوجه اسم خادم بروكنجز حاسوبك إلى المحتوى الذي يبحث عنه بالتحديد، والذي يتم بإرجاع ال أي بي IP إلى الجهاز الذي يستضيف ذاك المحتوى.

في الحقيقة، هذه العملية معقدة أكثر مما تبدو. فعلى سبيل المثال، فإن الخوادم عادة ما تخزن البيانات محلياً في وحدات تخزين مخبئة للاستخدام المستقبلي، فليس على كل طلب الذهاب إلى الجذر. ويتضمن البرتوكول حالات خطأ معينة للتعامل مع الأخطاء المتوقعة. ومع أن ذلك كان ملخصاً تقريبياً، فإنه يعطي حساً عن كيفية عمله بصورة مجملة.

والآن ومع معرفة حاسوبك لمكان البيانات، كيف للبيانات الوصول إلى حاسوبك؟ فعلى الخادم في بروكينجز معرفة أن عليه إرسال البيانات إلى جهازك، وعلى البيانات الوصل إليه هناك. إن الشكل 1.1 يوضح كيف لحاسوبك طلب صفحة على الإنترنت، بتفكيك الطلب إلى حزم ومن ثم إرسالها عبر الإنترنت. أولاً، عند "طبقة" البرنامج، فإن متصفحك يفسر ضغطتك على الفائرة بأنها أمر في بروتكول نقل النصوص المتشعبة "إتش تي تي بي"، والذي يبين طريقة طلب المحتوى وكيفية إيصاله. وبعدها يتم تمرير هذا الأمر إلى طبقة النقل ومن ثم إلى طبقات الشبكة. إن طبقة النقل مسؤولة عن تفكيك البيانات إلى قطع بحجم الحزم، والتأكد من أن كل القطع قد وصلت خالية من الأخطاء، وأنه تم تجميعها بالترتيب الصحيح لتناسب طبقة البرنامج الذي يليها.



الشكل 1.1

إن طبقة الشبكة هي المسؤولة عن بذل قصارى جهدها لتوجيه الحزم عبر الإنترنت. إذا فكرت في البيانات التي تحاول إرسالها أو استقبالها على أنها طرود من المعلومات، فإن طبقة النقل هي المسؤولة عن حزم واستقبال تلك الطرود، بينما نقلها من مصدرها إلى وجهتها المنشودة هي مسؤولية طبقة الشبكة. حالما تصل الحزم إلى وجهتها، يتم إعادة تجميعها والتأكد من صحتها ومن ثم ترسل –في هذه الحالة–إلى البرنامج، والذي هو المحتوى الذي طلبته، أُرسل لك عن طريق خادم الشبكة.

ولكن كيف للحزم معرفة كيفية التنقل عبر الإنترنت، للوصول لوجهتها؟ وكما هو الحال في نظام دي إن اس الذي يساعد حاسوبك في إيجاد الصفحة التي يبحث عنها، فإن منظومة شبكات الإنترنت يمكن تصورها على شكل هرمي. فكل حاسوب هو جزءٌ من شبكة، شبكة مثل تلك التي تربط كل من زبائن مزود خدمة الإنترنت أي اس بي ISP (Internet Service Provider). إن مزودي خدمات الإنترنت هم المنظمات الأساسية التي تقدم خدمة الوصول إلى الإنترنت، بجانب خدمات أخرى ذات صلة مثل البريد الإلكتروني أو استضافة صفحات الإنترنت. إن معظم مزودي خدمات الإنترنت هم شركات تجارية برمجية خاصة، وهذا يتضمن عدد من شركات الهواتف وشركات الكوابل التلفزيونية التي بدأت بتوفير الوصول إلى الإنترنت حالما بدء المجال بالازدهار، بينما هناك شركات إما مملوكة للحكومة أو ملكية عامة.

هذه الشبكات بدورها، تشكل نقاط التقاء في الإنترنت العالمي تدعى بـ أنظمة التحكم الذاتي "أي اس" Autonomous Systems (AS). إن أنظمة التحكم الذاتي تُعرف أسلوب بناء روابط الإنترنت. يتم توجيه حركة البيانات محلياً من خلال نظام تحكم ذاتي ويتحكم فيها عن طريق سياسات تلك المنظمة. إن كل نظام تحكم ذاتي يملك كتل من عناوين أي بي التي تمثل "المصدر" لتلك الوجهات. فكلها أو واحدة منها على الأقل مربوط بـ نظم تحكمٍ ذاتيةٍ أُخرى، بينما قد يكون هناك العديد منها في المزودين الكبار لخدمة الإنترنت. لذا فإن التوجيه لعنوان أي بي معين يصبح ببساطة مسألة إيجاد نظام التحكم الذاتي الخاص به.

بالرغم من ذلك، فإن هناك مشكلة: إن الإنترنت ضخم. اليوم هناك ما يزيد عن اربعين ألف نقطة ربط لنظام ذاتي التشغيل "أي اس" في الإنترنت، وترابطهم الداخلي في تحول وتغير مستمر على مر الزمن. بهذا المعيار، فنهج عالمي لتوجيه كل شيء بنفس الطريقة أمرٌ مستحيل.

لذلك، فإن الإنترنت يستخدم نظام توزيع يتسم بالديناميكية، الذي لا يحتفظ بشكل ثابت لطبيعة الشبكة في أي وقت كان. إن مبدأ التوجيه بسيط إلى حد ما: ففي كل نقطة من الشبكة، هناك مُوجِّه ينظر في عنوان الحزمة المستقبلة؛ إذا كانت الوجهة المنشودة داخل الشبكة فإنه يحتفظ بها ويرسلها للحاسوب ذي الصلة. إن كان غير ذلك، فإن المُوجِّه يستشير طاولة توجيهات، ليحدد أفضل خطوة تالية لإرسال الحزمة في أقصر طريق نحو وجهتها.

إن الدهاء يكمن في تفاصيل تركيب طاولة التوجيه تلك. بما أنه لا يوجد دليل عناوين عالمي، فعلى نقاط الاتصال في الشبكة مشاركة المعلومات الأساسية مع المُوجِّهات الأخرى. مثلاً، مشاركة عناوين أي بي IP المسؤول عنها والشبكات الأخرى التي يمكن التواصل معها. تتم تلك العملية بطريقة منفصلة عن توجيه الإنترنت فيما يسمي بـ "لوحة التحكم". تشارك المُوجِّهات المعلومات أيضاً مع جيرانها ويتشاركون الجديد من أخبار حالة الشبكة، ومن يمكنه التواصل مع من. ومن ثم يُعدّ كل مُوجِّهٍ نموذجاً داخلياً موقتاً خاصاً به عن أفضل طريقة لتوجيه حركة البيانات المارة من خلاله. وبالمقابل فإن ذاك النموذج يتم مشاركته مع جيرانه ليتعرفوا على كيفية تمرير حركة البيانات الجديدة لذاك المُوجِّه.

إذا بدا ذلك معقداً، فلأنه بالفعل معقد. في بضع صفحات، قد لخصنا ما أخذ من أبحاث علوم الحاسوب عقوداً للوصول إليه. إن الأساس في الأمن الإلكتروني هو أن النظام كله قائم على الثقة. إنه نظام يعمل بكفاءة، ولكنه قد يتعطل، إما بدون قصد أو عن طريق تغذية النظام ببيانات ضارة.

إن ما فعلته الباكستان يوضح ماذا يحصل إذا ما تم استغلال الثقة. فإن رقابة الحكومة قد عطلت الإنترنت، بادعائها زورا أنها تملك اتصال مباشراً مع عنوان أي بي الذي يمثل يوتيوب. كان ذاك إعلان بدافع سياسي مقصورٌ محلياً. ولكن بسب طريقة عمل الإنترنت، فسرعان ما كان كل مزود لخدمة الإنترنت في آسيا

يحاول توجيه كل حركة البيانات المتجهة ليوتيوب إلى باكستان. فقط لأنهم اعتقدوا أنه أقرب من الوجهة الحقيقية المنشودة. كانت نماذج المُوجِّهات مبنية على معلومات خاطئة. وبازدياد عدد الشبكات التي اتبعت ذلك، صار جيرانهم أيضاً يعتقدون أن عنوان يوتيوب هو عنوان أي بي IP الباكستاني. لم تحل المشكلة إلا بعد أن أعلن مهندسو قوقل وبغضب الطريق الصحيح عبر الشبكة.

باختصار، فإن إدراك أسلوب بناء الإنترنت اللامركزي الأساسي يقدم رؤيتين متعلقتين بالأمن الإلكتروني. يقدم تقديراً عن كيفية عمل الإنترنت من دون تنسيق يبدأ من القمة نزولا إلى القاعدة. ولكنه أيضاً يوضح أهمية التصرف الحسن لمستخدمين الإنترنت وحماته، وكيف أن لنقاط الاختناق المدمجة أن تصبح نقاط ضعف كبيرة مالم يحسنوا التصرف.

من القائم على أمره؟ فهم إدارة الإنترنت

في عام 1998، قام جون بوستل وهو باحث في علوم الحاسوب وقيادي مرموق في المجتمع الشبكي، بإرسال بريد إلكتروني بدا غير ضارٍ إلى ثمانية أشخاص. قد طلب فيه منهم إعادة ضبط خوادم شبكتهم لتوجه حركة الإنترنت الخاصة بهم باستخدام حاسوبه في جامعة كاليفورنيا الشمالية، بدلاً من حاسوب في هرندون في فيرجينيا. وقد فعلو ذلك بدون طرح أي سؤال، فقد كان بوستل رمزاً في المجال (كان جزء من الفريق الذي أعد شبكة "اربانت" الاصلية) وقد شغل منصب المسؤول الرئيسي لنظام التسمية في الشبكة.

بذاك البريد الإلكتروني الواحد، قام بوستل بأول عملية استيلاء على الإنترنت. إن الأشخاص الذين راسلهم يديرون ثمانية من أصل اثني عشر منظمة تتحكم في خوادم التسمية، والتي هي الحواسيب التي في نهاية المطاف مسؤولة عن ترجمة اسم نطاق ما مثل "Brookings.edu" إلى عنوان أي بي IP يفهمه

الحاسوب. أما الحاسوب الموجود في فيرجينيا والذي وجه عنه ثلاثي الخوادم الأساسية للإنترنت كان تحت تحكم حكومة الولايات المتحدة. بينما قال بوستل فيما بعد، أن سيطرته على أغلب خوادم الإنترنت الأساسية لم تكن الا "تجربة"، بينما يعتقد أخرون أنه قد فعل فعلته احتجاجاً، وليثبت لحكومة الولايات المتحدة أنها لن تتمكن من انتزاع التحكم في الإنترنت من مجتمع الباحثين الشاسع، والذين بنوا وحافظوا على الشبكة خلال الثلاثة عقودٍ المنصرمة.

وضح الانقلاب الذي قام به بوستل الدور الحاسم لقضايا الحكم حتى بالنسبة لفضاء تقني. أصبح السؤال مهما أكثر فأكثر عمن يدير الإنترنت، الذي كبر من كونه شبكة للبحوث إلى أن صار دعامة لمجتمعنا الرقمي. أو كما قال إريك اسشمدت (والذي صار فيما بعد مديراً تنفيذياً لشركة صغيرة تسمى قوقل) في مؤتمر للمبرمجين عام 1997 في سان فرانسسكو "إن الإنترنت هو أول شيء من صنع البشرية ولم تفهمه البشرية، وأكبر تجربة فوضوية قد قمنا بها قط".

طالما أن الموارد الرقمية ليست نادرة كما هي الموارد التقليدية؛ فمسألة حكمها قد تختلف قليلاً. لذا فالمسائل الأساسية لحكم الإنترنت تكمن في قابلية التشغيل المشترك والاتصالات، وليست هي قضية التقسيم التقليدية، والتي شغلت كثير من المفكرين السياسيين بداية بـ سقراط إلى ماركس. على كل حال، حتى في عالم رقمي تبدو موارده بلا نهاية، فإن القضايا التقليدية للحكم تظهر في الفضاء الإلكتروني، والتي تتضمن التمثيل والقوة والشرعية.

إن نقاط الاختناق للقرارات الرئيسة تتمحور حول المعايير التقنية للتشغيل المشترك والتوزيع لأرقام أي بي التي تعطي الحاسوب عنوانا وتمكنه من إرسال واستقبال الحزم وإدارة نظام التسمية للإنترنت. ومن المثير

للاهتمام، أن التداخل ما بين التقنين وغير التقنين في هذه الفئة الأخيرة من جانب التسمية قد أنتج الجدال الأكبر.

تتطلب عمليات تشغيل الإنترنت جهات فاعلة مستقلة تتبع قواعد أساسية لتضمن التشغيل المشترك، تسمى بالمعايير. هذا النهج المستند على المعايير يرجع إلى بدايات الإنترنت، عندما نشر المهندسون الذين يبنون النظام الأولي طلبات للحصول على تعليقات "ار اف سي" RFCs (Requests For Comments) للحصول على ردود على المعايير المقترحة. مع الوقت، نمت هذه المجموعة من الباحثين والمهندسين إلى منظمة طوعية دولية للمعايير، سميت بـ فريق عمل مهندسي الإنترنت "أي إى تي اف" IETF (Internet Engineering Task Force). يطور فريق عمل مهندسي الإنترنت معايير وبروتكولات جديدة للإنترنت، ويعدلون في الموجودة، وذلك لتحسين الأداء. كل ما يتم تطويره بواسطة فريق عمل مهندسي الإنترنت، يقع تحت مجموعات عمل محددة تركز اهتمامها في مجالات مثل التوجيه والبرامج والبنى التحتية. هذه المجموعات عبارة عن منتديات مفتوحة، غالباً ما تعمل من خلال القوائم البريدية، وإن أي شخص مرحب به للمشاركة. كثير من الأفراد المتواجدون هم من شركات تقنية كبرى، ولكن لا يوجد ممثل واحد أو حزب صغير يمكن أن يغير مسار العملية، والتي تعتمد على الإجماع.

الانفتاح أو حتى شعور بالغرابة يعتبر أمراً بالغ الأهمية لثقافة فريق عمل مهندسي الإنترنت. في بعض اجتماعات مجموعة عاملة يتم أخذ القرار في قضية ما عن طريق الهمهمة لصالح المقترح أو ضده. والمقترح الذي يحصل على أعلى همهمة يؤخذ به. مع أن ذلك يبدو سخيفاً، فهي الطريقة التي رأوا فيها المحافظة على أخلاق الصانعون الاصليون للإنترنت لتعزيز التوافق والوصول إلى قرار بسرعة نسبياً. إن حجم الهمهمة يساعد أيضاً في الحفاظ على مستوى من السرية في عدم الكشف عن صاحبه، ما لم تسئ استخدام النظام: هذا يعني

أنك تستطيع الهمهمة أو لا بدون فتحك فمك، ولكن من الصعب الهمهمة بصوت عالي للهيمنة على تصويت بدون أن تجعل الأمر واضحاً، والذي سيؤدي إلى ردة فعل عنيفة.

وبالرغم من الشعور بالمتعة الذي يمكن أن يدفع أعضاء مجموعات العمل، فإن الأمن يعتبر مبدأ بالغ الأهمية في النظام. بالإضافة إلى تركيز مجموعات العمل على قضايا أمنية محددة، فيجب على كل مقترح أن يكون به قسمٌ واضحٌ جليٌ عن "ما يتعلق بالأمن". أضف على ذلك قيام مديرية للأمن بمراجعة كل المعايير المقترحة التي اجازتها مجموعات العمل إلى مجموعة التوجيه.

بينما لا يملك فريق عمل مهندسين الإنترنت مجلسا رسميا أو حتى قيادة عليا، فإن مجموعة مهندسين الإنترنت للتوجيه "أي إى اس جي" IESG (Internet Engineering Steering Group) تقدم مراقبةً وارشاداً لعمليات اختيار المعايير والمعايير نفسها وبالمقابل، فإن مجلس هيكلة الإنترنت "أي اى بي" IAB (Internet Architecture Board) والذي تتطور من المجلس الاستشاري التقني للإدارة الأولى لـ "اربانت" في أوائل السبعينيات، يقدم مزيدا من المراقبة على مجموعة مهندسين الإنترنت للتوجيه.

كل من هذه المنظمات تقع تحت رعاية مجتمع الإنترنت "أي اس أو سي" ISOC (Internet Society) وهي مجموعة دولية تم إنشاءها عام 1992 والتي تشرف على اغلب عملية المعايير التقنية. تكونت "أي اس أو سي" عندما انتقلت إدارة الإنترنت إلى ما بعد أمور التنسيق التقني. عندما أصبح الإنترنت عالميا، وبدأت الشركات في الاعتماد على الأعمال التجارية عبر الإنترنت، أصبح مزيداً من المشاركين لديهم حصة إما سياسية أو نقدية في تطور النظام بطريقة أو بأخرى. بدأت المنظمات بالاعتراض على العمليات، والتدخل المركزي لحكومة الولايات المتحدة اقلق الكثيرين. تم إنشاء "أي اس أو سي" كمنظمة عالمية مستقلة، لتقديم وسائل رسمية وقانونية لحماية العمليات المستقلة والمفتوحة للمعايير. تستمد "أي اس أو سي" ISOC قوتها من

أعضاءها، فهي مفتوحة لأي فرد، وبرسوم لكل المنظمات. ومن ثم ينتخب هؤلاء الأعضاء من هم اهل للثقة، والذين يتم تعينهم في قيادة مجلس هيكلة الإنترنت "أي اى بي" IAB، والتي تشرف على إدارة عمليات مجموعة مهندسي الإنترنت للتوجيه وعملية المجموعات العاملة التي ترشدها.

تخيل كل هذا المزيج المختلط من المجموعات الرسمية وشبه الرسمية وغير الرسمية، يتداخل كله معاً. يعزز هذا الهيكل درجة عالية من الاستقلالية في حين لا يزال يترك مجال المسؤولية لمجتمع الإنترنت. عندما يتعلق الامر بوضع المعايير فإن هناك اعتراضات ذات دوافع سياسية ومالية، إن هذه العملية قد عززت المصلحة العالمية المشتركة للحفاظ على عمل الإنترنت.

برغم من ذلك، أصبحت اخلاقيات هذا الاهتمام المشترك، أمراً صعبا في التعامل فيما يتعلق بحقوق الملكية وموارد نادرة على الإنترنت. قد يبدو أن جحم الإنترنت لا حصر له على ما يبدو في الحجم، لكن لا تزال له مباريات محصلتها صفر.

إن المعرفات مثل عناوين أي بي وأسماء النطاقات يجب أن تكون فريدة وغير متشابهة –فالإنترنت لن يعمل إذا حاولت عدة أطراف استخدام نفس عنوان أي بي، أو انهم حاولوا حل اسم نطاق منافس. واحدة من الأدوار الأولى للمراقبة كانت في توزيع الأرقام والاسماء. والنتيجة كانت قيام سلطة الإنترنت لتعيين الأسماء والأرقام، والتي هي جهود مشتركة بين حكومة الولايات المتحدة والباحثين الأوائل الذين طوروا التكنولوجيا الأولى. ومع ذلك ومع تقدم الإنترنت، فإن التحكم في هذه العملية بدا أمراً بالغ الأهمية. فتعين الأسماء والأرقام يعني التحكم فيمن يمكنه وكيف له الدخول إلى الإنترنت. إن "الاستيلاء" الذي قام به جون بوستل، قد أوضح الحاجة إلى هيكل إداري يمكن الوصول إليه وذا شفافية.

إن الضغط المتزايد لشبكة إنترنت تجارية والشعور بحقيقة أن الأمريكيين لن تدوم سيطرتهم على الشبكة للأبد، كان ذلك يعني أن هذا الهيكل الجديد لن يدار بواسطة حكومة الولايات المتحدة. في عام 1998، وبعد فترة دراسة سعت إلى جمع مشاركات من قيادين رئيسين للإنترنت وعامليين ومن المنظمات، تحولت المسؤولية إلى شركة مستقلة مع هيكل للحكم "يعكس التنوع الوظيفي والجغرافي للإنترنت". فقد ولدت مؤسسة الإنترنت لتعين الأسماء والأرقام أو ما تختصر بـ"أي سي اى ان ان".

كانت منظمة غير ربحية، مستأجرة مكان في كاليفورنيا، بدأت "أي سي ان ان" تحرك طريقة ذات هيكلة هي الأنسب في لتوزيع عناوين أي بي لتعكس الطابع العالمي للإنترنت. تبعتها سلطات الأقاليم في أمريكا الشمالية ثم اروبا ثم اسيا وتبعتها أمريكا اللاتينية وأخيراً افريقيا في عام 2004، التي تولت هذه المهمة واستمرت في أدائها إلى اليوم.

لم يكن الأمر سهلاً بالنسبة إلى "أي سي اى ان ان"، فأسماء النطاقات تعرف هويتك على الإنترنت، والتي تجلب الصراع بين المصالح التجارية والسياسية. إن القرارات بشأن من يحصل على هوية على الإنترنت، تخلق في ذاتها رابحين وخاسرين؛ بإضافة نطاقات من الدرجة الأولي مثل tech. يُمكّن نماذج أعمال جديدة ولكن يطلب مزيداً من المصروفات لحماية العلامة التجارية وصد المحتلين. يمكن للعلامات التجارية نفسها أن تشكل مخاطراً. على سبيل المثال، كانت هناك حاجة لعملية لتقرير أي من الاعمال التجارية الكثيرة والتي تحوي كلمة "أبل" Apple هي جديرة باسم النطاق Apple.com. في نفس الوقت، ما كان لتلك العملية أن تُشوه لتُنكر فرص حرية التعبير، مثل sucks.com < سمى ما لا تحب من العلامات التجارية> . هذه العملية كانت أيضاً قد مست قضايا حرجة للهوية القومية. متى ما تحقق استقلال بلاد أو نشبت فيها حرب أهلية، فمن

يتحكم في نطاق الدرجة الأولى لتلك الدولة؟ ففي الصحراء الغربية، كِلاَ الطريفين لصراع عمره أربعون عاماً، طالب بأحقيته باسم نطاق الدرجة الأولى. eh.

جلت العملية وإدارة "أي سي اى ان ان" ICANN الكثير من الجدل. يستخدم علماء السياسة مصطلح "عملية أصحاب المصلحة المتعددين" ليصف نهجها الاساسي المفتوح غير التمثيلي. يفترض بالقرارات أن تكون بالإجماع، بينما هناك حشد من اللجان الاستشارية التي تساعد في تمثيل الدوائر الرئيسة التي تساهم في انسياب عمليات الإنترنت، مثل مزودي خدمات خدمة الإنترنت ومجتمع الملكية الفكرية. يتم تمثيل المصالح الوطنية حول العالم من خلال اللجنة الاستشارية الحكومية. ولكن هذا النموذج للمساهمين الكثر يتخلص من البعض لصالح الأقوياء. تستطيع الحكومات والمستثمرين الكبار دفع رواتب لطاقم للمساهمة في تلك المنتديات، بينما هناك مجموعات مجتمع مدني غير ربحية قد تفتقر الموارد للجلوس في تلك الطاولة على الاطلاق. هناك نقاش يدور حول أن هناك عدد كبيرا من ممثلي القطاع الخاص بين صناع القرار. وإن هناك من يُردها أن تكون مثل المنظمات العالمية التقليدية والتي تتبع نموذج الأمم المتحدة "وطن واحد، صوت واحد".

بغض النظر عن الجهود المبذولة لجعل حكم الإنترنت عالمياً، فإن كثيرون ما زالوا يرون أن "أي سي اى ان ان" ICANN أسيرة لمصالح الولايات المتحدة. إن التحكم في تعيين الأسماء والأرقام لا يزال ظاهريا يتبع لوزارة التجارة الأمريكية انضمت لها "أي سي اى ان ان" ICANN بعقد قابل للتجديد. وبذلك تكون الولايات المتحدة قد احتفظت بالتحكم الكلى، بينما مهمة الإدارة تقوم بها منظمة تقودها الصناعة، واللذان لهما مصلحة معينة بالحفاظ على الوضع الراهن.

إن التحدي يكمن في أنه لا توجد مؤسسة ولا عملية يمكنها أن تحل محل "أي سي اى ان ان" بسهولة، بينما نجد أنه من السهل نقدها، إلا أنه لا يوجد نموذج عملي لمنظمة بديلة يتوجب عليها التمثيل والمساواة بين مجموعة واسعة من المصالح حول العالم وكل الجوانب المعقدة للقضية السياسية.

إن النقطة الأساسية لقضية الحكم المتعلقة بالأمن الإلكتروني هذه، ليست هي الدور المهم الذي لعبته الثقة والعقول المنفتحة في نمو الإنترنت (جوانب واجهة تحديات مع زيادة المخاوف الأمنية) ولكن طالما عُرِّف الإنترنت بأنه فضاء يتحدى نماذج الحكم التقليدية. ففي عام 1992 صرح ديفت كلارك الذي هو أحد الرائدين في مجال الإنترنت في شركة "ام أي تي" MIT، بقول فصل للمجتمع:

نحن نرفض: الملوك والرؤساء والتصويت.

نحن نؤمن بـ: الإجماع العام وكود برمجي يعمل.

انتشرت تلك المقولة انتشاراً واسعاً. على عكس ما قاله كلارك في الرسالة التي تلت "ما الذي لا نجيده؟ زيادة أنظمة عملياتنا لتناسب حجمنا"

في الإنترنت، كيف لهم أن يعرفوا إذا ما كنت كلباً ام لا؟

الهوية والتفويض

لدى البروفيسور إلساندرا كويستي من جامعة كريج ميلون خدعة في الحفلات، مسلية ولكن مخيفة: أرِه صورة لوجهك من الإنترنت وسيقوم بتخمين رقم حمايتك الاجتماعية.

إن فهم كيفية قيام كويستي بتلك الخدعة مهم حتى لغير الأمريكيين (الذين يفتقرون لتلك الأرقام الضرورية للحماية الاجتماعية)، لأنها توضح قصة الهوية والتفويض وكيف لها أن تنحرف. يقوم كويستي أولا باستخدام تقنية لتشابه الصور لإيجاد صورتك على موقع شبكة للتوصل الاجتماعي. إذا كان تاريخ ميلادك والمدينة التي ولدت مذكورة على الإنترنت، كما هو حال معظم الناس، يستطيع بعدها استخدام الأنماط التي تربط الزمان والمكان بأول خمسة أرقام من أصل تسعة أرقام والتي تُكوّن رقم حمايتك الاجتماعية، ومن ثم يصبح الأمر لعبة تخمين لبقية الأرقام. إذا كنت من ولاية صغيرة مثل ديلويد، فإن رقم حمايتك الاجتماعية يمكن تحديده في أقل من عشرة محاولات.

نظريا، لا يجب أن يولى أحد اهتماماً، طالما أن أرقام الحماية الاجتماعية ما كانت تعتبر سراً فيما مضى. قبل عام 1972، كان مطبوع على بطاقات الأمن الاجتماعي "ليست للهوية" ولكن مع بداية استخدامنا للحواسيب لتعقب الناس، أصبح من الضروري للحواسيب التفريق بين الأفراد. استخدام الاسم وحده ما كان يكفي: فهناك كثير من الأشخاص حول العالم يسمون بجون اسميث. على مدى كل قواعد البيانات، فكل سجل كان يحتاج إلى مُعرِفٍ فريد لذاك الشخص للوصل إليه. وبما أن لكل أمريكي رقم حماية اجتماعي فريد، كان من المناسب استخدامه لذاك الغرض.

إلى حد ما كان ذلك جيداً، كان الرقم وسيلة للبحث عن شخص ما عن طريق حاسوب. ولكن أصبح هذا الرقم الوسيلة التي يعرف بها نظامان أنهما يتحدثان عن نفس الشخص. وسرعان ما استخدام رقم الحماية الاجتماعية لتعقب حسابات البنوك وتفاصيل الضرائب وكل الجوانب المتعلقة بالمعلومات الشخصية. أثناء حدوث ذلك، افترضت المنظمات طالما أن أرقام الحماية الاجتماعية لم تنشر فهي ليست عامة، وإذا لم تكن عامة فيجب أن تحفظ سراً. وذلك خطأ.

في عالم الحاسوب، تعتبر الهوية فعلاً يتم فيه رسم كيان من بعض المعلومات عن ذاك الكيان. يمكن أن يكون أمراً عاديا كموقع كرة قدم للمعجبين يقبل الجمع بين الشخص والاسم الذي يدعيه ذاك الشخص، أو أمراً حاسماً كمطابقة سجل طبي لمريض فاقدٍ الوعي.

ومن المهم التفريق بين الهوية و "المصداقية" والتي هي دليل على الهوية. تم تعريف هذا الدليل قديما بـ "شيء أنت تعرفه أو شيء تمتلكه أو شيء أنت هو". إن الذي تعرفه هو النموذج الأساسي لكلمة السر. إنه سرٌ غالباً معرفته مقصورة على الشخص الصحيح. الشيء الذي تملكه يرجع لمكون مادي ذا وصول محدود، يقتضي على الشخص الصحيح ملكه. في حالة مكينة الصراف الآلي؛ هي البطاقة. بينما حاليا وبكثرة أصبح الهاتف الجوال في الواقع معرفا للهوية، وذلك باستقبال رسالة نصية تحتوي على رمز للاستخدام مرة واحدة. بإدخال ذلك الرقم يتخذ الناس اجراء على الإنترنت يثبت أن لهم التحكم في الهاتف الجوال المُتحققُ منه والذي استقبل الرسائل. في النهاية يمكن أن تثبت من أنت عن طريق شيء يمكن تميزه. وبما أن هذا غالبا يدل على شخص واحد، يسمي بـ "القياس الحيوي". يمكن للقياسات الحيوية أن تكون بسيطة مثل شخص أخر يتعرف على وجهك، أو معقدة كحساسات تتعرف على شبكية عينك.

تلك البراهين بها نقاط ضعف، يمكن لكلمات السر أن تُخَمّن أو تُكسَر وتتطلب جهداً ادراكياً (عليك حفظهم كلهم). إذا ما استخدمت كلمة السر في عدة مواضع، فاختراق نظام واحد يتيح للمخترق الوصول للنظام التالي. الأشياء التي تملكها يمكن أن تُسرق أو تزيف، وحتى القياسات الحيوية يمكن أن تُخترق. فمثلاً، الدخول عبر قارئ بصمات يتطلب بصمة مميزة، تم تضليله بواسطة بصمة إصبع مزيفة تمت طباعتها على حلويات على شكل دب صغير، أو بشكل أبشع، بوضع إصبع مبتور على القارئ (يبدو أن رجال العصابات الروسية وبشكل ساخر، لا يحبون الحلوى على شكل دببة لطيفة).

هناك عدة آليات لدعم تلك القياسات، واحدة منها أن تتصل بصديق موثوق، للتأكد من أولئك الأفراد وما ادعوه. تلك الفكرة جاءت من المقولة القديمة "إن الأمر متعلقٌ بمن تعرف". بما أن الصديق الموثوق المشترك المُتحقِقُ من ذاك الشخص بأنه هو نفسه صاحب الهوية المدعاة. هناك أنظمة تكون هي العامل لتضليل التحكم. أي شخص يمكنه صنع صفحة على الإنترنت يدعي فيها أيً كان، ولكنها تحتاج إلى مجهود ووقت للحفاظ على وجود تلك الصفحة وابقائها نشطة لأطول فترة ممكنة على منصة موقع تواصل اجتماعي مثل فيس بوك وتوتير. ونأتي مرة اخري لنقول إنه يمكن اختراق تلك أيضاً، أو تزويرها. ولكنها قد تكلف المعتدي كثيراً إذا ما استمر فيها.

بعد ما تمت إجازة الهوية، فإن النظام بات يعرف من أنت وما الذي يمكنك فعله؟ في تأمين الحواسيب التقليدي كان التفويض يمنح الدخول إلى ملفات الشبكة. ولكن في عالمنا الذي زاد فيه الترابط، فإن الحصول على تفويض قد يفتح لك الأبواب عمليا لكل شيء. إن التفويض هو الجزء الذي يربط هذه القضايا التقنية بالسياسة والأعمال والمسائل السياسية والأخلاقية. هل للفرد الحق في شراء شيء ما، مثل حساب على موقع لعب قمار على الإنترنت؟ وإن كان كذلك، فهل الشخص كبير بما فيه الكفاية للمشاركة؟ أو على مدى عالمي

أكبر بقليل، فقط لأن الشخص يستطيع الدخول لشبكات عسكرية سرية، هل لذاك الشخص التفويض بقراءة ونقل كل الملفات على الشبكة (ممارسة ستطارد الجيش الأمريكي في تسريبات برادلي مانق وإدورد سنودن)؟

ربما أفضل توضيح للمشكلة كان في أكثر رسم كرتوني اُستُشهِد به في على مر الزمن. ففي عام 1993 نشرت مجلة نيويورك رسم لبيتر ستنر لكلبين جالسين بالقرب من جهاز حاسوب، قال أحدهما للأخر: "في الإنترنت، لن يعرف أحد أنك كلب".

وهذا لا يعني القول بأن الناس لن يعرفوا عنك تفاصيل خاصة إذا ما أرادوا ذلك. فكل نشاط على الإنترنت يعتبر بيانات يتم توجيهها من بروتكول عنوان الإنترنت (أي بي IP) وكما رأينا في الجزء السابق، فإن عنوان أي بي هو بطاقة رقمية تم تعينها لاتصال معنون على الإنترنت. بالنسبة لأغلب المستهلكين فإن عنوان أي بي لا يتم تعينه لجهازهم للأبد، ولكن بالمقابل فعنوان أي بي يكون ديناميكياً. إن مقدم خدمة الإنترنت للمستهلك يقوم بتعيين عنوان أي بي لفترة من الزمن، ولكن قد يعاد تعيينه لشخص أخر حالما يقطع المستخدم الاتصال. ولكن على كل حال، إذا احتفظت الجهة المقدمة للإنترنت بالبيانات ذات الصلة، فعندها يمكن ربط استخدام عنوان أي بي في تاريخ وزمن محددين بمشترك معيين.

إن عنوان أي بي ليس هو في ذاته معلومات، ولا يتضمن هوية شخص ما، ولكنه قد يقدم بعض المعلومات عن الموقع الجغرافي والوسائل التي اُستُخدِمت بواسطة ذاك الشخص للوصل للإنترنت. إن الاحتمال في كيف لعنوان أي بي أن يُجمَع مع معلومات أخرى (أو لسبب ما تم جمعه مع معلومات اخرى) يمكن أن تكشِف الهوية المعنية. إذا استَطعت جمع ما يكفي من المعلومات من داخل شبكة الإنترنت وخارجها، فإنك تملك بيانات تكفيك لتخمين من، وما الذي كان يفعله وأين. فمثلاً، في فضيحة المدير العام لوكالة الاستخبارات المركزية ديفت بتروس عام 2012، تمكنت "اف بي اي" FBI (Federal bureau of Investigations)

من تعقب المُرسِل المجهول لعدد من التهديدات عبر البريد الإلكتروني إلى مركز تجاري تابع لفندق، والذي أُكتُشِف لاحقا أن عشيقته كانت متواجدة فيه.

إن المعلومات التي يتم جمعها عن الهوية ليست هي الدليل على الهوية. إن الاعتماد على عنوان أي بي سيكون كاعتمادك على ارقام لوحات سيارات لتتعرف على السائقين. إذا كانت مستخدمة متمرسة يمكنها بسهولة إخفاء أو تمويه عنوان أي بي الخاص بها، عن طريق توجيه نشاطها عبر نقطة أخرى على الإنترنت. والتي ستجعل من تلك النقطة هي المسؤولة عن حركة البيانات الاصلية. على كل حال، توجد اشكال أخرى من البيانات يمكن جمعها والتي من الصعب إخفائها. حتى نمط المستخدمين الافراد في التصفح والنقر خلال صفحات الإنترنت، يمكن استخدامه للتعرف على هوياتهم.

إن السؤال عن كيف **يمكننا** التبين والتحقق من النشاطات على الإنترنت، هو سؤال يختلف عن كيف يجب أن نفعل ذلك. قد لا تريد الكشف عن رقم حمايتك الاجتماعية في حفله، أو أن ذاك الكلب يفضل أن تظل هويته سراً، على الأقل حتى يخرج كليكما في أكثر من موعد على الإنترنت.

ولأغراض الأمن الإلكتروني، فالخلاصة هي أن الهوية الرقمية هي توازن ما بين حماية ومشاركة البيانات. إن الحد من المعلومات المكتسبة أمر جيد، ليس فقط للخصوصية، بل يمكن أن يمنع الأخرين من الحصول على معلومات للقيام باحتيال خطير للمصداقية. في نفس الوقت فكل نظام له محفزات لزيادة كمية البيانات التي يجمعها. إضافة إلى استخدام تلك البيانات لخدمة أهدافه الخاصة.

ما الذي نعنيه بـ "الأمن" على أي حال؟

هناك طرفة قديمة في قطاع الأمن، عن كيف لك ان تؤمن أي حاسوب: افصله فقط! ليست المشكلة أن الطرفة أصبحت قديمة في عصر اللاسلكي والأجهزة القابلة للشحن. إن أول ما يتم إيصال الالة، فهناك عدد لا حصر له من الطرق التي تمكن عمليا من تحريف استخدامها إلى غرض غير الذي صممت من أجله. هذا الانحراف يعتبر عطلاً. إذا ما اختلف أداء الاله عما هو متوقع منها، بسبب عدو ما (عكس الخطاء البسيط أو الحادث) فإن العطل يصبح مشكلة أمنية.

إن مفهوم الأمن ليس فقط السلامة من الخطر، كما هو الفهم العام. لكنه مرتبط مع وجود مُعتّدى. في تلك الحالة فهو مثل الحرب؛ تحتاج إلى طرفين على الأقل لجعلها حقيقية. الأشياء قد تتحطم والاخطاء قد تقع، ولكن مشكلة إلكترونية تصبح قضية أمن الإلكتروني فقط إذا ما سعى مُعتدٍ للحصول على شيء من فعلته، سواء اكانت معلومات خاصة أو تعطيل النظام أو منع استخدامه المشروع.

للتوضيح، ففي عام 2011، أمرت إدارة الطيران الفدرالية بإغلاق أكثر من نصف الأجواء الملاحية للطيران في الولايات المتحدة، واجبار أكثر من ستمائة طائرة على الهبوط. بدا ذلك إعادة لما حصل عقب هجمات الحادي عشر من سبتمبر من إغلاقٍ لأجواء الطيران. ولكن هذه الحادثة لم تكن قضية أمنية، فلم يكن خلفها أحد. لقد كان السبب خلل برمجي في حاسوب واحد في مبني الإدارة العليا بأطلتنا. خُذ نفس الموقف وغيّره من خلل إلى اختراق، عندها ستكون تلك قضية أمنية.

إن الأهداف المشروعة للأمن في بيئة المعلومات تأتي نتيجة مفهوم تهديد ما، على نحو تقليدي فإن هناك ثلاثة اهداف: الخصوصية والنزاهة والتوفر، يُدعون في بعض الأحيان بـ "مثلث سي أي اى" CIA (Confidentiality, Integrity and Availability).

إن الخصوصية تشير إلى حفظ البيانات بشكل سري. ليست الخصوصية هدفا سياسيا أو اجتماعي. ففي عالم رقمي، إن للمعلومات قيمة. وحمايتك لتلك المعلومات هو من الاهميات الأساسية. لا يجب حفظ الأسرار الداخلية والبيانات الشخصية فقط، فقد تكشف البيانات المتداولة تفاصيل هامة عن العلاقات بين الشركات والأفراد. إن الخصوصية محمية بأدوات تقنية مثل التشفير والتحكم في الدخول، وأيضاً الحمايات القانونية.

تعتبر النزاهة هي الجزء الرقيق وربما الأكثر أهمية لأمن المعلومات التقليدي في تلك المنظومة الثلاثية. إن النزاهة تعني أن النظام والبيانات التي فيه لم تُغيّر أو تُبدّل بطريقة خاطئة وبدون تفويض. فهي ليست مسالة ثقة فقط. يجب أن تكون هناك ثقة بان النظام سيكون متوفرا ويعمل بكفاءة كما هو متوقع.

إن رقة النزاهة هي التي تجعل منها هدفا متكررا لأغلب المُعتدين المتمرسين. فغالبا ما يقومون أولاً بإبطال الآلة التي تحاول تحديد الهجمات. بنفس الطريقة التي تسعي بها الأمراض المستعصية، مثل الإيدز، خلف الدفاعات الطبيعية في جسم الإنسان. فمثلاً في هجوم ستكسنت (سنستعرضه لاحقاً في القسم الثاني) كان الوضع متعارضاً، فالحواسيب المصابة كانت تظهر لمشغليها الإيرانيين أنها تعمل بشكل طبيعي، حتى بوجود فيروس ستكسنت الذي كان يعمل على تخريبها. كيف لنا أن نعرف ما إذا كان النظام يعمل بشكل طبيعي، إذا ما اعتمدنا على ذلك النظام ليطلعنا على وضعه الحالي.

التوفر يعني القدرة على استخدام النظام كما هو متوقع. وهنا أيضاً، ليس بالضرورة أن يكون تعطل النظام ما يجعل من التوفر قلقاً أمنياً، فأخطاء البرامج و"شاشات الموت الزرقاء" تحصل لحواسيبنا كل الوقت. ولكنها تصبح قضية أمنية إذا ما حاول أحدهم استغلال عدم التوفر بطريقة ما. قد يفعل مُعتدٍ ذلك، إما بحرمان المستخدمين من نظام يعتمدون عليه (وذلك ككيفية خسارة نظام تحديد المواقع الجغرافي إعاقة الوحدات العسكرية أثناء صراع ما) أو بمجرد التهديد بخسارة النظام، والذي يُعرف بهجوم "فيروس الفدية". أمثلة لتلك الفديات قد تتراوح من اختراقات ذات مدى قصير على الحسابات البنكية للأفراد، وإلى محاولات الابتزاز العالمية ضد مواقع الرهانات والقمار قبل أحداث رياضية كبيرة مثل كاس العالم ونهائي الدوري الوطني الأمريكي.

نعتقد أنه من المهم إضافة المرونة كطرف أخر لمثلث الأمن التقليدي. إن المرونة هي التي تسمح للنظام بتحمل التهديدات الأمنية بدلا من التعطل بشكل خطير، إن مفتاح المرونة هو تقبل حتمية وقوع التهديدات وحصر القصور في دفاعاتك. كما تمثل الاستمرار في التشغيل مع تفهم أن الحوادث تحصل بوتيرة مستمرة. هنا أيضاً، هناك شبه بجسم الإنسان. فجسمك يجد طريقة للاستمرار في العمل مع أن طبقة دفاعك الخارجية –بشرتك–تم اختراقها بواسطة جُرحٍ أو حتى تخطيها بواسطة عدوى فيروسية. وكما في جسم الإنسان، ففي حال حدوث أمر في الحاسوب، يجب ان يكون الهدف هو اعطاءُ الأولية للموارد والعمليات وحماية الأصول الرئيسية والنظام من الهجمات، وفي النهاية إعادة التشغيل بطريقة طبيعية.

ليست كل هذه الجوانب الأمنية قضايا تقنية فقط: بل هي تنظيمية وقانونية واقتصادية وأيضاً اجتماعية. ولكن الأكثر أهمية، أنه عندما نفكر في الأمن فيجب تميز حدوده. أيُ مكسب امنيٌ دائما ما يتضمن نوعا من المقايضة. يكلف الأمن مالا ويكلف الوقت والقدرات أيضاً، ويسلب الراحة والحريات وهلم جرا. وفيما نستعرضه

لاحقا، فالتهديدات المختلفة للخصوصية والتوفر والنزاهة والمرونة، كل واحدة تحتاج استجابة مختلفة عن الأخرى. بغض النظر عن فصل الحاسوب، فليس هناك ما يسمى بالأمن المطلق.

ماهي التهديدات؟

قد يبدو من الغريب لصحفيين أخذ طائرة ركاب إلى أيداهو، فقط لمشاهدة هجوم حاسوبي. لكنه ما حصل بالضبط عام 2011.

قامت وزارة الأمن الداخلي باصطحاب صحفيين من ارجاء البلاد جواً إلى مختبر أيداهو القومي قبل أربع سنوات، وذلك لقلقها حيال عدم تفهم الجمهور حجم تضخم التهديدات الإلكترونية. أجري مختبر أيداهو القومي الذي هو مؤسسة ذات سرية وأمن عالي جداً والتي حوت مؤسسة البحوث النووية لوزارة الطاقة، اختباراً سريٌ للغاية، لتدمير مولد كهربائي ضخم بواسطة هجوم حاسوبي. وفي عام 2011 اتخذت جهوداً لرفع مستوى الوعي للتهديدات الإلكترونية، فقام خبراء من الحكومة برفع السرية، ليس فقط عن فيديو الاختبار الذي أُقيم عام 2007، ولكنهم أيضاً قاموا بإجراء تدريبات عامة بحضور الصحفيين لمشاهدة هجوم حاسوبي مزيف، هجوم على مصنع وهمي للمواد الكيميائية. ارادت الحكومة اظهار عدم القدرة حتى لمختصيها من منع فريق مأجور من المخترقين (معرفون بالفريق الاحمر) من اجتياح دفاعات منشئة حساسة.

تعتبر هذه الحادثة عرضا جيداً لقلق من يفكرون ويتحدثون بطريقة احترافية عن الأمن الإلكتروني، من أن نقاشهم للمهددات يتم تجاهلها أو التقليل من شانها. ونتج عن احباطهم أنهم عادوا لرفع درجة الصوت لأقصي حدودها، بإجراء تجربة غريبة والتحدث عن الأمر بأكثر الطرق حدة، والتي رجعت بصداها نحو الإعلام والجمهور. بالتأكيد تبع ذلك عدد من التحذيرات من قيادين في حكومة الولايات المتحدة وبحلول عام 2013

كان هناك ما يزيد عن نصف مليون مرجع في الإنترنت في الإعلام عن هجوم "بيرل هاربر الإلكتروني" وربع مليون أخر عن مخاوف "هجوم حاسوبي شبيه بهجوم الحادي عشر من سبتمبر".

إن الرضي الذي قلق بشأنه هؤلاء الخبراء، ينبع من جزء في ممانعة نظامنا السياسي لمعالجة المشاكل الصعبة والمعقدة بشكل عام والأمن الإلكتروني بشكل خاص. ولكن هذا النوع من المضمون يتغذى على سوء فهم التهديدات. فمثلاً، في صيف عام 2011، قام ثلاثة من أعضاء مجلس الشيوخ بالولايات المتحدة بالإشراف على مشروع قانون كبير للأمن الإلكتروني. وثم كتبوا افتتاحية في صحيفة واشنطن بوست، تلح بدعم تشريعهم. أشاروا فيه إلى سلسلة من الهجمات الأخيرة، تضمنت تلك التي كانت ضد شركات سيتي قروب City Group وشركات أمن المعلومات التجارية وهجوم فيروس ستكسنت على الأبحاث النووية الإيرانية. المشكلة هي أن هذه الحالات الثلاثة تعكس أنواع مختلفة من التهديدات بشكل كبير. كان الهجوم على شركات سيتي قروب City Group احتيالاً مالياً، وكان الهجوم على شركات أمن المعلومات سرقة صناعية، أما ستكسنت فكان شكلاً جديداً من أشكال الحرب. فيما بينهم بعض القواسم المشتركة ولكن الحواسيب تورطت فيها كلها.

عند مناقشة الحوادث الإلكترونية أو الخوف من حوادث محتملة، فمن المهم التفريق بين الضعف والتهديد. إن الباب غير الموصد يعتبر نقطة ضعف وليس تهديدا مالم يدخل منه أحد. وعلى عكس ذلك، فنقطة ضعف واحدة قد تقود إلى العديد من التهديدات: فذاك الباب غير الموصد قد يقود ارهابين لتهريب قنبلة، أو منافسين يحصلون على أسرارٍ تجارية، أو لصوص يختلسون سلع ثمينة أو مثيري شغب محليين يخربون الممتلكات أو حتى قطط تتجول وتشتت انتباه موظفيك اثناء لعبها على لوحات المفاتيح. ان الجوانب التي تُعرِّفُ التهديدات هي الفاعل والنتيجة.

أن الاعتراف بالفاعل يدفعنا إلى التفكير في التهديدات بطريقة استراتيجية. يمكن للمعتدي أن ينقى ويختار أي من نقاط الضعف شاء، ليستغلها في خدمة أي هدف كان. هذا يعني أنه لا يجب علينا معالجة مجموعة من نقاط الضعف فقط فيما تتعلق باي تهديد معين، ولكن تفهم أن التهديد قد يتطور نتيجة لإجراءاتنا الدفاعية.

هناك العديد من انواع الجهات الفاعلة السيئة، ولكن من السهل إيجاد الراحة في استخدام العبارة الإعلامية "مخترقون" لجمعهم كلهم. تُعتبر معرفة هدف الفاعل نقطة بداية جيدة إذا ما أردنا تقسيمهم. في تنوع الهجمات التي ذكرها أعضاء المجلس أعلاه. فإن الذين نفذوا الهجوم على سيتي قروب City Group أرادوا تفاصيل الحسابات البنكية للزبائن، لهدف أساسي وهو السرقة المالية. أما الهجوم على شركات أمن المعلومات التجارية، أراد المعتدون الحصول على الأسرار التجارية الرئيسية لغرض التجسس على الشركات الأخرى. أما بالنسبة لفيروس ستكسنت (حالة سنعرضها لاحقاً في القسم الثاني) كان هدف المعتدين إعاقة التحكم في العمليات الصناعية التي تدخل في تخصيب اليورانيوم ولذلك لتخريب البرنامج النووي الإيراني.

في النهاية، من المفيد الاعتراف عندما يأتي الخطر من الداخل، حالات مثل برادلي مانينج ووكيليكس WikiLeaks أو ايدورد استورت وفضيحة "إن اس اى" NSA (National Security Agency) التي توضح أن التهديد الداخلي هو صعب بالتحديد؛ لأن الفاعل يستطيع البحث عن نقاط الضعف داخل النظم، التي صممت لتستخدم فقط من قبل من هم أهل بالثقة. إن المطلعين ببواطن الأمور قد تكون لهم منظورات أفضل عما هو قيم، وكيف لهم السيطرة عليه. إذا ما كانوا يحاولون سرقة أسرار أو تخريب عملية.

من المهم أيضاً الاخذ في الاعتبار ما إذا كان الفاعل المهدد يريد الهجوم عليك أو أنه يريد الهجوم فقط. بعض الهجمات تستهدف جهات معينة لأسباب محددة، بينما يسعى معتدون أخرون خلف اهداف معينة،

بغض النظر عمن يتحكم فيها. بعض الكود البرمجي الضار غير المُستهدِف قد يصيب الآلة عن طريق البريد الإلكتروني مثلاً، ثم يبحث عن تفاصيل بطاقة الائتمان المخزنة على الآلة لأي شخص كان، ثم يرجع بها إلى الشخص الذي أنشأ ذاك الكود الضار بدون أي تدخل بشري. الفرق الأساسي في هذه الهجمات الآلية هو واحد من حيث التكلفة، من منظور المعتدي والمدافع معا. بالنسبة للمعتدي، فالتشغيل الآلي يُخفضُ التكلفة بشكل كبير، حيث لن يحتاج لصرف ماله في كل مهمة احتاج اداءها، من اختيار للضحية إلى تعريف الأصول إلى إعداد الهجوم. فالهجوم غالباً له نفس التكلفة، بغض النظر عن عدد الضحايا المُتحصلِ عليها. من ناحية أخري فالهجوم المُستَهدِف قد يزيد التكلفة بارتفاع عدد الضحايا. هذه الديناميكيات نفسها التي تشكل الفوائد المتوقعة. إذا أراد المُعتَدى ان يصرف ماله في هجمات مُستَهدِفَةٍ، فعلى المعتدى أن تكون له توقعات بفوائد ذات قيمة أعلى مع كل ضحية بالمقارنة، فالهجمات الآلية قد تعود بهامش ربح قليل.

إن الأخبار السارة هي أنه يوجد فقط ثلاثة أشياء يمكنك فعلها للحاسوب: سرقة بياناته أو إساءة استخدام صلاحياته أو اختطاف موارده. للأسف فاعتمادنا على نظم المعلومات يعني أن فاعلاً متمرساً يمكنه الحاق الكثير من الضرر بفعل أي من التي سبق ذكرها. فسرقة البيانات قد تكشف عن الخطط الاستراتيجية لبلد ما، أو إضعاف المنافسة لقطاع كامل. الصلاحيات المسروقة قد تعطي القدرة على تغير أو تدمير البيانات أو كود برمجي، أو تغير قائمة الرواتب أو فتح السدود، وأيضاً القدرة على إخفاء الأثر. اختطاف الموارد قد يمنع شركة من الوصول إلى زبائنها أو سلب جيش القدرة على التواصل.

في النهاية، فهناك الكثير من الأشياء يمكن أن تحدث، ولكن يجب أن يكون خلفها شخص ما. يجب أن يتم تقيم التهديدات بفهم الجهات الفاعلة السيئة المتوقعة. ما الذي يحاولون فعله، ولما؟

وأنت لست بحاجة للطيران كل المسافة إلى أيداهو لمعرفة ذلك.

هجوم مرةً ومرتين وهجوم احمر وهجوم إلكتروني: ماهي نقاط الضعف؟

واجهت الشرطة في لندن عام 2011 ارتفاعاً غامضاً وغير طبيعي في سرقة السيارات. الغريب في الأمر ليس عدد السيارات التي تمت سرقتها والتي كان عددها ما يقارب الثلاثمائة سيارة، ولكن السيارات كانت من سيارات بي ام دبليو BMW الجديدة. وكان اللصوص يسرقون بدون تفعيل الإنذار في مئات من السيارات في التي تم تجهيزها بأفضل أنظمة الأمان تقدماً في العالم.

بعد مشاهدة صور من كاميرات مراقبة مخفية للصوص أثناء السرقة، سرعان ما اكتشفت الشرطة أن اللصوص قد وجدو طريقة لاستخدام التقنية المتقدمة في السيارة ضدها. أولاً، يستخدمون مشوشاً لترددات الراديو لمنع إشارة المفتاح الإلكتروني للسيارة. بدلا من أن تُغلق الأبواب عندما يبتعد عنها صاحبها، فإنها تظل غير مُغلقة. حالما يدخل اللص في السيارة يقوم بالتوصيل في منفذ "أو بي دي 2-" OBD-II (On-Board Diagnostics) (منفذ الإلكتروني تستخدمه الماكينات في تحليل اعطال سيارتك) ثم استخدامه للحصول على الهوية الرقمية الفريدة لمفتاح السيارة. وبعدها يقوم اللص ببرمجة مفتاح الكتروني جديد للاستجابة مع الهوية الرقمية للسيارة. وبعدها يقودها مبتعداً بكل بساطة، تاركين صاحب السيارة الفارهة المتقدمة في حيرة من أمره. فلم يستغرق الأمر برمته سوى دقائق قليلة. نقاط الضعف تلك أدت لكثير من السرقات، مما دفع الشرطة لترك منشورات ورقية على كل سيارة بي ام دبليو BMW واقفة في لندن، تحذرهم فيه من الخطر المُحدِق.

إن قضية السيارات الفارهة التي تمت سرقتها، يوضح بصورة جيدة كيف لنظام تم بناه بتعقيد أن يخلق فرص جديدة ونقاط ضعف مخفية، يمكن استغلالها من قبل أُناس سيئون. اختلاف نقاط الضعف يسمح للمعتدين من تحقيق اهداف مختلفة. في بعض الحالات، قد تكون القدرة على قراءة ملفات سرية، أو قد يكون الهدف الجائزة الكبرى بالاستحواذ على نظام بأكمله. عندما يكون للمعتدي "وصول مطلق" فعندها يمكن تنفيذ أي أمر،

وتصبح الضحية ضعيفة بالكامل، أو ما يسميه المخترقون "تمت السيطرة" "بيوند" (pwned) (في قصة مُختلقةٍ، أراد مخترق طباعة انه قد أمتلك الضحية "أوند" "owned" ولكنه كان يطبع بسرعة، فضغط على مفتاح حرف "بي" P بدلا من مفتاح حرف "أو" O الذي هو بجواره، فتمت ولادة مصطلح جديد).

إن أسهل طريقة في الغالب للحصول على التحكم في نظام، هي ببساطة أن تسأل. تقليد قديم في خرق الأنظمة في الأيام الأولى للاختراق، هو أن تستدعي موظف من درجة صغرى وتجعله يدعى أنه من القسم التقني ويسأل الشخص عن كلمة السر الخاصة به. هذا يقع تحت فئة ما يسمى بـ "الهندسة الاجتماعية"، إنها التلاعب بالناس للكشف عن معلومات سرية لتساعد المعتدي. إن التلاعب قد يأخذ عدة صور، غالباً ما يحاول المعتدي استخدام سيناريو تم تصميمة لتشجيع التعاون من خلال الآليات النفسية. يُعتبر الخوف من الدوافع القوية. عندما يَعرِضُ الحاسوب رسالة بها تهديد بكشف نشاطاتك على موقع في الإنترنت لا يجب أن تكون فيه، عندها خوف الضحية يقودها لدفع المال. مع ذلك وفي أحيانا كثيرة، يتبع المستخدمين فقط الإرشادات الاجتماعية. في حياتنا ليومية دائماً ما نواجه مشاكل تحتاج لحل، مثل برنامج لا يغلق حتى "تضغط هنا" أو أناس يحتاجون مساعدتنا، مثل العمة سوزي التي بطريقة ما تمت سرقتها في أيسلندا، وتحتاج منك مالاً ترسله لها عن طريق بانكوك.

نوع شائع بشكل خاص من الهندسة الاجتماعية هو هجوم "الصيد". قد يشبه البريد الإلكتروني المُتَصَيد البريد الرسمي من بنك الضحية أو من مديره في العمل أو كيان قد يعطيه الثقة. يدعون فيه الضحية للقيام بإجراء معين، قد يكون تصحيح خطاء في بيانات الحساب أو طلب الاطلاع على رسالة في فيسبوك، والتي تُخدع بها الضحية لزيارة صفحة مزيفة على الإنترنت يطلب منهم فيها ادخال بيانتهم السرية. إذا ما أدخلت الضحية بيانات حسابها فإن المعتدي يستطيع الآن فعل أي شيء بتلك المعلومات، من إرسال أموال إلى قراءة

رسائل سرية في البريد الإلكتروني. صفحة الإنترنت المزيفة قد يكون عنوانها قريب من عنوان الصفحة الأصلية. إذا لم تمعن النظر فإن www.paypai.com قد تبدو مثل www.paypal.com . في هجمات الصيد المعقدة، فإن الصفحة المزيفة قد توصلك بالصفحة الاصلية، لتقليل فرصة الكشف.

واحد من أصعب فروع هجوم الصيد، ما يعرف بـ "الصيد بالرمح". لا تستهدف هذه الشبكات فقط بل الأفراد الأساسين داخل هذه الشبكات. إن الفرق بينك جنباً إلى جنب مع العشرات من الناس، تلقي بريد الكتروني من ذاك الأمير النيجيري اللطيف الذي يحتاج لبيانات حسابك البنكي، مقابل تلقي بريد الكتروني يبدو بالضبط كأنه من أمك. هذا توضيح جيد للاختلاف بين التهديدات ذات الاستهداف الآلي، التي قراءة عنها في القسم السابق. إن هجمات مخصصة مثل تلك تحتاج جمع مسبق للمعلومات، لتحديد الطريقة التي تمكنك من خداع شخص معين والتي غالباً ما تحفظ لأهداف رئيسية.

إن المعتدين يجعلون من الأنظمة التي تتجاهل الاحتياطات الوقائية الأساسية، فريسة لهم. مثل المنتجات التي لها اسم مستخدم وكلمة سر افتراضية. والتي عادة ما ينسى مستخدميها تغيرها. كثير من مُوجِّهات شبكة الإنترنت المنزلية لها كلمة سر افتراضية، فيدهشك عدد المستخدمين الذين يقطنون المكان. جد الكلمة المناسبة وستتمكن من سرقة الإنترنت من جهاز واي–فاي Wi–Fi في بيت جيرانك والتجسس على محادثاتهم. هذا النوع من نقاط الضعف يمكن أن يأتي من المصنع، الذين لا يعطون أولوية للأمان، أو فشل في عامل ما، غالبا خطاء بشري أو تكاسل من الزبون. فمثلا منتج مايكروسفت لقواعد البيانات "ام اس–اس كيو إل" MS–SQL 2005 يباع بدون كلمة سر للمدير، مما يسمح لكل مستخدم التحكم في قاعدة البيانات بأكملها، ما لم يتم وضع كلمة سر لمدير. مواقف أخرى قد تتضمن أنظمة ذات خصائص مناسبة ولكنها تشكل ضعف أمنياً حقيقياً، مثل التي في مفتاح التحكم عن بعد لسيارات بي ام دبليو BMW.

قد تخلق التطبيقات نقاط ضعف إذا ما لم يتم تهيئتها بشكل صحيح. قام باحثون في دارتموث بدراسة بحثية في خدمة من واحد لواحد لتبادل الملفات. والتي فيها يشارك المستخدمين ملفات محددة من حواسيبهم الشخصية مع الأخرين. عادة ما تكون ملفات ترفيهية مثل الأفلام والمسلسلات التلفزيونية. بسبب الإعدادات غير الصحيحة، فبجانب مشاركة حلقة من مسلسل ما بين المستخدمين، فإن عدد منهم وبغير قصد منهم قد شاركوا كشوفات حساباتهم البنكية الشخصية ومستندات ضريبية. دراسة مماثلة وجدت عدد كبير من المؤسسات المالية أنها تسرب مستندات داخلية حساسة بغير قصد، عن طريق تطبيقات لم تُهيئ بطريقة سليمة.

من جهة أخرى، قد تُشكل الأخطاء في الأنظمة نفسها – نقاط ضعف برمجية–والتي تُستغل بواسطة مُعتدين متمرسين. إنه من المستحيل عملياً بناء نظام تقنية معلومات حديث بدون نقاط ضعف مخفية تنتظر من يكتشفها. أنظمة التشغيل الحديثة بها ملاين من سطور الكود البرمجي ولها مئات من العناصر الفرعية التي تتفاعل معها. إن هدف المعتدي هو إيجاد بعض الصدوع في درع ذاك الكود، والتي لا يتصرف فيها النظام بالطريقة التي صمم لها، ومن ثم كشف ذاك الضعف. إن الهجوم الذي يكشف عن نقطة ضعف لم تُعرف مسبقا يسمي زيرو دي"Zero Day". إنه مصطلح أتي من مفهوم أن الهجوم تم في اليوم رقم صفر من إدراك ذاك الضعف لبقية العالم، وبالتالي قبل أن يتم القيام باي عملية معالجة له.

هناك أنواع كثيرة من نقاط الضعف مع عدة طرق لاستغلالها. ولكن النهج الأكثر شيوعا هو إيجاد طريقة للتحايل على حاسوب الضحية بتنفيذ أوامر المعتدي بدلاً من أوامر البرنامج المستهدف. لأن جوهر الأمر يكمن في أن أغلب أنظمة الحواسيب تتعامل مع البيانات على أنها معلومات ليتم معالجتها، وأوامر يجب تنفيذها. إن هذا المبدأ يعتبر أساس فكرة الحواسيب الحديثة ولكنه أيضاً مصدرٌ جوهريٌ لعدم الأمان. لتوضيح جيد، فإن حقن "اس كيو ال" SQL (والتي تنطق "سيكول") هو واحد من أكثر الطرق الشائعة التي تُهاجم بها

صفحات الإنترنت. كثير من تطبيقات الإنترنت تُبنى على لغة الاستعلام الهيكلي "سيكول"SQL (Structure Query Language)، التي هي نوع من أنواع لغات البرمجة تستخدم لإدارة البيانات. وهو نظامٌ فاعل يرجع لفترة السبعينيات. ولكن بدلاً من أن يُدخل المعتدي الاسم والعنوان كما هو مطلوب، يمكن أن يُدخل أوامرا تم تصميمها خصيصا لتجعل قاعدة البيانات تتجاوب معها على أنها كود برمجي بدلاً من بيانات ليتم تخزينها. تلك الأوامر يمكن استخدامها للاستعلام عن قاعدة البيانات وقراءة البيانات وانشاء حسابات جديدة. في بعض الحالات، يمكن استخدامه لاكتشاف وتغير إعدادات الأمان لخادم الإنترنت، مما يسمح للمعتدي بالتحكم في كل نظام الإنترنت. كما سنعرض لاحقاً في الجزء الثاني الفصل عن المخترقين الناشطين، فإن مجموعة المجهولون "انونيمس" (Anonymous) استخدمت نفس هذا النوع من الهجوم لاختراق الأمن لشركة اتش بي غري HB Gary ونشر أسراره المحرجة للعالم.

هناك ما يتجاوز الهجوم على التطبيقات، فيمكن للمعتديين استغلال نقاط الضعف في الكود البرمجي على مستوي النظام. فإن تجاوز سعة التخزين المؤقت هي نقطة ضعف شائعة. تستخدم الحواسيب الذاكرة لتخزين البيانات والتعليمات، إذا ما تم خداع برنامج ما بكتابة بيانات مُدخلة أكثر من المتوقع، عندها قد يفيض عن المساحة أو منطقة التخزين المخصصة، وبالتالي إعادة الكتابة على منطقة يُخزن الحاسوب التعليمات التالية التي يجب تنفيذها. إذا ما قراءة وترجمة مساحة الذاكرة المكتوبة حديثا، فإن البرنامج يمكن له أن يتوقف أو يتبع تعليمات المعتدي. عندها وعندما ينفذ البرنامج التعليمات الاعتباطية، يمكن للمعتدي الحصول على التحكم بنحو فعال للنظام. نظريا، فإن ذاك يتبع نفس مبدأ سيكول "SQL" والتي يفسر فيها الحاسوب البيانات على أنها تعليمات، ولكنه الآن يحصل على مستوي ذاكرة النظام.

يتطلب تصميم ذاك النوع من الهجمات درجة عالية من المهارة والخبرة، ولكن بمجرد استغلال نقطة الضعف يصبح جمع ما هو مطلوبٌ أمراً سهلاً نسبياً. هذا "الاستغلال" هو قطعة من برنامج أو مجموعة من الأوامر يمكنها استغلال نقطة الضعف. عندها ينتقل الخطر الإلكتروني إلى مرحلة حرجة جديدة بالكامل. فتسمح لأخرين، من معتديين أقل تمرسا من الدخول في الصورة. الأمر يبدو كما لو أن لصاً محترفاً يكتب كتاباً عن فتح الخزن والذي يأتي معه طقم معدات سهلة الاستعمال.

إن البرامج الضارة (مال وير) "Malware"، هي عبارة عن استغلال للضعف مسبق الجمع في ملف واحد. غالبا ما تكون هناك مجموعة من التعليمات توضح للنظام ماذا يفعل بعد ما يتم الاستحواذ عليه. بعض البرمجيات الخبيثة تحتوي تعليمات بالتكاثر، لغرض نشر الهجوم. إن الديدان تنشر نفسها تلقائيا في الشبكة، في بعض الحالات قد يتسبب ذلك بضرر بالغ: أغلب الديدان التي هاجمت مايكروسفت ويندوز في أواخر التسعينيات وأوائل السنوات من 2000s، لم يكن لها أثر ضار مباشر، ولكنها غمرت الشبكات المجتمعة. لأنها تحاول ارسال عدد كبير من النسخ. حتى أن واحدة من الديدان تقوم بالبحث عن الحواسيب التي بها نقاط ضعف لتصلحها، تلك دودة صالحة. ولكنها تظل سبباً في شل الشبكة. يتم استغلال بعض نقاط الضعف للسماح للمعتدي من أخذ بياناتٍ شخصية ذات قيمة، أو تدمير بيانات على حاسوب الضحية، بطريقة فوضوية.

إن البرامج الضارة قد تنتشر في الإنترنت عن طريق هجوم "المرور". والذي يكون خطاء الضحية الوحيد هو زيارة الصفحة الخاطئة على الإنترنت. تستغل هجمات مثل تلك نقاط الضعف في متصفح الإنترنت، أو في العناصر العديدة والملحقات التي يستخدمها المتصفح للاستفادة من صفحات الإنترنت المعقدة. يستحوذ المعتدي على خادم الإنترنت أولاً، ثم يحاول ببساطة استغلال نقاط الضعف في المتصفح الذي يطلب ملفات من تلك الصفحة على الإنترنت. إن المعتديين المنفذين لهجمات "المرور" غالبا ما يستهدفون مجموعات عن

طريق السعي خلف صفحات على الإنترنت تُستخدم بواسطة مجتمع معين، تسمي أيضاً بهجمات "منهل الماء" (أتت الفكرة من ان الأسود الذكية لا تُطارد فرائسها عبر الغابة، ولكن تنتظرها فقط للورود لمنهل الماء). على سبيل المثال، فإن ارادت مجموعة سرقة أسرار من شركة دفاع أمريكية، فإنها تستهدفها بطريقة غير مباشرة بواسطة الاستحواذ على صفحة مجلة محبوبة عن تكنلوجيا الفضاء على الإنترنت يقرئها كثير من موظفي تلك الشركة. في بعض الحالات، فهجوم منهل الماء قد يصيب خمسمائة حساب في يوم واحد.

مؤخرا، لم يعد استخدام البرامج الضارة مقصوراً على التحكم بحاسوب ما، ولكن الحفاظ على ذاك التحكم بذاك الحاسوب أيضاً، لغرض استغلال قدراته الإلكترونية ومصادر الشبكة. عن الاستيلاء على أنظمة الضحايا وتنسيق تصرفاتهم، يستطيع المعتدي جمع جيوش من الحواسيب تكون مثل "الزومبي" Zombies. ملايين من الآلات يمكن التحكم فيها بواسطة فاعل واحد عن طريق مجموعة مختلفة من الأوامر واليات التحكم، يمكن وصفهم بالحواسيب المصابة الخارجة عن السيطرة "بوتنت" botnet، واغلب مستخدمي الحواسيب لن يدركوا ما إذا كانوا جزء منها ام لا.

تعتبر الحواسيب المصابة الخارجة عن السيطرة من الموارد القوية لاستضافة نشاطات شنيعة. إن الوصول العادي لآلات الضحايا يسمح بالمراقبة للاستيلاء على بيانات قيمة. يستطيع المتحكمين في الحواسيب المصابة التحكم في اتصالات الشبكة لأنظمة ضحاياهم لإرسال رسائل ضارة أو استضافة صفحات على الإنترنت أو بيع منتجات غير قانونية أو الاحتيال على المعلنين على شبكة الإنترنت. ومن المحتمل أن معظم الحواسيب المصابة باستطاعتها شن هجوم نشر رفض الخدمة "دوز" DDoS (Distributed Denial of Service).

تستهدف هجمات "دوز" DDoS النظم الفرعية المسؤولة عن الاتصالات بالإنترنت. مثل خوادم الإنترنت. إن ضعفهم مبنى على مبدأ أن الاستجابة لطلب قادم يستهلك القدرة الإلكترونية واتصال النطاق العريض. إذا اتصل شخص بهاتفك باستمرار، ستفقد أولا قدرتك على التركيز وثم تفقد القدرة على استخدام الهاتف لأي غرض أخر. وذاك يشبه ما يحصل في عالم الحاسوب، إذا استطاع المعتدي غمر رابط الاتصال، فإن النظام يتأثر وينفصل من الإنترنت. إن من السهولة بمكان الدفاع ضد معتد واحد ومن مصدر ثابت: كل ما عليك هو أن تحظر المرسل، كما لو أنك تحظر رقم متصل مزعج عن هاتفك (ليست أمك إطلاقاً). يستخدم المعتدي في هجوم "دوز" DDoS الافاً بل ملايين من الحواسيب المصابة الخارجة عن السيطرة لغمر خادم الضحية. انه كمحاولة الالاف بل الملايين من الناس الاتصال بهاتفك في الوقت ذاته، عندها لن تستطيع إنجاز أي شيء وحسب؛ ولكنك لن تستطيع استقبال المكالمات التي تريدها بسهولة.

هذا النوع من النفوذ، وحقيقة أن هجمات مثل تلك واضحة وجلية، فإن هجمات "دوز" غالبا ما تكون مرتبطة بأهداف أخرى. قد تهدد العصابات الإجرامية أصحاب صفحات على الإنترنت بإغلاقها ما لم يدفعوا للحماية (يا لها من صفحة رائعة تملكها، يا للأسف لو حصل شيء ما). أو تستخدم كتمويه، بإشغال انتباه دفاعات الضحية بينما يتم السعي خلف بيانات من جهة أخرى. كما أنها شائعة بكونها نوع من أنواع الاحتجاج السياسي أو القمع. في المراحل الأولية من الأزمة السورية عام 2011، شارك الذين يدعمون النظام الحاكم أدوات "دوز" للهجوم على من ينتقدون الحكومة وعلى المنظمات الإخبارية التي غطت العنف المتزايد.

في النهاية، فإن كل نوع من أنظمة المعلومات موجود في الفضاء الإلكتروني به نقاط ضعف. بغض النظر عن مقدار الخوف في ذلك، فإن اغلب هذا الضعف ليس بجديد. على سبيل المثال، فالهجوم الذي يهدف

لتجاوز سعة التخزين، تم تطويره أولا في السبعينيات والذي كاد ان يدمر الإنترنت اليافع في الثمانينيات. ظهر دليل يبين الطريقة بحلول عام 1996 في مجلة المخترقين.

بتطور التهديدات، تتطور معها ردودنا لتك التهديدات. فالبعض يمكن تقليله بتغيرات بسيطة في تصرف الحاسوب أو تغيرات طفيفة في الكود البرمجي. بينما هناك أنواع كاملة من نقاط الضعف يمكن كشفها عن طريق تطوير وتحقيق تقنيات جديدة. نقاط الضعف الأخرى هي ببساطة عواقب بنائية لكيفية استخدمنا النظم. كما سنستعرض في الجزء الثالث، أنه بتفحصنا لتلك التهديدات نجد أن علينا في النهاية تقبل أن الأشخاص السيئون سيستغلون ذاك الضعف، وثم تطوير أفضل ردود ممكنة تسمح لنا بالحفاظ على الاستفادة من الجزء الصالح من العصر الإلكتروني.

أو يمكنك الانسحاب، وبيع عربتك الفارهة المتطورة وركوب البص بدلاً منها. ولكن احرص من عدم التأكد من مواعيد البص على الإنترنت.

كيف لنا أن نثق بأحد في الفضاء الإلكتروني؟

ربما ليس هناك واجب مهم على المواطن مثل التصويت، وليس هناك جزء مهم في عملية التصويت غير المحافظة على نزاهة ذاك الصوت. لم يتخيل الأب الواضع للدمقراطية في أمريكا عالماً من الات التصويت المحوسبة، ولا كان أحد تخيل أن لعبة الفيديو "باك-مان" Pac-Man قد تشق طريقها للانتخابات.

بدأت الواقعة كواحدة من المشاريع الترفيهية التي يتقوم بها المخترقون، يقضون فيها قليلاً من أوقات بعد الظهيرة يعبثون بقطعة قديمة من معدات الحاسوب. كان الاختلاف في هذه الحالة، هو أن المعدات كانت مكينة التصويت الإلكترونية "أي في سي-ايدج" AVC Edge والتي استخدمت في انتخابات عام 2008.

أنظمة مثل تلك يفترض بها أن تكون مضادة للتلاعب أو على الأقل أن تكشف ما إذا حاول أي شخص فحصها. ومع ذلك فقد استطاع باحثان من جامعة مشقن وجامعة برنستون إعادة برمجة الالة بدون ترك أي أثر على ختم كشف التلاعب. عندما اختار الاثنان برمجة الة التصويت بطريقة غير ضارة للعب لعبة باك–مان، لعبة الفيديو المحبوبة من فترة الثمانينيات. فقد أشاروا وبوضوح إلى أن الالة التي يفترض بها أن تكون مقاومة للتلاعب بها نقاط ضعف لهجمات أكثر مكراً.

كما أوضحت الواقعة، فإن اعتمادنا على الأنظمة الرقمية يعني أنه وبطريقة متزايدة نواجه السؤال عن كيف لنا الثقة بتلك الأنظمة. على المستخدم الثقة بالأنظمة في الأمن الإلكتروني، وعلى الأنظمة معرفة كيفية الوثوق بالمستخدمين. ليس على كل آلة إظهار لعبة باك–مان غير مرغوب بها على شاشتها لتخبرنا أن هناك خطب ما. كيف لنا أن ندري إذا ما كان الحاسوب يتصرف بالطريقة التي يفترض به أن يتصرف، أو أن ذاك البريد الإلكتروني من زميلك هو حقا من ذاك الشخص. وكما هو من الأهمية بمكان أنه كيف للحواسيب معرفة ما الذي يفترض بنا أن نكون أو أننا نتصرف بالطريقة التي يفترض بنا أن نتصرف بها.

إن الثقة على الإنترنت مبنية على التشفير- فإن تأمين الاتصالات يرجع إلى أوائل الشيفرات التي استخدمها يوليوس قيصر وجنرالاته لمنع العدو من فهم رسائلهم السرية. عادة ما نفكر في التشفير على أنه وسائل لحفظ المعلومات بشكل سري، ولكنه يلعب دورا بنفس الأهمية في النزاهة، أو القدرة على تحديد أي تلاعب.

أن اللبنة الأساسية في بناء التشفير هي ما يسمي "هاش" (Hash). إن مهمة الهاش هي في أخذ أي جزء من البيانات وتوزيعه على مخرجات أصغر ذات طول محدد مع خاصيتين محددتين: أولاً، أن المهمة تتم باتجاه واحد، والتي تجعل من الصعب تعقب أصل البيانات من المخرجات. ثانياً، والأكثر أهميةً، هو أنه من

الصعب بطريقة لا تصدق إيجاد جزئيين مدخلين من البيانات بنفس الهاش الناتج. يُمكننا ذلك من استخدام مهمة الهاش لوضع بصمة على مستند أو بريد الكتروني، عندها قد نتمكن من استخدام البصمة للتأكد من صحة المستند. إذا لم تتطابق بصمة موثوقة على مستند مع بصمة أنت صنعتها باستخدام نفس الطريقة، فإن الذي بين يديك مستند مختلف.

التحقيقات في نزاهة التشفير أمر مفيد، ولكن لجعلها تطبق عل الثقة نحتاج لبعض الوسائل لتعريف الهوية. إن الثقة كما هي اسم فهي أيضاً فعل متعد يتطلب شخص ما أو شيء ما لتثق به. توفر التوقيعات الرقمية المشفرة تلك الثقة باستخدام التشفير غير المتماثل. بدأ هذا الشرح بأخذ منحىً معقداً، لذلك وربما من المفيد الانحراف قليلاً لفهم بعض النقاط الأساسية للتشفير.

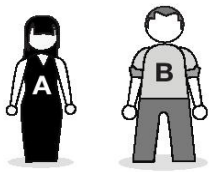
تعتمد أنظمة التشفير الحديثة على "مفاتيح" كطريقة سرية لتشفير أو فك تشفير معلومات قائمة على الثقة. يعتمد التشفير غير المتماثل على مشاركة نفس المفتاح مع طرف اخر موثوق. فأنا أقوم بتشفير البيانات بنفس المفتاح الذي تستخدمه أنت لفك تشفيرها. إن الأمر كما لو أننا نتشارك نفس المفتاح لخزينة بالبنك.

ولكن ماذا لو لم نلتقي من قبل؟ كيف لنا أن نتبادل هذه المفاتيح السرية بشكل آمن. إن "التشفير غير المتماثل" يحل تلك المشكلة. إن الفكرة تكمن في أن يتم فصل المفتاح السري إلى مفتاح عام والذي يتم مشاركته مع كل شخص، ومفتاح خاص يظل سراً. إن المفتاحان تم انتاجهما بطريقة تُمكن إذا ما تم تشفير شيء بالمفتاح العام يفك تشفيره بالمفتاح الخاص المتوافق معه، وبالعكس. يوضح الشكل 1.2 طريقة عمل المفتاح العام في تشفير وحماية خصوصية رسالة ونزاهتها معا. لنفترض أن اليس وبوب –الابطال الابجديين لأمثلة التشفير– ارادا التواصل. يملك كل منهما زوجا من المفاتيح، ويستطيعان الوصول للمفاتيح العامة لكليهما. إذا ارادت

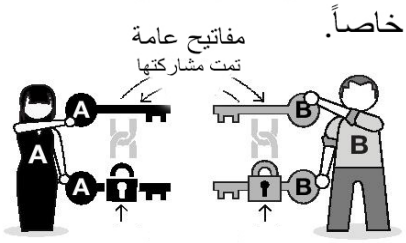
اليس إرسال رسالة لبوب فإنها تقوم بتشفير الرسالة بمفتاح بوب العام، عندها فإن الشخص الوحيد الذي بمقدوره فك تشفيرها هو من يملك الوصول لمفتاح بوب الخاص.

طريقة عمل المفتاح العام في التشفير

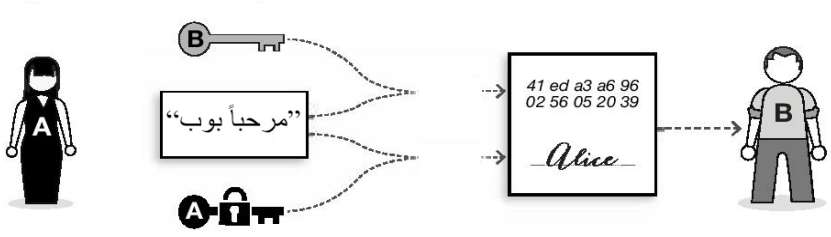
1. هذان أليس وبوب. يودان التحدث مع بعضهما بطريقة آمنة.



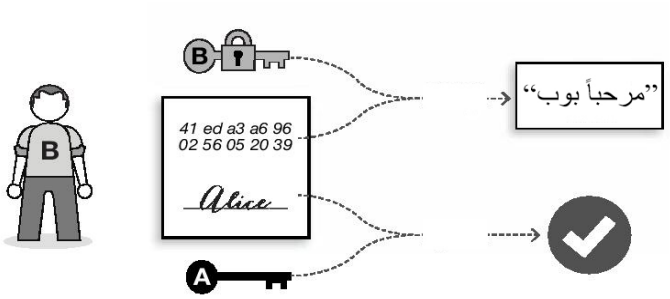
2. لكل منهما زوج من المفاتيح مرتبطة مع بعضعا، يتشاركان واحداً ويحتفظان بالأخر خاصاً.



3. لإرسال رسالة، تقوم أليس بتشفير الرسالة بمفتاح بوب العام، وثم تقوم بالتوقيع عليها بمفتاحها الخاص.



4. يتلقى بوب الرسالة، يقوم بفك تشفيرها بمفتاحة الخاص، ثم يستخدم مفتاح أليس العام للتأكد من توقيعها.



يحمي التشفير مصداقية الرسالة، بينما يوفر التوقيع الإلكتروني النزاهة بمنع حدوث تعديل.

الشكل 1.2

يربط التوقيع الرقمي لرسالة مفهوم البصمة بتشفير المفتاح العام معاً. بالرجوع لأصدقائنا اعلاهم، تأخذ اليس بصمة لمستند وتوقعه بمفتاحها الخاص ثم تمرره لبوب بصحبة مستند غير مشفر. يتأكد بوب من التوقيع باستخدام مفتاح اليس العام ثم يقارنه ببصمة يستطيع إنشائها من مستند غير مشفر. إذا لم يتوافقا فهناك من بدل المستند بينهما. يمكن لهذه التوقيعات الرقمية توفير النزاهة لأي نوع من البيانات ويمكن ربطها لتسمح بثقة ممتدة.

ولكن من اين أتت الثقة في المقام الأول؟ فمثلا، أستطيع التأكد من صلاحية برنامج انزلته من شركة عن طريق التحقق من مفتاح الشركة العام. ولكن كيف لي أن اعرف أن ذاك المفتاح يعود لتلك الشركة حقا؟ تذكر بان التوقيع يدل فقط للوصول إلى المفتاح الخاص الذي يتوافق مع المفتاح العام وليس صلاحية ذاك المفتاح العام. يتطلب التشفير غير المتماثل بعض الوسائل للوثوق بالمفاتيح العامة. في اغلب الأنظمة الحديثة فإننا نعتمد على "الطرف الثالث الموثوق". هي منظمات تنتج شهادات رقمية موثوقة تربط كيانا ما بمفتاح عام بشكل جلي وواضح، تعرف بمصدقي الشهادات "سي اى" Certificate Authenticators (CAs)، يقومون بتوقيع الشهادات، ومفاتيحهم العامة معروفة على نطاق واسع يحيل دون تقليدهم. إذا ما وثقت بمصدق شهادة فيمكنك الوثوق بالمفتاح العام الموقع بواسطة مصدق الشهادة ذاك.

يستخدم كل شخص على الإنترنت هذا النظام بوتيرة يومية، حتى ولو لم ندرك ذلك. عند زيارتنا لعنوان "اتش تي تي بي اس" HTTPs على الإنترنت، نلاحظ رمز قفل صغير يؤكد أمن الاتصال، فنحن عندها نزور موقعا آمن على الإنترنت ونثق بمصدق الشهادة. يسأل متصفحنا النطاق الآمن عن مفتاحه العام وشهادة موثقة من مصدق شهادات تربط المفتاح العام بشكل جلي وواضح بطاق الإنترنت ذاك. بالإضافة إلى التأكد من انتماء الخادم الذي يتحدث معه متصفحنا إلى المنظمة التي يدعي الانتماء إليها. يمكن هذا أيضاً من اتصالات

موثوقة عن طريق تبادل مفاتيح التشفير. تخدم نقطة مثل تلك كأساس كل الاتصالات الآمنة تقريبا على الإنترنت ما بين طرفين لا يرتبطان بصلة.

كمصدر للثقة، فإن مصدقي الشهادات يلعبون دوراً حاسما في النظام البيئي للفضاء الإلكتروني. وربما مهم أكثر مما ينبغي. إذا استطاع أحد ما سرقة المفتاح الذي يستخدمه مصدق الشهادات لتوثيق الشهادات، عندها يمكن للص (أو أي جهة أخرى بحوزتها المفتاح) أن يعترض حركة البيانات الآمنة بدون ملاحظة الضحية. من الصعب النجاح في ذلك، ولكنها حصلت بالفعل. ففي عام 2011، شخص ما (التسريبات لاحقاً إشارات بأصبع الاتهام نحو وكالة الأمن القومية "إن اس اى") تمكن من سرقة مفاتيح مصدق شهادات هولندي واستخدمها في اعتراض دخول المستخدمين الايران لمزود البريد الإلكتروني "جيميل" Gmail من قوقل. يشتكي البعض من وجود العديد من موثقي الشهادات حول العالم، والكثير منها في بلدان ما كان لها إلا القليل في تاريخها بالأمن والخصوصية. وبتطور التهديدات، فستصبح جذور الثقة في خطر محدق أكثر مما سبق.

إذا كان جانب واحد من الثقة على الإنترنت هو شعور المستخدم بالثقة تجاه النظام والمستخدمين الأخرين. فالجانب الأخر هو كيف للأنظمة الثقة بالمستخدمين بعد التأكد من الهوية والمصداقية، فعلي النظام السماح للمستخدم باستخدام النظام. تستخدم أغلب الأنظمة نوع من "التحكم في الوصول" لتحديد ما يمكن لكل واحد فعله. وببساطة، فالتحكم في الوصول يعطي القدرة على القراءة والكتابة أو تنفيذ كود برمجي في بيئة تشغيل.

إن نواة كل نظام تكمن في سياسة التحكم في الوصول، هي مصفوفة من المواضيع والاهداف التي تُعرف من الذي يمكنه فعل أي شيء ولما؟ يمكن أن يكون بسيطاً (يستطيع الموظفون قراءة أي مستند في مجموعة عملهم الصغيرة، بينما يستطيع المدراء الوصول لأي مستند على مستواهم الاعلى) أو أكثر تعقيداً،

(يمكن لطبيب قراءة ملف أي مريض، طالما أن ذاك المريض له عرض مرضي يقابل قائمة مسبقة الإعداد، ولكنه يستطيع الكتابة فقط على ذلك الملف بعد أن يعطي نظام الحسابات الأحقية بعد عملية الدفع). تتطلب سياسات الولوج الجيدة للتحكم فهم واضح للأدوار التنظيمية وأسلوب بناء نظام المعلومات معاً، وأيضاً القدرة على توقع الاحتياجات المستقبلية. في المنظمات الكبيرة التي يستخدم مستخدميها قدراً واسعاً من البيانات، فإن تعريف هذه السياسات بطريقة مثالية أمراً صعباً بقدر لا يصدق. يؤمن الكثيرون بأنها قد تكون حتى مستحيلة.

كانت اعطال التحكم في الوصول خلف بعض الفضائح الإلكترونية ذائعة الصيت في السنوات الخيرة. كقضية برادلي مانينغ ووكيليكس في عام 2010 والتي سنستعرضها فيما يلي، وقضية إدوارد اسنودن عام 2013 (التي فيها متعاقد بدرجة صغري يعمل كمدير للأنظمة في وكالة الأمن القومي، وكان يستطيع الوصول إلى برامج دفينةٍ غاية في السرية ومثيرةٍ للجدل. والتي سربها للصحافة) هذه القضية توضح فقر التحكم في الوصول بكل ما يحمله من مجد. من افراد ذوي مستوي منخفض يعطون الوصول الافتراضي لأي شيء وكل شيء يطلبونه، إلى الجهود الضعيفة لتسجيل ومراجعة الوصول (بعد عدة شهور من اشهار إدوارد سنودن المستندات المسربة عن برامج المراقبة المتعددة للوكالة، لا تزال وكالة الأمن القومي تجهل عدد المستندات التي اخذها والتي لم يبح بها بعد).

بغض النظر عما إذا كانت المنظمة هي وكالة الأمن القومي أو متجر للخبائز، فإن الأسئلة عن كيف تُجزء البيانات أمراً ضرورياً. للأسف فإن أغلب المنظمات إما أنهم شديدي التحوط والحرص أو أنهم لا يعطون الأمر أهمية عندما يتعلق بالوصول، بدلاً من محاولة إيجاد حل وسط. تعطي المبالغة في الاستحقاقات الحق بالوصول للعديد من الأشخاص دون مصلحة واضحة في المؤسسة، مما يؤدي إلى خروقات كارثية محتملة من نوع وكيليكس. يشكل هذا النوع من الوصول المبالغ فيه في الكثير من مجالات الأعمال التجارية والرعاية

الصحية مخاطر خرق قوانين –صراع المصالح– التي يفترض بها أن تمنع الأفراد من الوصول إلى أنواع معينة من المعلومات. في النهاية، وما يتعلق بالأمن الإلكتروني أكثر، أنه إذا كان التحكم في الوصول ضعيفا، فقد تفقد المنظمات حمياتها لملكيتها الفكرية تحت قانون الأسرار التجارية.

أما في الجانب الأخر، فإن الحد من الاستحقاقات له أيضاً مخاطر. ففي الأعمال التجارية، قد يقلل قسم من قسم أخر بدون قصد إذا لم يكن له إمكانية الوصول إلى نفس البيانات. ففي مستشفى، قد يكون الأمر حرفياً مسالة حياة أو موت إذا لم يستطع الأطباء إيجاد ما يحتاجونه من المعلومات بسهولة في حالات الطوارئ. أشار ضباط سابقون في جهاز المخابرات إلى أن المراهنات أكبر في عالمهم، حيث أن عدم مشاركة المعلومات قد يخلف نقاطاً مصيرية غير متصلة ومؤامرات إرهابية مثل الحادي عشر من سبتمبر التي لم يتم ادراكها.

ما يوضحه هذا كله هو أنه حتى في خضم النقاش للتكنلوجيا والهاش والتحكم في الوصول، فإن الثقة دائما ما تعود إلى سيكولوجية البشر والقرارات التي تُستخدم لحسابات المخاطر الواضحة الجلية. إن باك–مان ليس برجلاً حقا، ولكن النظام الذي سمح له بالدخول في آلة التصويت وعواقب ذلك الدخول إنما هي كلها بشرية محضة.

تركيز: ما الذي حصل في وكيليكس:

Bradass87: سؤال افتراضي: إذا كانت لك حرية التحكم في شبكات سرية لمدة طويلة [*sic*] (اقتباس حرفي)، لِنَقُّل ثمانية أو تسعة شهور، وقد راءيت أشياء مذهلة وأشياء شنيعة، أشياء تنتمي للنطاق العام وليس في خادم مُخزن في غرفة مظلمة في العاصمة واشنطن – ماذا كنت لتفعل؟

Bradass87 (12:21:24 PM): فالنقل... قاعدة بيانات لنصف مليون واقعة خلال حرب العراق من عام 2004 حتي 2009، مصحوبة بتقارير ومجموعات زمنية بتواريخها ومواقع جغرافية وأرقام ضحايا. أو مئتان وستون ألف برقية لوزارة الخارجية من السفارات والقنصليات حول العالم، تشرح كيف يستغل العالم الأول العالم الثالث. بالتفاصيل ومن منظور داخلي.

Bradass87 (12:26:09 PM): لنقُل فقط أن هناك *شخص ما* أعرفه بشكل قريب جداً. كان يتسلل إلى شبكات الولايات المتحدة السرية ينقب عن الملفات التي ذكرتها سابقا، وكان ينقل تلك البيانات من الشبكة السرية عن طريق "فجوة هواء" إلى حاسوب على شبكة تجارية يخزن فها تلك البيانات ويضغطها ويشفرها ثم يرفعها إلى أُستراليٌ مجنون ذا شعر ابيض، والذي بدوره لا يظل في بلد واحد لفترة طويلة.

Bradass87 (12:31:43 PM): الشخص المجنون ذا الشعر الأبيض هو جوليان اسينغ.

Bradass87 (12:33:05 PM): بعبارة أخرى... فقد أحدثت فوضي عارمة.

هذه المحادثة دارت في برنامج آى أو أل (AOI) للرسائل الفورية، والتي أطلقت واحدة من أكبر الوقائع في التاريخ الإلكتروني. لم تُغير فقط وكيليكس الطريقة التي يفكر بها العالم عن الأسرار الدبلوماسية، ولكنها أصبحت نقطة محورية لفهم كيف أن الفضاء الإلكتروني قد غير علاقتنا جذريا بالبيانات والوصول.

أُطلِقَت صفحة الإنترنت وكيليكس عام 2006 بهدف "كشف الفساد والاستغلال حول العالم" مع أجندةٍ سماها الباحثون بالشفافية الجوهرية، كان الغرض اصلاح تصرفات ممثلين أقوياء عن طريق كشف أدلةٍ موثقةٍ لاعتداءاتهم على الإنترنت. كان ذلك بقيادة الرجل الذي أصبح يعرف رمزيا "بالرجل المجنون ذو الشعر الابيض" الأسترالي جوليان اسينغ. فقد استخدم نموذج ويكيبيديا Wikipedia "لمصدر مفتوح ووكالة استخبارات

ديموقراطية" والتي فيها الناشطون في انحاء العالم يضيفون المعلومات ويشاركونها خلال مشروع ارشيفي مركزي ولكنه عام.

سرعان ما اكتسبت المجموعة سمعة بنشرها معلومات متعلقة بمجموعة من الدول المختلفة، وفساد ومخالفات واخفاقات محتملة. كشفت المشاريع الأولى الاعتداءات المزعومة للسياسيين الكينين ومحامين الكنيسة السيانتولوجيا والمفاوضين التجاريين العالمين. وسرعان ما بدأت بتلقي الثناء من منظمات مكافحة الرقابة وحقوق الإنسان.

بالمقابل فسرعان ما أصبحت الشفافية الجوهرية واضحة للمنظمات وأنها اعتمدت على السرية. اشارت وزارة الدفاع الامريكية في تقرير عام 2008 أن وكيليكس تمثل قوة حماية محتملة ومضادة للمخابرات والعمليات السرية وأمن المعلومات وخطراً على جيش الولايات المتحدة (ولسخرية القدر، فقد علمنا بذاك التقييم السري فقط عن طريق وكيليكس نفسها التي نشرته عام 2010).

سبقت وزارة الدفاع الأحداث بصورة مدهشة في الوقت الذي كان فيه الموقع على الإنترنت يستعد لنشر عدد ضخم من المستندات، تفاوتت ما بين برقيات دبلوماسية ومذكرات داخلية وفيديوهات مرتبطة بالأعمال الحربية للقوات العسكرية للولايات المتحدة في العراق وأفغانستان. بداية القصة ترجع إلى bradass87 اسم المستخدم على الإنترنت لبرادلي مانينغ المولود عام 1987.

كان برادلي مانينغ جندي من الدرجة الأولي في جيش الولايات المتحدة، ولم يكن من السعداء. كما وصف في الرسائل الفورية التي أرسلها لمخترق أخر اتضح أنه صحفي "أنا محلل استخبارات في الجيش، المنتشر في شرق بغداد، في انتظار صرف من الخدمة لعدم التكيف بدلاً عن اضطراب في الهوية".

وجدت التحقيقات لاحقاً أن مانينغ كان يندمج مع الجنود بصعوبة، وأنه قد تم معاقبته بسبب الكشف عن معلومات أكثر من اللازم في رسائل الفيديو لأصدقائه وعائلته والتي كان يُحمّلها على يوتيوب. في الحقيقة، ما كان ليتم توزيعه في العراق بسبب وصف مشرفه له بأنه "خطر على نفسه وغالباً على الأخرين". ولكن الحاجة لعمال استخبارات في الميدان كانت كبيرة، ولذا تم إرساله لمنطقة الحرب.

بما أن تدريب مانينغ كان في التعامل مع المعلومات السرية، فهو لم يكن محللاً. بل كانت وظيفته "التأكد من أن يصل المحللون الأخرون في مجموعته لكل شيء هو مصرح لهم برؤيته". ولذلك فإن موقعه مكّنه من الوصول لنطاق واسع من انسياب البيانات من مختلف حواسيب الشبكات الحكومية.

بعد ازدياد توتره من الحرب، أتت ردة فعله ممتزجة مع اضطراباته الشخصية، فقرر مانينغ أن "المعلومات يجب أن تُتحرر". في الوقت الذي منعت فيه وزارة الدفاع أجهزة تخزين "يو اس بي" USB خوفا من البرامج الضارة ومحاولة منها لعزل الشبكة عن الإنترنت. لكنهم لم يمنعوا الأقراص المضغوطة القابلة لإعادة الكتابة. فكان مانينغ يجلب معه أقراص بها موسيقي ثم يمحوها وينقل عليها ملف تلو ملف من البيانات السرية. وكما كتب "كنت استمع لأغنية "تيلفون" Telephone للمغنية "ليدي قاقا" Lady Gaga وأحرك شفتاي معها [*sic*] (اقتباس حرفي)، في الوقت الذي كنت فيه اسحب أكبر تسريب بيانات محتمل في التاريخ الأمريكي".

نشرت وكيليكس عام 2010 مقطع فيديو بعنوان مثير "أعمال قتل عشوائية" من طائرة أباتشي العمودية التابعة للولايات المتحدة، عرض الفيديو المحرر بطريقة مفصلة الطائرة وهي تطلق النار على مدنين في العراق منهم صحفيين اثنين من وكالة رويترز الاخبارية. نشرت وكيليكس بعدها كمية من البيانات تعتبر كالكنوز الدفينة بكم هائل في يوليو واكتوبر من عام 2010 لمستندات سرية متعلقة بالحروب في أفغانستان والعراق.

في الوقت الذي أراد فيه ماننغ ان يظل مجهول الهوية كما هو نموذج وكيليكس. سعى ميسر اموره اسينغ لتحقيق العلانية المطلقة. تم عرض الفيديو لأول مرة في مؤتمر إخباري في نادي الصحافة القومية في العاصمة واشنطن. أما بالنسبة للمستندات السرية فقد عمل اسينغ مع "نيويورك تايمز" New York Times وصحيفة "قارديان" Guardian و "دير سبيقل" Der Spiegel للتأكد من صحة المستندات وتحليلها وتقديمها للجمهور. وبشكل غير مفاجئ، فقد ادان المسؤولون الأمريكيين نشر تلك المستندات بلهجة قوية، وبدأوا بتتبع مصدر التسريبات.

بعدها بعدة شهور فقط، اسقطت وكيليكس قنبلة افتراضية أخرى. هي تسريب البرقيات الدبلوماسية للولايات المتحدة، فيما أصبح يعرف بـ "كيبل قيد" Gable gate، سلم ماننغ أيضاً 251,287 برقية لوزارة الداخلية كتبت بواسطة 271 سفارة وقنصلية أمريكية في 180 دولة، ينحدر تاريخها من ديسمبر 1966 إلى فبراير 2010. كانت أغلب الأشياء مملة، ولكن كان هناك عدد من الأسرار المحرجة أيضاً، بدأ بأوجه نظر السفراء الأمريكيين في نظرائهم إلى حقيقة أن الولايات المتحدة كانت تسترق السمع سراً على الأمين العام للأمم المتحدة فيما أدى لحرب العراق. ومن المدهش أن حكومة الولايات المتحدة أمرت الموظفين الفدراليين والمتعاقدين بعدم قراءة المستندات التي تضمنت أسرار وزارة الداخلية التي تم نشرها على الإنترنت، ووصفت نيويورك تايمز هذه الحادثة بـ "فعل تقليدي لإغلاق باب الحظيرة بعد خروج الحصان".

في الحقيقة، اعتمدت وكيليكس على مصادر إعلامية مثل قارديان و "إل باس" El Pais و "لى موند" Le Monde لنشر البرقيات، والتي نشروها بقدر قليل. ركزت الجهات الإعلامية على ما ظنت انه أكثر أهمية وحررت محتواه متي ما رأت انه قد يشكل خطرا على شخص ما تم ذكره في البرقيات بدون قصد، مثل معلومات سرية. لم تتم نشر سوى مئة أو ما يزيد في المرة الواحدة، والتي هي جزء صغير من جملة المستندات المسروقة.

بعد عدة شهور تلت، وبطريقة ما، تم نشر كلمة السر لكامل قاعدة البيانات "عن طريق الخطاء" (القى كل من الصحفيين من صحيفة قارديان واسينغ اللوم على الأخر). وبما أن الصفحة الآن أصبحت متاحة للوصول، فد قررت وكيليكس نشر كنز المعلومات السرية التي بحوزتها بصورة غير محررة ومعدلة.

أُدينت المستندات المسربة بشكل صارم، واتهمت وكيليكس بوضع الناس في خطر، وليس المسؤولون الأمريكان وحدهم. وعلى سبيل المثال، في الصين، بدأت المجموعات الوطنية ما سموه بـ "صيد الأشرار على الإنترنت"، يهددون بالعنف ضد الصينين المعارضين الذين وردت أسمائهم في البرقيات بأن لديهم اتصال بالسفارة الامريكية.

أصبحت وكيليكس في هذه النقطة أكثر من كونها ازعاج لمن هم في السلطة. وعلى حسب رأي مدير المخابرات الوطنية الأمريكية، فإن التسريبات "شكلت ردود فعل خطيرة وكبيرة علي أمننا القومي"، وأن عضو مجلس الشيوخ قد دعي بأن يحضر اسينغ لمحاكمته بالتجسس. بينما سعي أخرون لتهدئة ردة الفعل. كما قالها لاحقاً وزير الدفاع قيتز "هل هذا محرج؟ نعم. هل هو غريب؟ نعم. عواقب على السياسة الخارجية للولايات المتحدة؟ "اعتقد ان ذلك واضح ببساطة".

في كل الحالات، فقد بلغ الغضب ذروته تجاه المنظمة ومؤسسيها الرئيسين. أُغلق حساب اسينغ الشخصي في بنك سويسرا على أساس أنه قد ادعى زوراً عيشه في جنيفا في وقت فتح الحساب. وحتى أن هناك ما كان أكثر ضرر، وهو اصدار النيابة العامة السويسرية مذكرة بحق اسينغ في اعتداء جنسي. وبعد صراع قانوني خسره بشأن تسليمه، سعى اسينغ خلف اللجوء السياسي في السفارة الأكوادورية في لندن، والتي ظل فيها وكانت مقره حتى وقت صدور هذا الكتاب.

وفي توضيح اخر عن كيفية تداخل العالم الإلكتروني مع العالم الحقيقي، فقد تمت ملاحقة المجموعة بواسطة الجبهة المالية على الإنترنت. فقد أعلنت شركة "بي بال" PayPal للمعاملات المالية على الإنترنت عن عدم السماح للأفراد بإرسال المال لحساب وكيليكس، نقلا عن خطاب من حكومة الولايات المتحدة تعلن فيه انخراط وكيليكس في اعمال إجرامية. تبعتها شركات "ماستر كارد" MasterCard و "فيزا" Visa، مما جعل الأمر أكثر صعوبة على المتعاطفين حول العالم للمشاركة في الدفاع القانوني والتقني للصفحة.

نجت منظمة وكيليكس برغم من كل ذاك الضغط. ان الملفات المسربة ما زالت موجودة على الإنترنت على عدة نسخ من صفحات الإنترنت لكل شخص يود الاطلاع عليها (ماعدا الموظفين الفدراليين)، في الوقت الذي أظهرت فيه المجموعة فضائح لاحقة كشفت التجسس الداخلي لوكالة الأمن القومي "إن اس اى" NSA على الملفات السورية، نشر أكثر من مليوني رسالة بريد الكتروني للنظام الحاكم السوري، تضمنت رسائل شخصية من بشار الأسد. والأكثر أهمية، ان نموذج وكيليكس قد اثبت قوته، فقد الهم محاولات تقليد مثل "لوكل ليكس" Local Leaks، التي هي صفحة مرتبطة مع مجموعة المجهولين "انونيمس" Anonymous. وحظيت لوكل ليكس بالأهمية عام 2012، عندما نشرت دليلاً على اعتداء جنسي جسيم تم بواسطة لاعبي كرة قدم مشهورين في المرحلة الثانوية في مدينة أوهايو.

بالنسبة لمانينغ، فقد افتضح دوره بواسطة نفس الشخص الذي شارك معه الدردشة التي كان يفترض بها أن تكون سراً على الإنترنت. أخبر مخترق يدعى ادريان لامو مانينغ "أنا صحفي وكاهن. أختر أيهما شئت، وتعامل مع هذا إما على أنه اعتراف بخطيئة أو مقابلة صحفية (لن تنشر ابداً) وتمتع بالقليل من الحماية القانونية." وعوضاً عن ذلك، فقد سلم لامو مانينغ لمكتب التحقيقات الفدرالية "إف بي اى". مثل مانينغ لاحقاً

أمام المحكمة العسكرية بتهمة سرقة البيانات والتجسس، وحكم عليه بالسجن خمس وثلاثون سنة في سجن عسكري.

في النهاية، فإن هؤلاء الذين تمنوا إطلاق المعلومات حرة، هم أنفسهم لم يعودوا احراراً. قد يرتدع أخرون بما حل بأبطال هذه الرواية، أو يتشجعوا بما خلفوه من أثر دائم.

ما هو التهديد المتطور المستمر Advanced Persistent Attack(APT)؟

كنا في اجتماع في العاصمة واشنطن تضمن مسؤولون حكوميون وقادة رجال الأعمال. أمضي ما يسمى مستشار في الأمن الإلكتروني (على الأقل هذا ما كتب على موقعه على الإنترنت، ومن نحن لنشكك في الإنترنت؟) نصف عرضه يروج عن البعبع الخطر الإلكتروني الهائل الذي لاح في الأفق لنا جميعا، وذكر مراراً الشبح الجديد للتهديدات المتطورة المستمرة APTs "اى بي تي اس" ولكن لحسن الحظ، فقد أمضي النصف الأخر من حديثه يشرح كيف أن كل ما هو مطلوب لردع التهديدات أن تكون "جيدة بما فيه الكفاية." وقال نكته فيما لو كان صديقان يلاحقهما دب، فأخبر أحدهما الأخر "ليس علي سبق الدب، فقط أنت." بشرط أن تتأكد من أن دفاعاتك أفضل ولو بقليل من دفاعات الشخص التالي، وأوضح بان المعتدين سرعان ما يستسلمون ويتركوك وشانك. وسيدهشك أن تعرف بان لشركته حزمة متكاملة للبيع ترضي جميع احتياجاتنا في الأمن الإلكتروني. كان العرض ماهراً وفعالاً... وخاطئاً.

إن التهديدات المتطورة المستمرة هي ظاهرة قد حظيت بسمعة سيئة في السنوات الأخيرة (أشارت تقارير من قوقل أن المصطلح قد أُستخدم أكثر من 10 ملاين مرة في عام 2013) ومع ذلك لا يزال غير مفهوم

وواضح. وذلك يوضح التحدي في سياسة العالم في جلب الانتباه لتحديدات حقيقة قادمة في الفضاء الإلكتروني، ولكنه يتجنب المبالغة في ردة الفعل والضجة والهستيريا.

إذا كانت التهديدات للأمن الإلكتروني عبارة عن أفلام، فإن التهديدات المتطورة المستمرة تكون مثل فلم "أوشن ايلفن" Ocean 11. ليس لأن نجوم التهديدات المتطورة المستمرة هم بوسامة الممثلين مثل جورج كلوني وبراد بين؛ في الحقيقة، من الأرجح أنها تدار بواسطة نقائضهم، يرتدون الأقمصة قصيرة الأكمام بدلاً عن البدل الأرمينية. ولكن مثل السرقة الكبيرة التي تمت في الفلم، فإن التهديدات المتطورة المستمرة على أي حال لها مستوي من التخطيط يضعهم بعيداً عن التهديدات الإلكترونية الأخرى. إنها عمل فريق يجمع بين التنظيم وجمع المعلومات والتعقيد والصبر. وكما هو في الفلم فسرعان ما تتبعها عواقب. لا أحد يعلم كم عدد التهديدات المتطورة المستمرة الموجودة في العالم، ولكن أخبرنا مدير إحدى شركات الأمن الإلكتروني أنه "كان قبل خمس أعوام قد أتحمس ويعتريني الفخر إذا ما وجدت علامة لتهديد متطور مستمر داخل شبكات العميل، ذاك شيء كان قد يحدث كل بضعة أشهر، أما الأن فإننا نجدها يوميا".

تبدأ التهديدات المتطورة المستمرة بهدف محدد. يعرف الفريق ماذا يريد ومن يسعي خلفه لينال ما يريد. تتفاوت أهداف التهديدات المتطورة المستمرة ما بين تصاميم لطائرات حربية إلى أسرار تجارية لشركات البترول. وحيث يعتقد العديد منا أنه مهم لدرجة أنه قد يستهدف بواسطة تهديد متطور مستمر، فالحقيقة أن كثير منا لا يرتقي لذاك المستوى. ولكن إذا ما حصل ذلك، فمن الأفضل لك أن تحترس، فإغلاق النوافذ مثل أي شخص أخر في الحي غالباً لا يكفي. إن الدب في قصة البائع في الحقيقة أنه لا يهتم بالسرعة التي يركض بها صديقك، إنه يريد فقط أخذ قضمه منك.

إن السمة المميزة للتهديدات المتطورة المستمرة، هي في فريقه المتناسق من الخبراء المتخصصين، الذي يأخذ كل منهم أدوار مختلفة. كثيراً ما يبدوا الأمر مثل لص "يدرس" بنكاً، أو جاسوسا يراقب قاعدة عسكرية؛ فإن فريق المراقبة يقوم بما يسمى "بإنماء الهدف"، يعرف فيه كل شيء يستطيع عن ذاك الشخص أو المنظمة التي يسعون خلفها مع نقاط الضعف الرئيسة لها. ولهذا الغرض فإن أدوات البحث على الإنترنت وشبكات التواصل الاجتماعي كانتا بمثابة نعمة مرسلة من الله للمعتديين. أتريد سرقة قطعة ما، وتحتاج لمعرفة من هو نائب مدير قطاع الإنتاج؟ في الماضي لكنت بحاجة إرسال جيمس بوند لإغراء موظفة الاستقبال في قسم الموارد البشرية ثم التسلل إلى ملفاتها بينما هي تغط في نوم عميق بعد احتسائها الكحول وقضاء الليلة مع جيمس بوند. أما الآن فالأمر أصبح مملاً، ما عليك سوى كتابة الاسم في محرك بحثٍ على الإنترنت لتجد كل شيء عنه بدأ من السيرة الذاتية لذاك المدير إلى اسم حيوان بنته الأليف "أكواتا". كما أوضح الخبير في مجال الأمن الإلكتروني قري ماك كرو "إن أكثر أداة مدهشة في مجموعة أسلحة المعتدي هي قوقل."

إن هذه هي المرحلة التي يُصنف فيها الهجوم على أنه "مستمر"، فالاستطلاع والإعداد قد يأخذ شهوراً. لا تحاول الفرق فقط فهم تنظيم الهدف ولكن أيضاً الاهتمامات الرئيسية وحتى انتماءاته. فمثلاً، في واحد من الهجمات المتطورة المستمرة على شركة تقنية تقع رئاستها في منيسودا Minnesota، اكتشف أعضاء الفريق أخيراً أن أفضل طريقة لخرق النظام هي الانتظار لحين حدوث عاصفة ثلجية كبيرة. ثم قاموا بإرسال رسائل بريد إلكترونية مزيفة عن تغير الشركة لسياسة يوم العاصفة الثلجية. الكل يعطي شيء مثل ذلك في مينيسودا فإن الكل اهتماماً، من المدير إلى أصغر موظف. وفي محاولة أخرى، فقد القى مسؤولون الأمن القومي الحكومي على المخابرات الصينية والوحدات العسكرية بجمع تفاصيل ليس فقط عن مساعدي وأصدقاء المستهدفين ولكن حتى التعابير التي يستخدموها بينهم للتوقيع على الرسائل الإلكترونية (مثل اتمني لك الأفضل

وتحياتي الحارة واستمر في أداء المهمة) لتقليدها واستخدمها في هجمات الصيد بالرمح "سبير فشنج" Spear phishing.

بعد الفهم التام للهدف يعمل "فريق التدخل" على خرق النظام. ومع ذلك، فإنه من الملاحظ ان الهدف الأولي عادة ليس هو ما يسعون خلفه. الطريقة الفعالة لدخول الشبكة هي عن طريق من هم أهل للثقة خارج الشبكة، والذين عادة لهم مستوي منخفض من الدفاعات. أو عن طريق استهداف أُناس داخل الشبكة لهم صلاحياتٌ للوصول واستخدامها لفتح البوابة. على سبيل المثال، فإن عدد من مراكز الأبحاث الأمريكية (والتي ضمت مكان عملنا) تم استهدافها عام 2011 ومجدداً في عام 2012 عن طريق تهديد متطور مستمر، والذي سعى للوصول لحسابات الباحثين الذين عملوا بقضايا الأمن الاسيوي. لم يكونوا مهتمين فقط بملفاتهم، ولكن أيضاً بدفاتر عناوينهم التي حوت معلومات اتصال لقيادات كبيرة في الحكومة. لكن التهديد المتطور المستمر سعى أولا خلف الموظفين الذين لهم صلاحياتٌ إدارية ووصول لكلمات السر.

كثيرا ما يستخدم هؤلاء المعتدين الصيد بالرمح "سبير فشينج" (Spear Phishing) ورسائل البريد الإلكترونية المزيفة، مع بعض الاستغلال المخفي داخل ملفات أو برامج ضارة يتم تحميلها. في عملية الفار المشبوه (التي هي تهديد متطور مستمر سنتحدث عنه لاحقا في القسم الثاني). عندما يتم فتح الملف المرفق مع البريد الإلكتروني المزيف عندها تتم زراعة البرنامج الضار. والتي عندها يتم صناعة باب خلفي للتواصل مع خادم انترنت خارجي والذي بدورة تم الاستحواذ عليه بتعليمات مخفية في الكود البرمجي لصفحة الإنترنت. وذاك مجهود من المعتدي لإخفاء أثاره.

إن البرنامج الضار المستخدم في تلك الملفات المرفقة عادة ما يكون في غاية التعقيد، وينصب التركيز على التخفي، لذا لا يحاول صانعي البرامج فقط التخفي من الدفاعات التقليدية لمضادات الفايروسات ولكن

الاختباء عميقا في الشبكات وفي نظم التشغيل لتفادي الاكتشاف، في محاولة للتحايل على حركة البيانات في الشبكة بطريقة شرعية غير مشكوك بها. وكما هو الحال في الأعمال التجارية الأخرى فإن المجموعات التي تقوم بالتهديدات المتطورة المستمرة عادة ما تقوم بإجراء تجارب وحتى اختبارات لتأكيد الجودة للتقليل من عدد البرامج المضادة للفيروسات التي تستطيع تحديدهم. ولكن البريد الإلكتروني ليس هو السبيل الوحيد للوصول، فعلى سبيل المثال، استخدمت تهديدات متطورة مستمرة أخرى شبكات التواصل الاجتماعي مثل فيس بوك، لإجاد أصدقاء أفراد ذوي مستوى عالي داخل الشبكة المستهدفة، ثم الاستحواذ على الرسائل الفورية لذاك الصديق للتسلل داخل الشبكة. وربما أكثر مثال مثير للاهتمام على استخدام وسائل شبكات التواصل الاجتماعي، هو عندما تم خداع كبار الضباط البريطانيين ومسؤولين الدفاع بقبول طلبات صداقة من حساب مزيف بالفيس بوك تحت اسم الأدميرال جيمس استيفرسن قائد قوات منظمة حلف شمال الأطلسي. من قد لا يرغب بأدميرال كصديق؟، ولكن تخيل خيبة أملهم عندما اكتشفوا أنه مخترق.

حالما يصبح الفريق بالداخل فإنهم ينتشرون كالعدوى الفيروسية، ذلك عادة مع انضمام المزيد من الافراد للمهمة. يتحركون من نقاط الارتكاز الأولية والاستحواذ على مزيد من الآلات داخل الشبكة التي تستطيع تشغيل البرنامج الضار، ومن ثم استخدامها للدخول والخروج. عادة ما يتضمن هذا تنصيب برنامج لرصد لوحة المفاتيح الذي يستطيع تتبع ما يقوم الناس بطباعته. وبرنامج امر وتحكم الذي يستطيع توجيه الكود البرمجي الضار للبحث عن المعلومات الحساسة.

تم الاستحواذ على الهدف في هذه المرحلة "بيوند" (pwend)، وأنه الآن تحت رحمة المعتدين. ويقوم "فريق التسلل" بالعمل علي جلب المعلومات التي استهدفتها التهديدات المتطورة المستمرة طيلة تلك الفترة. وهنا سمة مميزة أخرى للتهديدات المتطورة المستمرة وهي بدلاً من المعتقد العام للمجرمين في أخذ كل ما

تستطيع أخذه، فإنهم يسعون خلف ملفات محددة جداً. وكثيرا ما لا يفتح المعتدين تلك الملفات، باعتقادهم أن الاستطلاع الذي قاموا به كاف تماماً لدرجة أنهم لا يحتاجون لمراجعة ما استهدفوه. وبالمقابل فإن شخصا ما يضع قائمة محددة لما يجب جمعة، وان الفريق منضبطا كفاية للالتزام بها.

ليست كل التهديدات المتطورة المستمرة تقوم فقط بنسخ البيانات ثم الخروج. فالبعض يقوم بإضافة تكنلوجيا تمكنهم من سرقة أسرار خارج ما كان موجود داخل الشبكة أو حتى الاستحواذ على التحكم. على سبيل المثال فقد القى مسؤولون فرنسيون اللوم على تهديدات متطورة مستمرة مرتبطة بالمخابرات الصينية، في التمكن من الوصول لحواسيب قادة تجاريين وسياسيين فرنسين عالين المستوى. ومن ثم تفعيل الميكروفونات والكاميرات لاستراق السمع على المحادثات. وحتى أن هناك ما هو أشنع في أفعال هؤلاء الذين لا يكتفون بسرقة البينات فقط ولكن يغيرون في الملفات. والذي كما سنستعرضه لاحقا سيكون له عواقب كبيرة. هذا يغير التهديدات المتطورة المستمرة كلياً من كونها فعلاً اجرامياً أو تجسساً لتصبح أفعال تخريب أو حتى حرب.

في مرحلة الهروب، وعندما تغادر كميات من البيانات الشبكة (مثل خروج ملف بريد الكتروني كامل) وقتها يتم كشف العديد من التهديدات المتطورة المستمرة الناجحة. ينتج من مرحلة الاتصال بالقاعدة حركة بيانات غير انتظامية في الشبكة يصعب التغطية عليها.

ولذلك تسعي فرق الهروب لاستخدام كل أنواع الخدع لتسريب البيانات خارج الشبكة وثم تغطية أثارهم. تضمن واحدة من التكتيكات الشائعة توجيه البيانات خلال محطات في بلدان متعددة. وذلك قريبا مما يفعلونه من يغسلون الأموال المسروقة، بتمريرها خلال بنوكا من كل انحاء العالم. لا يجعل هذا من تقفى أثارهم أمراً صعباً وحسب، ولكن أيضاً يجول بناشطي التهديدات المتطورة المستمرة خلال بلدان ونظم قانونية مختلفة، والذي يُعقّد في نهاية المطاف محاكمتهم.

والذي يجعل من التهديدات المتطورة المستمرة أكثر تهديدا، هو عندما تعلم الضحية أخيراً أنه تم الهجوم عليها، فإن الألم لم ينته بعد. إيجاد أي من الماكينات داخل النظام تمت اصابتها قد يستغرق شهوراً. هناك ما هو اسوأ، إذا كانت المحاولة حقاً مستمرة. لنقل إذا ما كانت الضحية لها قيمة مستمرة للمعتدى، فقد تكون هناك وحدة إضافية في التهديدات المتطورة المستمرة والتي وظيفتها بالتحديد هي الحفاظ على نقطة ارتكاز الكترونية في الشبكة. ولكن بدلاً من التركيز على ماهية البيانات التي ستسرق، فإن هذه الوحدة ستراقب الرسائل الإلكترونية الداخلية لمعرفة الطريقة التي يحاول بها المدافعون إخراجهم بها. في واحدة من الحوادث، تعاقدت شركة أمريكية مع شركة تابعة لوزارة الدفاع متخصصة في أمن الحاسوب. لتطهير شبكتها المصابة بعد ما تم استهدافها بواسطة تهديد متطور مستمر. على الرغم من ذلك، وبعد عدة شهور، تم القبض على منظم حرارة وطابعة في مبناهم وهي تقوم بإرسال رسائل لخادم إنترنت في الصين. وبما أن اتصالاتهم الإلكترونية تم الاستحواذ عليها، فإن ردة فعل المدافعين هي غالبا الرد بالطريقة القديمة. فإنهم سيقومون حرفيا بتحطيم الأقراص الصلبة في حواسيبهم ومن ثم نشر منشورات بخط اليد على الممرات حول سياسة تغير كلمات السر.

تعتبر التهديدات المتطورة المستمرة بمثابة سيناريو كابوس لأي منظمة. فأغلبهم لا يدري بأنه تم استهدافه حتى فوات الأوان. وحتى وإن استطاعوا معرفة ذلك، فمن المستحيل غالبا اثبات من كان خلفه. وذلك في الحقيقة ما يجعل من التهديدات المتطورة المستمرة من أكثر النواقل للتهديدات المثيرة للجدل. ماعدا في حالات يكون فيها المعتدين مهملين لحد ما، (إن مثالنا المفضل هو عندما استخدم ضابط برتبة عالية في الجيش الصيني نفس خادم الإنترنت للتواصل مع معشوقة له، ومن ثم تنظيم تهديد متطور مستمر). هناك القليل من الدليل الفعلي قد يستحضر في المحكمة أو أن يزحزح موقف بلد. والذي نُترك معه عادة هو الشك

وتوجيه أصابع الاتهام، وذاك الذي يجعل من التهديدات المتطورة المستمرة سُماً يهدد العلاقات الدبلوماسية. وكما رأينا في السنوات القليلة المنصرمة ما بين الولايات المتحدة والصين.

كيف نبعد الأشرار؟ أساسيات الدفاع الإلكتروني:

هي حتى الآن أكبر حديقة حيوان في العالم. في عام 2013 قد حوت أكثر من مائة وعشرة مليون نوعا مختلفا تم جمعها بعناية من الطبيعة، ومع ذلك فإنها نوع غريب من حدائق الحيوان. فيها قد لا ترى الحيوانات حقيقة، والسبب أنهم موجودون في العالم الافتراضي.

حديقة البرامج الضارة التابعة لمكافي McAfee أو هذا ما تسميه شركة أمن الحاسوب لمجموعتها من الأنواع المختلفة من البرامج الضارة والمؤذية (مالوير). التي صممت لتعيث فساداً على مستخدمي الإنترنت. إن نموها يوضح حجم نطاق المشكلة التي لا يمكن التغلب عليها فيما يبدو. في عام 2010 ظنت "مكافي" أنه من المدهش اكتشافها عينة جديدة من البرامج الضارة كل 15 دقيقة. في عام 2013 كانت تكتشف واحدة في كل ثانية.

إذا فكرنا في كل نوع من البرامج الضارة على أنه تهديد فريد، فإن تلك الأرقام تصبح ساحقة. وبالمقابل فعلينا فهم لماذا هناك عدد كبير من التهديدات الفريدة؟، تنعكس الإجابة في لعبة القط والفأر التي يلعبها المعتدين والمدافعين. منذ بدايات الإنترنت حاول المعتدين استغلال نقاط الضعف وسعي المدافعين لمنعهم. يتبنى الخصوم أنماط هجوم ويغيرون فيها، وبالتالي تتغير لتصبح لعبة متطورة.

إن ميزة الدفاع عن نظام حاسوب، تكمن في أنه حالما تعرف ماذا يمكن أن يهاجمك، يمكنك فقط إخبار الحاسوب عما الذي يمكن أن يهاجمه والطريقة التي يمكنه تجنبه بها. تعتمد البرامج التقليدية المضادة

للفيروسات على تحديد هذه العلامات المميزة للفيروس "سقنتشرز" (Signatures). يبحث البرنامج كل ملفات النظام وأيضاً حركة البيانات القادمة مع قاموس للبرامج الضارة المعروفة، باحثاً عن أي شيء قد يتطابق من تلك العلامات التخريبية المميزة للفيروس.

هذه الطريقة التقليدية لها بعض العيوب الصارخة. في الوقت التي تزداد عدد الهجمات فيه، تزداد معها تلك الملفات المُعرفة والزمن الذي تحتاجه للبحث فيها. اغلب هذه العلامات المميزة للفيروسات القديمة لا تمثل تهديدات حالية. ومع تكاثر التهديدات يصبح الأمر لعبة خاسرة. أوجدت دراسة أن 0.34 بالمئة من العلامات المميزة للفيروسات في البرامج المضادة للفيروسات الشائعة هو ما كان لازما لإيجاد كل البرامج الضارة الموجودة في كل رسائل البريد الإلكتروني الواردة. ومع ذلك فإن الحيطة والحذر تقضي منا التزام بالبحث فيما بقي من 99.66 بالمئة من تلك البرامج الضارة. وذلك في حالة تلاعب المعتدي ورجوعه إليهم.

إن المشكلة الكبرى تكمن في التطور. صارع صانعوا البرامج الضارة ضد طريقة مضادات الفيروسات التقليدية، عن طريق اخذهم درساً في علم الاحياء. وذلك مثل بعض الفيروسات مثل الإيدز والأنفلونزا التي تغير شكلها الخارجي البروتيني لتفادي تحديدها من قبل نظام المناعة البشري. فإن صانعي البرامج الضارة يغيرون من الشكل الخارجي لبرامجهم المهاجمة. يمكن للهجوم نفسه أن يُصنع بعدة آثار مميزة، متنكرة ببرامج تخلق ميزاتٍ الياً. هذا يزيد في العدد الضخم. مثل التي عكستها احصائيات حديقة الحيوان المذكورة أعلاه، ويجعل الطريقة القديمة للتحديد بواسطة العلامات المميزة للفيروسات اقل فائدة. أوجد تحليل لفترة ثمانية أيام، أنه بينما تمت إضافة مائة ألف من العلامات المميزة لفيروسات جديدة ضارةٍ معروفةٍ بواسطة كبرى الشركات المقدمة لخدمات الحماية من الفيروسات إلى قائمة ما يجب البحث عنه، فكانت الحصيلة اثني عشر تحديداً جديداً فقط. إن اثني عشر تحديداً من بين مائة ألف من العلامات المميزة للفيروسات تمت معالجتها، قد يبدو

الرقم ضئيلاً جداً. ولكن هذا يعكس تقنيات التمويه المستخدمة من قبل صانعي البرامج الضارة، أكثر من عدم نجاح شركات الحماية منها من الجهة الأخرى. إن تضخم عدد العلامات المميزة للفيروسات قد يجعل من مشكلة البرامج الضارة أن تبدوا أكبر مما هي عليه. ولكن سيكون من الخطأ أيضاً استنتاج أن البرامج الضارة ليست مشكلة على الإطلاق.

ولذا كان على شركات الأمن تغير الطريقة التي تحدد بها الكود البرمجي الضار. مضادات الفيروسات الحديثة لا تقوم فقط بالبحث، بل أنها تستخدم تحديدات إرشادية لمعرفة أداء كود برمجي للحاسوب مشبوه، بناء على قواعد وقوانين وتحليل منطقي. يقسم التحليل الإحصائي كود الحاسوب لأجزاء ومن ثم البحث عن نمط مرتبط مع تصرفات معتديٍ. إن الآلات الافتراضية والدفاعات الأخرى المعقدةِ تقوم بمحاكةٍ ديناميكيةٍ لتشغيل الكود البرمجي، لتحديد ما إذا كان الملف الذي تم فحصة سوف يسيء التصرف، وذلك بدون وضع النظام الحقيقي في خطر. وذلك مثل فرق الشرطة للكشف عن المتفجرات وهي تتفحص الطرود المشبوه. إن غرف التفجير الافتراضية قد تجعل الجزء من البرنامج الضار يعتقد مخطأً أنه في داخل الآلة لينفجر قبل أوانه.

إذا كان تامين نظام تشغيل حديث أمراً صعباً، فهناك طريقة أخرى تحاول منع الأشياء السيئة من الوصول إلى الحاسوب عبر الشبكة. إن أبسط شكلٍ لدفاع الشبكة هو جدار النار. مأخوذ من مفهوم الحواجز التي تُضرب على السيارات والأبنية لمنع النيران من الانتشار. جدران النار بالنسبة للحاسوب هي مثل المرشحات، التي ترفض حركة بينات على أساس قواعد محددة. تستطيع جدران النار منع حواسيب خارجية من التوصيل بالآلات التي ضرب عليها جدار النار، ماعدا تحت ظروف أُعدت مسبقا. أو منع تطبيقات معينة في الحاسوب من فتح اتصالات على الشبكة.

إن جدران النار هي مرشحات تسمح بالنشاط المشروع فقط على الشبكة. وأن الطبقة التالية من الدفاعات هي مجموعة من الحساسات التي تبحث عن تصرفات غير مشروعة. "أنظمة كشف التطفل" موجودة على مستوي الحاسوب أو الشبكة. تكشف تلك الأنظمة عن توقيعات (Signatures) الهجوم، والتعرف على التصرف الغريب ("إن القائم على بوابة الحاسوب عادة لا يفتح اتصالاً مشفراً مع مولدوفا في الثانية صباحاً"). تُحذر هذه الأنظمة الإداريين من هجمات محتملة، وتقوم بحفظ سجل تحليل شرعي مفصل. لدا معظم أنظمة الكشف الان بعض القدرة أيضاً لمنع التطفل. حيث تقوم بإغلاق اتصالات الشبكة المشبوه وابعاد حركة البينات الغريبة بعيداً. مثل البرامج المضادة للفيروسات، فهذه الأنظمة تأتي مع ثمن، بالإضافة إلى زيادة التكلفة فإنها تُكلف الوقت واستهلاك موارد الآلة، خاصة إذا ما أُضر النظام لمعاينة كل حركة البيانات القادمة على شبكة كبيرة في وقت حقيقي.

سمعت سابقا عن اليوم رقم صفر الذي يكون بعد اكتشاف نقطة ضعف جديدة. فإن اغلب الهجمات تحاول استغلال نقاط الضعف التي تم اكتشافها مسبقا بواسطة من يقدمون خدمات الحماية. ومحاولتهم تصليحها بواسطة تحديث في الكود البرمجي، أو عن طريق "برنامجٍ للتصحيح". إن وجود برنامج تصحيحي يشير على أن المقدم للحماية قد وجد نقطة ضعف ويريد التخفيف من تهديد تم التعرف عليه. وربما الأكثر أهمية هو الإصلاح البنائي في الكود برمجي الموجود.

تكمن المشكلة في أن العديد من المستخدمين دائماً مالا يراعون الانتباه لتلك التحديثات الأمنية ويتركون نقاط الضعف غير مصلحة. ولذلك فقد رأينا التطور من المنشئين وهم يرسلون إشعارات بسيطة لتحديثات جديدة والتي تضع عبء التنفيذ على جزء المستخدم، إلى تنزيلات أتوماتيكية أو حتى تثبيت لذاك الإصلاح. ولكن جاءت تكاليف أخرى مع ذاك التحويل، إن البرامج الحديثة معقدة جداً، وإصلاح نقطة ضعف صغيرة واحدة قد

يؤثر في عمليات للبرنامج لا حصر لها. قصص رعب تصف تصليحات حولت هواتف ذكية جديدة كليا لتصبح ثقالة ورق أنيقة. أو تخريب شبكات مؤسسة بأكملها. طالما أن كل منظمة كبيرة تشغل برنامج مختلفا، ولديها إعدادات مختلفة، فإن إدارة التصليحات هي جزء مهم لأي قسم دعم تقني.

وكما هو الامر في أن دفاعات جسمك ليست فقط على حد الجلد، فإن تهديدات خطيرة يتم التصدي لها ليس فقط بحفظها خارجا. هناك إجراءات لحماية ما هو مهم حتى إذا تمكنت التهديدات من الدخول. في حالة التجسس الإلكتروني إذا لم تستطع منع المعتدين من الوصول إلى البيانات فيمكنك حصر قدرتهم على فهم البيانات عن طريق التشفير.

إن خط الدفاع الأخير شبيه بالاستراتيجية التي تستخدمها الراهبات لحراسة حفلات الرقص في المدرسة الكاثوليكية. عادة ما تقوم الراهبات بوضع بالونات بين المراهقين الذين يرقصون قريبا من بعض، لخلق فجوة هواء لتأكد من عدم حدوث أي شيء. في مصطلحات الأمن الإلكتروني فإن فجوة الهواء هي تفريق حقيقي بين الشبكة والأنظمة الحساسة، ممارسة مثل تلك هي شائعة في البنى التحتية الحساسة، مثل التي في شركات الطاقة. والتي حاولها الإيرانيون لحماية بحوثهم النووية من هجوم الإلكتروني.

إن مشكلة فجوات الهواء تشبه إلى حد كبير التقشف الذي تحاول الراهبات فرضة، والذي غالباً لا ينجح عند التنفيذ. إن التخلي عن الضوابط التشغيلية للبنية التحتية ينطوي على تضحيات في الكفاءة والفعالية. إن شركات الطاقة المعزولة مثلاً، قد تكون لها نقاط ضعف أقل. ولكنهم لا يستطيعون تشغيل شبكات كهرباء ذكية تحفظ المال وتحافظ على البيئة.

على حد سواء، فإن الحفاظ على فجوة هواء غالباً أنه أمرٌ غير حقيقي. كما اكتشف الإيرانيون أن انظمتهم التي يفترض بها أن تكون معزولة بفجوة هواء ومع ذلك فقد أصيبت بفيروس ستكسنت. في نقطة

معينة، فعلي البيانات القديمة أن تخرج، وتعليمات جديدة تحتاج أن تدخل. والأنظمة تحتاج لإصلاح وتحديث وصيانة. في الواقع فإن المركز القومي للأمن الإلكتروني ودمج الاتصالات، قد أجرى المئات من التقييمات لنقاط الضعف في القطاع التجاري الخاص الأمريكي في محاولات لعزلة بفجوة هواء. وأنها لم تجد ولو مرة واحدة شبكة تعمل بنجاح وهي منفصلة عن شبكات حواسيب المؤسسة الأخرى.

في النهاية فإن أحدهم قد أيد الشعار القديم الذي يقول "إن أفضل دفاع هو دفاع جيد". في العالم الإلكتروني هذا ما يعرف بـ "رد الاختراق". وأن عدد من الشركات قد أظهرت النية بالسعي خلف شبكات حاسوب المعتدي الخاصة. مثل الاقتصاص غير القانوني، قد يشعرك بشعور جيد وقد يعلم المعتدي الأصلي درساً.

إن العمل على رد اختراق له مشكلتان رئيسيتان، الأولى، هي عدم اتضاح من له الحق في تنفيذ هجمات الإلكترونية، وهذا يعني أن الشركات التي تقوم بالهجمات الإلكترونية أنها "تتزلج على ثلج هش" قانونيا. أو كما قال نيت فيك مدير شركة "إندقيم" Endgame للأمن الإلكتروني. أما الثانية، فإنه ليس من الواضح أيضاً أن رد الاختراق قد يؤثر على مدى طويل، وكما أوضح هارفي الذ هو استراتيجي للأمن يعمل في شركة "فورتنت" Fortinet، "أنه ليس من الصعب اختراقهم واغلاقهم، ولكن واحد جديدا سيظهر وستنعم بعدة دقائق من السلام والهدوء".

إن خلاصة الأمر فيما يختص بالدفاع الإلكتروني هو أنه عمل شاق. مع عدة خيارات هي بعيدة من أن تكون مثالية. ولكن الخيار الأخر الوحيد هو إغلاق حديقة الحيوان وإطلاق سراح البرامج الضارة.

ما هو الرابط الأضعف؟ العوامل البشرية:

في عام 2008 كان هناك جندي أمريكي يعبر موقفٌ للسيارات خارج قاعدة جيش أمريكية في الشرق الأوسط، عندما لاحظ قطعة حلوى غير مفتوحة مرمية على الأرض، ومن دون أن يعرف من تركها وكم من الزمن هي على الأرض، فقد قرر اخذها داخل القاعدة واكلها على الغداء.

قد يبدو ذلك غريباً وحتى مقززاً بعض الشيء، اليس كذلك؟ فالتبدل وحدة تخزين "يو اس بي" محل قطعة الحلوى وستتكون لك القصة عما بدأ "بكشوت يانكي" Buckshot Yankee واحدٌ من أكبر الاختراقات الإلكترونية في تاريخ الجيش الأمريكي. في عام 2008 تركت وكالة استخبارات أجنبية وحدات تخزين "يو اس بي" صغيرة في موقف السيارات خارج قاعدة أمريكية، ذاك نهج معروف بـ "إيقاع الحلوى". رأى جنديٌ واحدةً من تلك القطع في التراب وفكر بانها فكرة جيدة ايصالها بحاسوب في شبكة القيادة للجيش الأمريكي. قامت وحدة التخزين تلك بتحميل دودة معروفة بـ "ايجنت.بي تي زت" Agent.btz التي بحثت في الحواسيب عن البيانات وانشأت أبوب خلفية، وربطت بخوادم قيادة وسيطرة. أمضت وزارة الدفاع الأربعة عشر شهر التالية في التطهير من تلك الدودة، وكل ذلك بسبب أن جنديا واحدا لم يكن له حس بديهي لتطبيق "قاعدة الخمس ثواني" في كيفية التعامل مع حاسوبه.

إن المعركة الحقيقة في الأمن الإلكتروني ليست فقط عن التقنيات العالية. إنها أيضاً مُسيرةٌ بالعامل البشري، الصراع حول تصرفاتنا. إن التورية من الحروب القديمة، في انه لا يجب دائما تحطيم الجدران التي تحمي الشبكة أو حفر نفق تحتها بواسطة معتدي. في بعض الأحيان كما صار في قصة حصان طروادة "تروي" (Troy) القديمة، قام الحراس الغافلون بفتح البوابات بدون ملاحظة تخفي العدو. في الوقت الذي توجد فيه العديد من التهديدات المتطورة للأمن الإلكتروني، فالكثير من التهديدات الأكثر نجاحا تستغل الخطاء

البشري الساذج القديم. الأمثلة تتراوح بين تنفيذي في شركة تقنية معلومات، الذي وجد قرصاً صلباً "سي دي" به برنامج ضار (مالوير) في حمام الرجال، أخذه وأدخله في حاسوبه ليرى محتواه (مرة أخرى، فكر في المقارنات: هل ستلتقط مشطا وجدته في مرحاض؟ أو ساندويتش؟) إلى موظف في شركة لوزارة الدفاع، الذي كان يستخدم شبكة عمله لمشاركة ملفات موسيقى. بجانب مشاركة ما يملك من أغاني الروك على الإنترنت، شارك بدون قصد منه التصاميم الإلكترونية للطائرة المروحية الرئاسية الامريكية مع مخترق إيراني.

ولهذا السبب يعتقد العديد من خبراء تقنية المعلومات أنه إذا ما حوت الشبكة على أي نوع من المعلومات السرية فيها، فعلى كل المستخدمين أخذ دورات منتظمة في أساسيات الأمن الإلكتروني. هذا يعني الكل، من أصغر طاقم إلى القيادة العليا. ليس هذا فقط عن التطبيق الجبري لقاعدة الخمس ثواني للأشياء التي توصلها بحاسوبك. يستغل المعتدون الاذكياء فطرة الثقة البشرية لإقناعنا بالضغط على روابط وفتح ملفات مرفقة أو حتى إعطاء كلمات سرنا لغرباء عبر الهاتف. بما ان 99% من الوقت الذي لا تكون فيه اتصالاتنا الهاتفية ورسائلنا الإلكترونية غير ضارة، فمن الصعب ان تكون يقظا دائما.

حتى الخبراء يمكن تغفيلهم. إن البروفسير جون سافيج الذي أوجد قسم علوم الحاسوب بجامعة برأون عام 1979، والذي كرس جزءا كبيرا من حياته المهنية المتميزة في دراسة أمن المعلومات، بما في ذلك تقديم المشورة لوزارة الخارجية. ومع ذلك واثناء درس في أمن الحاسوب، فقد نجح أحد تلاميذه بخداعة لضغط رابط على رسالة بريد الكتروني وقام بإدخال كلمة سره. (قمنا لاحقاً بتعين نفس ذاك التلميذ كمساعد في البحث لأجل هذا الكتاب.)

سنتوغل أكثر في هذا في الجزء الثالث، ولكن الهدف هو التعرف على الدور الرئيسي الذي تلعبه التصرفات البشرية في تفعيل التهديدات، ومن ثم بناء وعى مستمر نرسخه بتدريب جديد. إذا ما فشل المستخدمون

في تعلم دروس الحذر الملائم، عندها يجب إلغاء امتيازات وصولهم. في الحقيقة، فإن بعض الشركات مثل "لوكهيد مارتن" Lockheed Martin لديها برامج "فريق احمر" والتي من الحين للآخر يحاول خداع موظفيها. إذا ما فتح موظف رابط في رسالة بريد الكتروني مشبوهة، مثلا، فإنها تحيل الفاعل إلى دورة إضافية في الأمن الإلكتروني. ولكن من الأفضل تعلم الدروس بهذه الطريقة بدلاً من تحميل برنامج مالوير ضار حقيقي أو أحصنة طروادة أو أي من الهدايا الإلكترونية الأخرى المنقولة من حضارة اليونان.

الملحق

الاختصارات

Advanced Persistent Threat (APT)"أي بي تي"

التهديد المتطور المستمر

Advanced Research Projects Agency (ARPA) "أربا"

وكالة مشاريع البحوث المتقدمة

Advanced Research Projects Agency Network (ARPANET) "أربانت"

شبكة وكالة مشاريع البحوث المتقدمة

Autonomous System (AS) "اى إس"

أنظمة التحكم الذاتي

Certificate Authority (CA) "سي أى"

سلطة الشهادات

Distributed Denial of Service (DDoS) "دوز"

نشر رفض الخدمة

Domain Name System (DNS) "دي إن إس"

نظام اسماء النطاقات

HyperText Transfer Protocol (HTTP) "اتش تي تي بي"

برتوكول نقل النصوص المتشعبة

Internet Corporation for Assigent Names and Numbers (ICANN) "أي سي اى إن إن"

مؤسسة الإنترنت لإسناد الأسماء والأرقام

Internet Engineering Task Force (IETF) ‘‘أي إي تي إف’’

فريق عمل مهندسي الإنترنت

Internet Protocol (IP) ‘‘أي بي’’

بروتوكول الإنترنت

Internet Service Provider (ISP) ‘‘أي إس بي’’

مزود خدمة الإنترنت

Internet Society (ISOC) ‘‘أي إس أو سي’’

مجتمع الإنترنت

National Security Agency (NSA) ‘‘إن إس اي’’

وكالة الأمن القومي

Structured Query Language (SQL) ‘‘إس كيو إل’’

لغة الاستعلام الهيكلي

Supervisory Control and Data Acquisition (SCADA) ‘‘إسكادا’’

التحكم الإشرافي وجمع المعلومات

Transport Control Protocol (TCP) ‘‘تي سي بي’’

بروتكول التحكم في النقل

CYBERSECURITY AND CYBERWAR

WHAT EVERYONE NEEDS TO KNOW®

P. W. SINGER AND
ALLAN FRIEDMAN

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Oxford is a registered trademark of Oxford University Press
in the UK and certain other countries.

"What Everyone Needs to Know" is a registered trademark of Oxford
University Press.

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016

Library of Congress Cataloging-in-Publication Data
Singer, P. W. (Peter Warren)
Cybersecurity and cyberwar : what everyone needs to know / Peter W. Singer,
Allan Friedman.
ISBN 978–0–19–991809–6 (hardback)—ISBN 978–0–19–991811–9 (paperback)
1. Computer security—United States 2. Computer networks—Security
measures—United States. 3. Cyberspace—Security measures—United States.
4. Cyberterrorism—United States—Prevention. 5. Information warfare—United
States—Prevention. I. Title.
QA76.9.A25S562 2014
005.8—dc23
2013028127

1 3 5 7 9 8 6 4 2
Printed in the United States of America
on acid-free paper