تهديدات مجهولة المصدر

نحو مساءلة دولية في الفضاء الإلكتروني

جون إس. ديفيس الثاني (John S. Davis II)
بنجامين بودرو (Benjamin Boudreaux)
جوناثان ويليام ويلبورن
(Jonathan William Welburn)
جاير أغيري (Jair Aguirre)
كورداي أوغليتري (Cordaye Ogletree)
جوفري ماكغوفرن (Geoffrey McGovern)
مايكل إس. تشايس (Michael S. Chase)

RAND CORPORATION

تهديدات
مجهولة المصدر

نحو مساءلة دولية في الفضاء الإلكتروني

جون إس. ديفيس الثاني (John S. Davis II)
بنجامين بودرو (Benjamin Boudreaux)
جوناثان ويليام ويلبورن (Jonathan William Welburn)
جاير أغيري (Jair Aguirre)
كورداي أوغليتري (Cordaye Ogletree)
جوفري ماكغوفرن (Geoffrey McGovern)
مايكل إس. تشايس (Michael S. Chase)

تم هذا البحث تحت رعاية مؤسسة ميكروسفت

للحصول على مزيدٍ من المعلومات حول هذا المنشور، الرجاء زيارة الموقع الإلكتروني التالي:
www.rand.org/t/RR2081

البيانات الفهرسية الخاصة بهذا المنشور متوفرة في مكتبة الكونغرس
تحت الرقم المعياري الدولي للكتاب، كالتالي:
(ISBN): 978-0-8330-9840-5

نشرته مؤسسة RAND، سانتا مونيكا، كاليفورنيا

Cover graphic: erhui1979/GettyImages
صورة الغلاف: erhui1979/GettyImages

www.rand.org

المحتويات

قائمة بالأشكال والجداول ودراسات الحالة

الأشكال

الجداول

دراسات الحالة

حول هذه الدراسة

يتمثل تحديد مصدر الحادث الإلكتروني الخبيث في تحديد الجهة المسؤولة عن هذا النشاط. وتشكّل نتيجة تحديد مصدر الهجمات الإلكترونية شرطًا أساسيًا لمحاسبة الجهة الفاعلة على النشاط الخبيث. وقد حظيت في الآونة الأخيرة حوادث إلكترونية متعددة ذات تبعات جغرافية سياسية ونتائج تحديد المصدر المرتبطة بهذه الحوادث بتغطية صحافية بارزة. وقد عارضت شرائح متعددة من الرأي العام المصادر المُعلن عنها وشكّكت في موثوقيتها. ونستعرض في هذه الدراسة وضع تحديد مصدر الهجمات الإلكترونية وننظر في الآليات البديلة من أجل التوصّل إلى عملية موحّدة وشفافة لتحديد المصدر قادرة على تجاوز المخاوف المتعلقة بالموثوقية. وتتناول هذه الدراسة الاستطلاعية على وجه الخصوص القيمة التي تضطلع بها منظمة عالمية مستقلة تتمثّل مهمتها في التحقيق في الهجمات الإلكترونية الكبرى وتحديد مصدرها علنًا.

ويودّ المؤلفون التقدم بجزيل الشكر لهيرب لين (Herb Lin) وأيزاك بورش (Isaac Porche) ومارتن ليبيكي (Martin Libicki) على نقدهم الرسمي لمسودة سابقة من هذه الدراسة.

النتائج الرئيسية

يشير تحليل الحالات الأخيرة إلى انتشار ممارسة تحديد مصدر الهجمات على نحو متباين. ويعود ذلك إلى غياب منهجية موحّدة تُستخدم في التحقيقات لتقييم الأدلة وغياب مقياس موثوقية عالمي للتوصل إلى نتيجة.

وقد أُجريت تحقيقات في حالات كثيرة ولكن بدون أن تعلن وحدة التحقيقات أو الضحية عن أي نتيجة رسمية لتحديد المصدر. بالإضافة إلى ذلك، قوبلت البيانات العلنية عن تحديد المصدر بالريبة والارتباك والمطالبة بشفافية أكبر بشأن التحقيق والأدلة التي يستند إليها.

ويكمن التحدي الرئيسي عند تحديد مصدر الهجمات الإلكترونية في صعوبة التوصّل إلى نتيجة بشأن المصدر. وتشكّل المؤشّرات التقنية والسياسية ومؤشرات المصادر كافة أدواتٍ يتم اللجوء إليها عند تحديد مصدر الهجمات وتُستخدم عادةً ضمن مجموعات معيّنة.

ويتعلّق التحدّي الآخر عند تحديد مصدر الهجمات الإلكترونية بمسألة نقل النتائج على نحو مقنع إلى الجمهور المستهدف. وتتوقّف الموثوقية على عوامل متعددة وهي: الأدلة الدامغة وإظهار المعرفة والمهارات اللازمة للتوصّل إلى الاستنتاج الصحيح وسجلّ حافل بالعناية والدقة وسمعة جيدة في التحليل الموضوعي والنزيه ومنهجية شفافة تشمل عملية مراجعة مستقلة.

وستعكس التحقيقات الفعّالة المتعلقة بتحديد مصدر الجرائم الإلكترونية هذه الاعتبارات وستحقق الموثوقية في نظر الجمهور المستهدف.

وقد استفاد التحليل بشكل كبير من النقاشات غير الرسمية مع عدد من الباحثين والعاملين في مجال الأمن الإلكتروني.

وقد رعت مؤسسة ميكروسفت (Microsoft Corporation) هذا البحث وطلبت من مؤسسة RAND تقييم مؤهلات المنظمة وتحدياتها المحتملة لتولّي تحديد مصدر الهجمات الإلكترونية ولدراسة إنشاء منظمة مماثلة. وأُجري هذا البحث في مركز سياسات الدفاع والأمن الدولي (International Security and Defense Policy Center) التابع لمعهد أبحاث RAND للدفاع الوطني ((RAND National Security Research Division (NSRD)). ويُجري معهد أبحاث RAND للدفاع الوطني أبحاثًا وتحليلات تتعلّق بشؤون الدفاع والأمن القومي لمصلحة الولايات المتحدة والتحالف الدفاعي والسياسات الخارجية والأمن القومي وأجهزة الاستخبارات ومؤسساتها وسواها من المؤسسات والمنظمات غير الحكومية التي تُعنى بتحليل الشؤون المتعلّقة بالدفاع والأمن القومي.

للحصول على معلومات إضافية حول مركز سياسات الدفاع والأمن الدولي التابع لمؤسسة RAND، يمكنك زيارة الموقع الإلكتروني http://www.rand.org/nsrd/ndri/centers/isdp أو الاتصال بالمدير (تتوفر بيانات الاتصال على صفحة الموقع الإلكتروني).

المقدمة

تزداد مخاطر الحوادث الأمنية الإلكترونية ذات التبعات الجغرافية السياسية التي تشكّل تهديدًا محتملًا على السلامة والأمن والرفاه الاقتصادي. وتشمل الأمثلة الأخيرة الجديرة بالذكر الهجوم على شبكة الكهرباء الأوكرانية (فريق الاستجابة للطوارئ الإلكترونية لنظم التحكّم الصناعية Industrial Control Systems Cyber Emergency Response Team)، 2016) ودودة ستوكسنت (Stuxnet) التي استهدفت منشأة إيرانية لتخصيب اليورانيوم (زيتير (Zetter)، 2014a) واختراق المكتب الأمريكي لإدارة شؤون الموظفين (U.S. Office of Personnel Management) الذي أدّى إلى سرقة عشرات الملايين من سجلّات الموظفين شديدة الحساسية (هيرشفلد دايفس (Hirschfeld Davis)، 2015) وهجوم برنامج الفدية واناكراي (WannaCry) (بيرلروث وسانجر (Perlroth and Sanger)، 2017).[1] وربطت مجموعة متنوّعة من الخبراء مرتكبي هذه الجرائم في كل من هذه الحالات بجهات فاعلة مقتدرة حكومية وغير حكومية.

تشير الحوادث الإلكترونية الأخيرة، ومن ضمنها هجوم برنامج الفدية واناكراي (WannaCry) إلى تعاظم تهديد الجهات الفاعلة الخبيثة الحكومية وغير الحكومية.

ومع توسّع انتشار تكنولوجيا المعلومات وترسّخ استخدام الفضاء الإلكتروني في حياتنا اليومية، تزداد احتمالات الهجمات من قبل الجهات الفاعلة الخبيثة. وتشير تقديرات مكتب مدير الاستخبارات القومية الأمريكي (Office of the Director of National Intelligence) إلى تطوير أكثر من 30 دولة مستقلة برامج عمليات إلكترونية هجومية (مجلس الشيوخ الأمريكي، 2017). وبالإضافة إلى ذلك، تتوفر هذه القدرات على نحو متزايد بين أيدي الجهات الفاعلة الإجرامية وغيرها من الجهات غير الحكومية (أوينز ودام ولين (Owens, Dam, and Lin)، 2009). وينطوي انتشار القدرات الإلكترونية الهجومية وازدياد توفرها تجاريًا على إمكانية زعزعة استقرار الحكومات وتهديد تكنولوجيا الإنترنت التي يزداد اعتمادنا عليها. ونظرًا لغياب الآليات المؤسسية الموثوقة لاحتواء الأخطار في الفضاء الإلكتروني، يهدد خطر وقوع الحوادث السلام الدولي والاقتصاد العالمي.

ومن أجل تعزيز استقرار النظام الدولي والحد من خطر اندلاع النزاعات الناجمة عن أنشطة إلكترونية سعى عدد من الدول والجهات الفاعلة غير الحكومية والمؤسسات الدولية للتوصل إلى اتفاق بشأن قابلية تطبيق القانون

[1] تستخدم هذه الدراسة مفهوم الهجوم الإلكتروني بمعناه العريض والرائج ليشمل اختراقات الفضاء الإلكتروني التي تهدّد سريّة البيانات أو سلامتها أو توفّرها. ويشمل استخدامنا لمفهوم الهجمات الإلكترونية عمليات استخراج المعلومات والتجسس فضلًا عن الهجمات التخريبية أو الهدّامة. ويميّز باحثون آخرون بين الهجمات الإلكترونية والتجسس الإلكتروني. انظر مثلًا أوينز ودام ولين (2009) (Owens, Dam, and Lin، ص. 1-2).

الدولي وقواعد سلوك الدولة المسؤولة في الفضاء الإلكتروني. وفي تقرير اتفاق مجموعة من الخبراء الحكوميين تابعة للأمم المتحدة صدر في عام 2015 وفي بيان قادة مجموعة العشرين أكّدت قوى إلكترونية كبرى تشمل روسيا والصين والولايات المتحدة أن القانون الدولي ينطبق على الفضاء الإلكتروني وأنه يتعيّن على الدول الالتزام بقواعد السلوك بما في ذلك الالتزام بالامتناع عن تنفيذ الهجمات الإلكترونية التي تضعضع البنى التحتية الأساسية (مجموعة العشرين، غير مؤرّخ؛ الجمعية العامة للأمم المتحدة، 2015).[2] وقد أوضحت أيضًا الجهود الأخرى مثل دليل تالين 2.0 *(Tallinn Manual)* كيف يمكن أن ينطبق القانون الدولي على الإجراءات التي تتّخذها الدول في مجال الفضاء الإلكتروني (شميت (Schmitt)، 2013).[3] وتشكّل هذه التطورات خطوةً مهمة نحو بناء تفاهم مشترك يساعد على تعزيز استقرار العلاقات بين الدول. ولكن تغيب المؤسسات والعمليات الموازية لتشجيع الدول على الوفاء بالتزاماتها ومواجهة المظالم عند حدوث أنشطة إلكترونية خبيثة. وفي أوساط أخرى من العلاقات الدولية، تعهّد المجتمع الدولي بالتزامات رسمية بموجب معاهدات، مثل معاهدة الحد من انتشار الأسلحة النووية واتفاقية الأسلحة الكيميائية، وبالإضافة إلى ذلك، وُضعت آليات للمراقبة وإنفاذ الامتثال مثل الوكالة الدولية للطاقة الذرية ومنظمة حظر الأسلحة الكيميائية. ونظرًا للخلافات بين الدول بشأن القيمة التي تضطلع بها معاهدة الأمن الإلكتروني الرسمية ومضمونها والتحديات التقنية المرتبطة بمراقبة النشاط الإلكتروني وحداثة الفضاء الإلكتروني النسبية باعتباره مجالاً للعمليات الهجومية تغيب المؤسسات والعمليات المقبولة على نطاق واسع والمصممة خصيصًا لمحاسبة الجهات الفاعلة الإلكترونية الخبيثة على أعمالها.

ويكمن جزء من التحدي الذي تفرضه المساءلة في مجال الفضاء الإلكتروني في غياب الموثوقية العالية والإقناع العام بمسؤولية الحوادث الإلكترونية. ويتطلّب تحديد مصدر الهجمات الإلكترونية فحص الأدلة لتحديد المسؤولية على غرار دور اختصاصيي الأدلة الجنائية في نظام العدالة الجنائية. ويتطلّب التحقيق لتحديد مصدر الهجمات الإلكترونية تحليلًا دقيقًا جدًا للبيانات التقنية وفهم الدوافع السياسة أو الاقتصادية وتحليل المعلومات الاستخباراتية الشاملة ذات الصلة في حال توفّرت. ونظرًا للطبيعة الفنية المعقدة والمتعددة الجوانب لتحديد مصدر الهجمات الإلكترونية فإن القدرات المتخصصة والفعّالة تعد ضرورية لإجراء التحقيق الذي قد لا يتوصّل إلى نتيجة موثوقة وذات مصداقية عالية في الوقت المناسب حتى عندما تُخصص له الموارد. ويزداد عدد الهيئات الحكومية والشركات الخاصة والمنظمات المتخصصة بالأبحاث القادرة على إجراء التحقيقات من أجل تحديد مصدر الهجمات الإلكترونية. ولكن هذه الكيانات لا تتّبع منهجية بحث موحّدة وتستخدم مصطلحات تسمية مختلفة للجهات الفاعلة وراء التهديدات الإلكترونية ومقاييس الثقة لنتائجها كما يتّضح من تقاريرها المتعددة حول تحديد مصدر الهجمات الإلكترونية. وعندما تعلن هذه الكيانات عن المصادر المزعومة

[2] تجدر الإشارة إلى عدم تضمّن أي من البيانين اللذين صدرا عن مجموعة العشرين ومجموعة الخبراء الحكوميين التابعة للأمم المتحدة قواعد تحظّر التجسّس الإلكتروني.

[3] يمثّل دليل تالين *Tallinn Manual* وجهات نظر مجموعة من الخبراء في القانون الدولي ولا يشكّل وثيقة ملزمة قانونًا.

تُعتبر نتائجها أحيانًا مسيّسة ومرتكزة على أدلة محدودة أو مبهمة وينفيها المتّهمون وتُقابل بالتشكيك. ويشكّل التحديد المقنع لمصدر الهجمات الإلكترونية شرطًا ضروريًا لمحاسبة الجهات الفاعلة الخبيثة على أفعالها علنًا.. وبالإضافة إلى ذلك فإن مشاركة تفاصيل تكتيكات الهجوم الإلكتروني وهيكليته عن طريق نشر نتائجه قد تساعد حماة الشبكة على إحباط الهجمات المستقبلية. وقد يفرض تحديد مصدر الهجمات الإلكترونية في بعض الحالات كلفة مباشرة على الجهات الفاعلة من خلال "تسميتها والتشهير بها". ولكن لا بدّ من الإشارة إلى أن تحديد المصدر وحده لا يكفي دائمًا للمساءلة لا سيّما إذا لم يأبه المهاجمون بكشف هويتهم علنًا. وعلى الرغم من أن نتائج تحديد المصدر قد تسهّل آليات الإنفاذ الفعال فإنها لا تؤدي دائمًا بحد ذاتها إلى المساءلة. ومع ذلك سيعود تحسين ممارسات تحديد المصدر العلنية المقنعة بالنفع على مستخدمي الفضاء الإلكتروني ككل.

ونستعرض في هذه الدراسة الوضع الراهن لتحديد مصدر الهجمات الإلكترونية وندرس العوامل التي تضعضع موثوقية نتائج تحديد المصدر الملموسة ونتطرّق إلى المؤسسات والعمليات للتغلّب على التحديات التي تفرضها الموثوقية. ومن أجل تحقيق هذا الهدف استعرضنا عيّنةً من أبرز الحوادث الإلكترونية التي شهدها عام 2017 والتي شملت هجمات عابرة للحدود الوطنية واستشرنا عددًا من الاختصاصيين والباحثين في مجال الأمن الإلكتروني المطّلعين على عملية تحديد المصدر. ودرسنا هذه الحوادث من منظور تحديد مصدر الهجمات الإلكترونية ونظرنا في العوامل المؤثّرة في قرار إجراء تحقيق لتحديد المصدر أم لا ونوع المنظمة التي تتولّى التحقيق كما نظرنا في اعتبار البيان العام بشأن نتيجة تحديد المصدر موثوقًا ومقنعًا أم لا. وأخذنا في الاعتبار الطرق الحالية التي تعمل بها جهات التحقيق لتحديد المصدر والآليات المحتملة التي قد يؤثّر من خلالها التعاون غير الرسمي أو الرسمي في شفافية نتائج تحديد مصدر الهجمات الإلكترونية وموثوقيتها.

وندرس إنشاء منظمة دائمة تتألّف من القطاع الخاص ومن جهات فاعلة أخرى غير حكومية مكلفة بتحديد مصدر الهجمات الإلكترونية الكبرى. وتُكلَّف هذه المنظمة بمهمّة محددة تتمثّل في تحديد المسؤولية على أعلى مستوى ممكن من الموثوقية وبأكبر قدر من الدقة تسمح به الأدلة المتوفّرة وإتاحة الأدلة والنتائج للرأي العام. ولا بدّ من الإشارة إلى أهمية امتناعها عن القيام بأنشطة إنفاذ. وفي حين نناقش بإيجاز المنافع والسلبيات المرتبطة بهذه المنظمة الرسمية لا تهدف هذه الدراسة إلى إثبات أن اقتراحنا يشكّل النهج الأفضل والوحيد وإنما النظر في محاسنه المحتملة وتحدياته واستكشاف بنيته. ومن أجل الكشف عن ميزات منظمة تحديد مصدر الهجمات الإلكترونية ووظائفها قمنا بتحليل المنظمات الحكومية الدولية ذات الصلة وعمليات التحقيق المخصصة وهيئات أصحاب الشأن المتعددين.

ويشمل أحد العناصر الرئيسية في توصياتنا ألا تتضمّن منظمة تحديد المصدر الموثوقة والشفافة التمثيل الرسمي للدول. ويشير تحليلنا لممارسات تحديد المصدر إلى أن المسؤولين الحكوميين غالبًا ما يعلنون عن مزاعم تحديد المصدر لأسباب سياسية، وعندما يفعلون ذلك، لا يشاركون الأدلة وراء نتائجهم لأنها ترتكز على مصادر وطرق حساسة. وقد أدت هذه العوامل إلى

جانب التراجع العام في الثقة بالحكومة على الصعيد العالمي إلى إدراك أن مزاعم الحكومة بشأن تحديد المصدر تفتقر للشفافية والموثوقية. وبالرغم من امتلاك بعض الدول التي تتمتّع بقدرات عالية قدرات استخباراتية شاملة قد تكون مطلوبة لدعم نتائج تحديد المصدر تكثر الأمثلة عن تحقيقات تحديد المصدر التي يجريها القطاع الخاص وباحثون غير حكوميين ولا تتطلّب بالضرورة قدرات استخباراتية متخصصة. وتشير هذه الأمثلة إلى أن قدرات الحكومة الاستخباراتية ليست ضرورية دائمًا لتحديد المصدر بطريقة عالية الموثوقية. ولا ينبغي التوقع من منظمة لتحديد المصدر لا تشمل استخبارات حساسة مستمدة من الحكومة أن تتوصّل إلى تحديد المصدر على نحو عالي الموثوقية في الحالات كافة. وبالفعل ستظهر على الأرجح مجموعة من الحالات لا تكون فيها منظمة تحديد المصدر غير المنحازة للحكومة مجهّزة لاتّخاذ قرار بشأن المصدر بدون الرؤى التي قد تتمكن وكالات الاستخبارات الحكومية من توفيرها. ومع ذلك، تستطيع المنظمة التي تتمتّع بهيكلية ملائمة وبإدارة جيدة بدون عضوية حكومية أن تجري تحقيقات أكثر شفافيةً وأن تكون أكثر استعدادًا لتقديم الأدلة من أجل مراجعتها العامة، وذلك في الحالات التي لا تتطلّب موارد استخباراتية. وتستطيع المنظمة بهذه الطريقة أن تعزز موثوقية نتائجها عند تحديد المصدر وتمكين الجهات الفاعلة الأخرى من القيام بمتابعة إضافية لأعمال الإنفاذ واتّخاذ إجراءات دفاعية للشبكة.

ونستعرض في الفصول اللاحقة أبرز الهجمات الإلكترونية ونناقش تحديد مصدر الهجمات الإلكترونية عمليًا مع التركيز بشكل خاص على توفير الموثوقية والشفافية عند تحديد المصدر. وتهدف مناقشتنا إلى تقديم لمحة عامة رفيعة المستوى عن طريق استخدام الأمثلة التوضيحية بدلًا من التقييم الشامل أو المسهب لكافة جوانب هذا الحقل المعقّد والديناميكي. ونقدّم رؤى رئيسية متعددة حول ديناميات تحديد مصدر الهجمات الإلكترونية في الممارسة الحالية وننظر في آليات متعددة تُعنى بكيفية تعاون جهات التحقيق من أجل إجراء تحقيق لتحديد مصدر الهجمات الإلكترونية. وبعد اللمحة العامة عن تحديد المصدر عمليًا، ننتقل إلى اقتراحنا بإنشاء منظمة مستقلة لتحديد مصدر الهجمات الإلكترونية ومناقشة ميزاتها الأساسية.

ونعتبر هذا العمل دراسةً أولية تحفّز التفكير في كيفية بناء هيكلية منظمة مستقلة لتحديد مصدر الهجمات الإلكترونية. ويجري التطرّق إلى المسائل الرئيسية مثل التمويل بإيجاز ليس إلا. وبالفعل يُفضّل أن يتّخذ أعضاء المنظمة نفسها القرارات بشأن تفاصيل تنظيمية وإدارية كثيرة. والأهم من ذلك أننا نعترف بأن اقتراحنا ليس البنية الوحيدة القابلة للتطبيق إذ تتوفّر نهج جديرة أخرى لتحديد مصادر الهجمات الإلكترونية. ونرى أن اقتراحنا يتناسب مع مجموعة من الحلول، بما في ذلك قدرات الدول على تحديد المصدر، التي ستحسّن تحديد مصدر الهجمات الإلكترونية. وبالرغم من التحفظات نقدّم خصائص رئيسية متعددة لا بدّ من أخذها في الاعتبار إذا تم إنشاء مثل هذه الهيئة.

استعراض لأبرز الهجمات الإلكترونية

سعى ضحايا الحوادث الإلكترونية إلى معرفة مصادر الهجمات منذ نشأة الإنترنت.[1] وفي عام 1986 اكتشف كليف ستول (Cliff Stoll)، وهو مدير نظام يعمل في مختبر لورنس بيركلي الوطني (Lawrence Berkeley National Laboratory)، عمليات اختراق متعددة وأنشطة استخراج البيانات في أنظمة المختبر. وقد تعاون ستول مع شركات الاتصالات وموظفي إنفاذ القانون في الولايات المتحدة وألمانيا الغربية لإجراء تحقيق تقني امتد طوال أشهر وأسفر عن تحديد هوية المهاجمين واعتقالهم (ستول (Stoll)، 2012).

وتطورت في السنوات الـ 30 التي تلت تحقيق ستول المتخصص القدرةُ على رصد مصدر الاختراقات الإلكترونية ومنعها، فتحوّلت من مجرّد الاعتماد على مثابرة مجموعة من مدراء الأنظمة المتخصصين إلى قطاع تبلغ قيمته مليار دولار (مورغان (Morgan)، 2015). وقد حقّق سوق الأمن الإلكتروني العالمية تطورات في أمن الشبكات والأجهزة والاستخبارات المتعلقة بالتهديدات وجمع البيانات القابلة للقياس وتحليلها. ولا بدّ من الإشارة إلى ظهور قطاع متنام من شركات خدمات الأمن الإلكتروني، مثل فاير آي (FireEye) وكراودسترايك (CrowdStrike) وكاسبرسكي لاب (Kaspersky Lab) ونوفيتا (Novetta) وسيمانتك (Symantec) وتراند مايكرو (Trend Micro)، التي تقدّم خدمات استشارية ومن ضمنها التحقيقات لتحديد مصدر الهجمات الإلكترونية. وقد سعت الدول أيضًا إلى تحسين قدراتها في تحديد مصدر الهجمات الإلكترونية بعدما أدركت أن تحديد المصدر يشكّل عنصرًا أساسيًا للردع الفعّال.[2] ويعكس نضوج شركات الأمن الإلكتروني وتطوّر طرق تحديد المصدر المتقدمة وتزايد تعقيد العالم المتشابك تنامي نطاق الحوادث الإلكترونية والتهديد والضرر المحتمل الناجم عنها.

ونعرض في هذا الفصل عينةً من أبرز هذه الحوادث اختيرت لدرجة التنوّع التي تظهرها (في ما يتعلّق بالضحايا والنطاق وطريقة الهجوم والمعتدي والاستجابة لتحديد المصدر) وليس لتمثيليتها. وينبثق عن استعراض هذه

يجري عدد متزايد من شركات الأمن الإلكتروني – مثل فاير آي (FireEye) وكراودسترايك (CrowdStrike) وكاسبرسكي لاب (Kaspersky Lab) وسيمانتك (Symantec) – تحقيقات لتحديد مصدر الهجمات الإلكترونية.

[1] تشير كلمة ضحية في السياق المستخدم هنا إلى كيان أو منظمة تعرضت لهجوم إلكتروني.

[2] مثلًا، تفيد وزارة الدفاع الأمريكية في استراتيجية الأمن الإلكتروني التابعة لها لعام DoD Cyber Strategy 2015 أنه "في ما يتعلّق بالاستخبارات وتحديد المصدر والتحذير استثمرت وزارة الدفاع ومجموعة الاستخبارات إلى حد كبير في قدرات جمع البيانات من المصادر كافة وتحليلها ونشرها إذ يحدّ ذلك من مجهولية نشاط الجهات الفاعلة الحكومية وغير الحكومية في الفضاء الإلكتروني.

الحالات مجموعة متنوعة من الردود على تحديد المصدر ونهج الإبلاغ عنها التي تزيد من غموض هذا الموضوع المبهم أصلًا.

ويعرض الجدول 1 الجدول الزمني لأبرز الحوادث الإلكترونية التي تنطوي على هجمات عابرة للحدود الوطنية. وقد اخترنا هذه المجموعة من الهجمات لتحليلها إذ ترتّبت عليها تداعيات جغرافية سياسية ونوقشت على نطاق واسع في الأوساط البحثية والصحافة وسلّطت الضوء على رؤى مفيدة تتعلّق بممارسة تحديد المصدر. وشملت الحالات ضحايا من الحكومات وغير الحكومات وأدّت إلى مجموعة متنوعة من التأثيرات كالأضرار المادية واستخراج البيانات والخسائر المالية. وشملت الحالات أيضًا أساليب هجومية بسيطة ومعقّدة وغالبًا ما تُطلق على المهاجمين المتطورين تسمية التهديد المتواصل المتطور.[3] وقد استعرضنا هذه الحالات من منظور تحديد مصدر الهجمات الإلكترونية بما في ذلك أنواع الأدلة المتوفرة والأطراف التي حلّلت الأدلة وخصائص البيانات العامة بشأن نتائج تحديد المصدر وكيفية استجابة المهاجم المزعوم والأطراف الأخرى ذات الصلة. وبالإضافة إلى الموجز في الجدول 1 تتم مناقشة عدد من هذه الحوادث بتفاصيل أكبر في دراسات الحالة 1-5.

ويشير تحليلنا لهذه الحالات إلى أن ممارسة تحديد المصدر منتشرة النطاق ومتباينة. ولم تُستخدم في هذه الحالات أي طريقة موحّدة في التحقيقات اللازمة لتقييم الأدلة ولا مقياس موثوقية عالمي للتوصل إلى نتيجة. وأهم ما في ذلك أيضًا أن الحالات توضّح الأساليب المميزة التي استخدمتها الجهات للتصريح علنًا عن نتائج تحديد المصدر. وفي حالات متعددة، أُجريت التحقيقات بدون أن تنشر جهة التحقيق أو الضحية أي نتيجة رسمية لتحديد المصدر. مثلًا، وبالرغم من التصور الراسخ بأن الحكومة الصينية كانت مسؤولة عن اختراق المكتب الأمريكي لإدارة شؤون الموظفين، لم تلقِ عليها الحكومة الأمريكية المسؤولية علنًا. وفي الكثير من هذه الحالات قوبلت البيانات العامة بشأن تحديد المصدر بالريبة والارتباك والمطالبة بالشفافية بشأن التحقيق والأدلة التي يستند إليها.

وفي الفصل التالي، نعرض التحديات التي واجهتها الجهات التي تتولّى التحقيقات لتحديد المصدر. وبالرغم من تقدّم تحديد المصدر من منظور تقني من جرّاء تزايد نضوج قدرات تحديد المصدر، يكمن التحدي الكبير في شرح النتيجة والأدلة المستندة إليها للرأي العام.

[3] يشير تصنيف التهديدات المتواصلة المتطوّرة إلى مزيج من التقنيات المتطورة التي قد تعسّر بوجه خاص تحديد المصدر ومن طرق الوصول عن بعد الطويلة الأمد والمتواصلة التي تستهدف ضحية محددة. انظر المعهد الوطني للمعايير والتكنولوجيا (2011).

الجدول 1

أبرز الهجمات الإلكترونية وخصائص تحديد مصادرها

الحادث	السنة التي بدأ فيها	التأثير	تحديد المصدر في النطاق العام[a]
مختبر لورنس بيركلي الوطني (الولايات المتحدة)	1986	اختراق بيانات حساسة واستخراجها[b]	محاكمة جنائية في ألمانيا الغربية، 1990
تايتن راين (Titan Rain) (الولايات المتحدة)	2003	استخراج بيانات حساسة من منظمات تشمل وكالة ناسا (NASA) ولوكهيد مارتن (Lockheed Martin) ومختبرات ساندیا الوطنية (Sandia National Laboratories) ومكتب التحقيقات الفيدرالي فضلًا عن وزارتي الدفاع الأمريكية والبريطانية[c]	عزته الحكومة والمصادر الخاصة في وسائل الإعلام بدرجة كبيرة إلى الصين في عام 2005؛ وهو ما عارضته الدولة ا لصينية
هجمات القطع الموزّع للخدمة الإستونية (إستونيا)	2007	هجمات قطع موزّع للخدمة واسع النطاق على المواقع الإلكترونية الإستونية في إطار التوترات مع روسيا	اتهمت الحكومة الإستونية جهات فاعلة حكومية روسية؛ ألقت روسيا باللائمة على حركة شبابية مؤيدة للكرملين وليس على جهات فاعلة ترعاها الدولة
دودة ستوكسنت (إيران)	2010	أضرار مادية بأجهزة الطرد المركزي الإيرانية؛ أُصيبت بها أجهزة الكمبيوتر عالميًا	عُزي بدرجة كبيرة إلى الولايات المتحدة وإسرائيل؛ تسريبات من قبل مسؤولين أمريكيين
هجمات القطع الموزّع للخدمة على المصارف الأمريكية (الولايات المتحدة)	2012	هجمات القطع الموزّع للخدمة على أكثر من 46 من أبرز المؤسسات المالية في الولايات المتحدة	تصور واسع النطاق لرعاية الدولة الإيرانية؛ تسريبات أولية من الحكومة الأمريكية وفي نهاية المطاف اتهام الجهات الفاعلة الحكومية الإيرانية في آذار (مارس) 2016
أرامكو السعودية (السعودية)	2012 و2016	مسح 35,000 جهاز كمبيوتر تابع لأرامكو السعودية أو تدميرها؛ هجوم مماثل في أواخر عام 2016	في عام 2012 ربط مسؤولون أمريكيون الهجوم بإيران في وسائل الإعلام
حساب وكالة أسوشيتد برس (Associated Press) على تويتر (Twitter) (الولايات المتحدة)	2013	قرصنة حساب وكالة أسوشيتد برس على تويتر ونشر تغريدة كاذبة عن هجوم على البيت الأبيض ما أدّى إلى هبوط حاد في أسعار الأسهم	تبنّى الجيش السوري الإلكتروني Syrian Electronic Army الهجوم
البيت الأبيض ووزارة الخارجية (الولايات المتحدة)	2014	اختراق كبير لأنظمة الكمبيوتر غير السرية	عُزي بدرجة كبيرة إلى روسيا ولكن لم تحدد الحكومة الأمريكية رسميًا المصدر
سوني بكتشرز (Sony Pictures) (الولايات المتحدة)	2014	سرقة بيانات حساسة وتسريبها؛ تعطيل كبير للأعمال	عزاها الرئيس الأمريكي إلى جهات فاعلة حكومية كورية شمالية في كانون الأول (ديسمبر) ٢٠١٤ وعزتها عملية أوبريشن بلوكباستر (Operation Blockbuster) إلى مجموعة لازاروس (Lazarus) في عام 2016[d]
غيت هاب (GitHub) (الولايات المتحدة)	2015	هجوم قطع موزّع للخدمة كبير ومتواصل على موقع التعاون لتطوير البرمجيات	عزته الشركات الخاصة والباحثون بدرجة كبيرة إلى جهات فاعلة حكومية صينية
قناة تي في 5 موند (TV5Monde) (فرنسا)	2015	تعطّل القناة التلفزيونية لمدة 18 ساعة؛ أدى الحادث المموّه إلى الإلقاء باللائمة على داعش[e]	عزته شركة فاير آي لمجموعة القرصنة الروسية آي بي تي 28 (APT28) في حزيران (يونيو) 2015
المكتب الأمريكي لإدارة شؤون الموظفين (الولايات المتحدة)	2015	استخراج 21.5 مليون سجل خاص بموظفي حكومة الولايات المتحدة	عُزي بدرجة كبيرة إلى الصين علمًا أن الحكومة الأمريكية لم تحدد رسميًا المصدر

الجدول 1 – يتبع

الحادث	السنة التي بدأ فيها	التأثير	تحديد المصدر في النطاق العام[a]
البرلمان الألماني (ألمانيا)	2015	استخراج ونشر 2,420 ملفًا حساسًا ينتمي للاتحاد الديمقراطي المسيحي الألماني (Christian Democratic Union)	عزاه المكتب الفيدرالي لحماية الدستور (BfV) لمجموعة آي بي تي 28 في وسائل الإعلام في أيار (مايو) 2016 [f]
شبكة الكهرباء الأوكرانية (أوكرانيا)	2016	انقطاع الطاقة لساعات متعددة في محطات توزيع الطاقة الإقليمية وقطع الكهرباء عن 225,000 مستهلك	اتّهم مسؤولون أوكرانيون روسيا؛ أشارت شركات خاصة إلى جهات فاعلة حكومية محتملة و/ أو مجرمين إلكترونيين
اللجنة الديمقراطية الوطنية (DNC) (الولايات المتحدة)	2016	استخراج وثائق خاصة باللجنة الديمقراطية الوطنية والحملة الانتخابية ونشرها؛ تدخّل بالانتخابات الرئاسية الأمريكية في عام 2016	عزته شركة كراود سترايك (CrowdStrike) (حزيران (يونيو) 2016) وتقرير مكتب مدير الاستخبارات القومية الأمريكي (كانون الثاني (يناير) 2017) إلى جهات فاعلة حكومية روسية[g]
البنك المركزي في بنغلادش (بنغلادش)	2016	سرقة مبلغ 81 مليون دولار من حساب البنك المركزي في بنغلادش لدى البنك الاحتياطي الفيدرالي في نيويورك باستخدام نظام جمعية الاتصالات السلكية واللاسلكية بين المصارف على مستوى العالم في الميدان المالي المصرفي (SWIFT)	ربطه تقرير شركة سيمانتك بمجموعة لازاروس في أيار (مايو) 2016؛ ربطه تقرير وكالات الاستخبارات الأمريكية بدولة كوريا الشمالية وفقًا لوسائل الإعلام في آذار (مارس) 2017
موساك فونسيكا (Mossack Fonseca) (بنما)	2016	تسريب 11.5 مليون وثيقة تمثّل أكثر من 214,488 كيانًا خارجيًا أدّت إلى تهم عديدة بالتهرّب الضريبي والفساد	لم يُحدد مصدر حتى تاريخه؛ نشطاء محتملون من القراصنة الإلكترونيين و/ أو عملية داخلية
دين (Dyn) (الولايات المتحدة)	2016	هجوم قطع موزّع للخدمة باستخدام شبكة مصابة من أجهزة إنترنت الأشياء استهدف مزود نظام أسماء النطاقات دين وعطّل عددًا كبيرًا من المواقع الإلكترونية	لم يُحدد المصدر رسميًا؛ عُزي بدرجة كبيرة إلى منظمة قرصنة ناشطة مثل أنونيموس (Anonymous) أو نيو وورلد هاكرز (New World Hackers) أو سباين سكواد (SpainSquad)
واناكراي (عالميًا)	2017	هجوم برنامج فدية طال قطاعي الرعاية الصحية والنقل والبنية التحتية للاتصالات في جميع أنحاء العالم	لم يُحدد المصدر رسميًا؛ ربطته بعض الشركات الخاصة بمجموعة لازاروس؛ ألقت روسيا باللائمة على الولايات المتحدة لابتكارها برمجية إكسبلويت (Exploit) القادرة على تفعيل برنامج واناكراي

ملاحظة: إن المعلومات كافة مفتوحة المصدر وجُمعت من وسائل إعلام متاحة للعامة وواسعة الانتشار إلا إذا ذُكر خلاف ذلك.

[a] عزو المصدر إلى فرد أو مجموعة أو دولة وإتاحته للعامة عن طريق التقارير الرسمية ووسائل الإعلام والبيانات العامة. ويمكن أن تتولى نشر التقرير الشركات الخاصة أو الحكومات (بيانات عامة رسمية تحدد المصدر سواء عن طريق تقرير رسمي أو اتهام أو بيان رسمي صادر عن مسؤولين حكوميين وموجّه لفرد أو مجموعة أو دولة) أو وسائل الإعلام الإخبارية نقلًا عن مصادر رسمية وغير رسمية.

[b] ستول (Stoll)، 2012.

[c] ثورنبورغ (Thornburgh)، 2005؛ نورتون – تايلور (Norton-Taylor)، 2007.

[d] فريق الأبحاث المتعلقة بالتهديدات لدى نوفيتا (Novetta Threat Research Group)، 2016.

[e] الدولة الإسلامية في العراق والشام وتُعرف أيضًا بالدولة الإسلامية في العراق وسوريا أو الدولة الإسلامية

[f] هو وكالة استخبارات وطنية حكومية ألمانية (المكتب الفيدرالي لحماية الدستور واختصاره BfV)

تحديد مصدر الهجمات الإلكترونية على الصعيد العملي

تظهر تحديات كثيرة في تحديد مصدر الهجمات الإلكترونية وتشمل نقل النتائج على نحو مقنع إلى الرأي العام.

تشير الأوساط الأكاديمية والسياسية ومراكز التفكير بانتظام إلى ما يُعرف بتحدي تحديد مصدر التهديدات الإلكترونية بوصفه عائقًا خطيرًا أمام تعزيز الأمن الإلكتروني. ويسعى هذا الفصل إلى تقديم لمحة عامة عالية المستوى والمضي قدمًا بهذه النقاشات عبر التمييز بين نوعين مختلفين من تحديات تحديد المصدر. أولًا، يتمثّل التحدي موضع النقاش الدائم بالوصول إلى الأدلة التقنية وغيرها وتفسيرها ومقارنتها في محاولةٍ للتوصّل إلى نتيجة عالية الموثوقية وفي الوقت المناسب عند تحديد المصدر. وثانيًا، يكمن التحدي الإضافي في نقل نتائج تحديد المصدر على نحو مقنع إلى الجمهور المستهدف أو الرأي العام. سنستعرض هذين التحديين كل على حدة، ثم سنشرح عدد من الرؤى الأساسية للمساعدة على مواجهة هذين التحديين.

التوصّل إلى نتيجة عند تحديد مصدر الهجمات الإلكترونية

يتعلّق التحدي الأول بصعوبة التوصل إلى نتيجة عند تحديد مصدر الهجمات الإلكترونية. وتنطوي عملية تحديد المصدر على تحديد مجموعة الأجهزة التي أتاحت إمكانية اختراق أنظمة كمبيوتر الضحية وتحديد هوية الجاني الذي وجّه الاختراق و/ أو تحديد الخصم المسؤول في نهاية المطاف عن الحادث الخبيث (لين (Lin)، 2016). ولا بدّ من استعراض موجز لبعض ميزات الفضاء الإلكتروني التي تعقّد القدرة على تأدية مهمة تحديد مصدر الهجمات الإلكترونية بالرغم من كونه مسارًا مطروقًا. وبعد استعراض هذه الميزات نبيّن المؤشرات والأدلة التي استخدمها المحققون لتقييم المسؤولية.

بدايةً، يمكّن الفضاء الإلكتروني الجهات الفاعلة من العمل بدرجات متفاوتة من المجهولية. وتستطيع الجهات الفاعلة الخبيثة اختراق الشبكات وحتى ترك تأثيرات قد لا تُرصد لأسابيع لا بل سنوات. وثانيًا قد تعمل الهجمات الإلكترونية على نطاقات مكانية تتراوح بين أهداف محلية قريبة من أجهزة المهاجم من حيث المسافة وأهداف عالمية متّصلة من خلال تكنولوجيا الاتصالات وتفصل بينها مسافات بعيدة (انظر أوينز (Owens) ودام (Dam) ولين (Lin)، 2009). ونتيجةً لذلك، يستطيع

المهاجم، وقد يكون فعليًا أي شخص في العالم، أن يوجّه الهجمات عن طريق طرف ثالث بريء تعرّض للاختراق وإضفاء الغموض على مصدرها. وثالثًا يختلف على الأرجح الدليل على ارتكاب الجهة الفاعلة الخبيثة الهجوم الإلكتروني بدرجة كبيرة عن الدليل المستخدم لتحديد مصدر أنواع أخرى من الحوادث. وغالبًا ما تعتمد الأدلة التقليدية المستخدمة في المحاكم الأمريكية على الأدلة المادية التي يمكن مراقبتها وتسجيلها (تمامًا مثل مسار القذيفة الصاروخية أو أغلفة الرصاص من السلاح الناري). وفي المقابل لن يتمكن الشخص العادي من التمييز بين ترميز البحث الكمّي الحميد وترميز استخراج البيانات الخبيث. وبالإضافة إلى ذلك تستند القضايا القانونية التقليدية في الكثير من الحالات إلى معرّفات ثابتة وفريدة عالميًا أو على الأقل نادرًا ما تتكرّر (إذا تكرّرت) مثل بصمات الأصابع أو الحمض النووي. وبالمقابل، تتميّز شبكة الإنترنت بهيكلية غير مركزية وديناميكية ومفتوحة تسمح للمهاجم بإخفاء أثره بسهولة عبر فصل الأجهزة عن الإنترنت أو تغيير بروتوكول الإنترنت (IP) أو الاستفادة من التكتيكات والتقنيات والإجراءات (TTP) التي طوّرتها الجهات الفاعلة الخبيثة الأخرى. لذلك لا يضمن حتى تحديد الأجهزة والطرق المعنية بالهجوم تحقيق نتيجة عند تحديد المسؤولية.

وفي سياق متصل، تُطرح أسئلة أساسية حول مفهوم المسؤولية عن حادث إلكتروني خبيث. ومن أجل تحديد دولة معينة بوصفها مصدرًا للهجوم الإلكتروني لا يكفي مجرد تعقّب الهجوم إلى أجهزة كمبيوتر داخل على سبيل المثال. على سبيل المثال شمل الهجوم الإلكتروني على مزود نظام أسماء النطاقات، دين، أنظمة مخترقة من "ملايين عناوين بروتوكول الإنترنت في مختلف المواقع الجغرافية" (هيلتون (Hilton)، 2016). ويزيد من تعقيد المسألة تفاوت درجات التواطؤ عند النظر في احتمال رعاية دولة ما للهجمات الإلكترونية. فعلى سبيل المثال كيف ينبغي صياغة الإعلان عن تحديد المصدر إذا شجّعت قيادة الدولة ضمنيًا الهجمات الإلكترونية أو علمت بحدوثه وغضت الطرف عنه؟[1] حتى إذا حُدّدت هويات الأشخاص المتورطين في الهجوم قد تكون العلاقة بين الشخص أو الأشخاص والبلد المضيف غامضة.

ويقوم تحديد المصدر في الفضاء الإلكتروني على دراسة الأدلة التي يصعب المقارنة بينها وتفسيرها بما في ذلك المعلومات التقنية الشرعية والدوافع السياسية والاستخبارات الشاملة. ونتيجة للصعوبات التفسيرية المرتبطة بتحديد مصدر الهجوم الإلكتروني وُصفت عملية التحقيق بأنها فن بقدر ما هي علم (ريد وبيوكانان (Rid and Buchanan)، 2015). وبالفعل يفيد أحد الخبراء أن تحديد مصدر الهجمات الإلكترونية المتعدد المصادر يرتكز على "التقدير" وهو ليس استنتاجًا يمكن اثباته على نحو قاطع (لين، 2012). ومع ذلك تستخدم مجموعة متنوعة من الخبراء في مجال الأدلة الجنائية الإلكترونية ممارسات وطرق رائجة تلقي الضوء على تحديد المصدر. وفي حين لا تضمن أي أدلة تقريبًا نتيجة عالية الموثوقية توفّر عوامل متعددة أساسًا لتقييم المسؤولية.

المؤشرات التقنية

[1] للمزيد من المعلومات حول "طيف مسؤولية الدولة" انظر هيلي (2011) (Healey).

تشمل الطرق التي يلجأ إليها المهاجم وأدوات الهجوم عناصر تقنية متعددة يمكن استخدامها لدعم تحديد مصدر مزعوم (برثولوميو وغيريرو – سعادة (Bartholomew and Guerrero-Saade)، 2016؛ ديسيانو (DeCianno)، 2014). ويمكن استقاء هذه العناصر التقنية من الأنشطة الشرعية مثل تحليل الشبكة والتحقق من ملفات السجلات والبرمجيات وتنفيذ العمليات على أنظمة كمبيوتر الضحية والتحقق من الشبكات التي تستخدمها الضحية عن طريق طرف ثالث مقدّم للخدمات. وتشمل العناصر السلاسل النصية والأختام الزمنية وبنية الأوامر والتحكم (C2) وعيّنات من البرمجيات الخبيثة ومعرّفات مثل كلمات السر وعناوين بروتوكول الإنترنت (IP addresses).

وقد تتضمّن السلاسل النصية المكتشفة في هجوم ما لغةً مكتوبة تشير إلى مهاجم معيّن. وعلى سبيل المثال، احتوت دودة ستَوكسنت (Stuxnet) على سلسلة "ميرتوس" (myrtus) التي يعتقد بعض الخبراء أنها تورّط الإسرائيليين وذلك بالاستناد إلى مراجع توراتية (وعلى الرغم من أن آخرين أفادوا أن السلسلة هي مجرّد اختصار يرتبط بـ "وحداتي الطرفية النائية" (my remote terminal units)).[2] ويشير ذلك إلى أن السلاسل النصية قد تتضمّن أيضًا أسماء الوظائف البرمجية التي يُعثر عليها في الترميز الخبيث. فعلى سبيل المثال رُبطت وظيفة "المسح" (wipe-out) التي عُثر عليها في البرمجية الخبيثة المرتبطة بالهجوم على

[2] من الأمثلة على ذلك،، قد يخلّف المهاجمون معرّفات شخصية في الترميز الخبيث أو يمنعون العدوى عن طريق التحقق من وجود سلاسل نصية في مفاتيح التسجيل. انظر ماركوف وسانجر (2010) (Marko and Sanger).

دراسة الحالة 1

عملية سطو إلكتروني على البنك المركزي في بنغلادش (Bangladesh Central Bank)

في شباط (فبراير) 2016 تعرّض النظام المصرفي الدولي للقرصنة في محاولة لسرقة مبلغ 951 مليون دولار من البنك المركزي في بنغلادش. فقد أعطى المهاجم خلال هذه العملية تعليمات زائفة بسحب أموال من حساب البنك المركزي في بنغلادش لدى البنك الاحتياطي الفيدرالي في نيويورك باستخدام شبكة سويفت المصرفية لاستكمال التحويل (زيتير (Zetter)، 2016). ونجحت عملية القرصنة بسحب مبلغ 101 مليون دولار قبل أن يوقفها البنك الاحتياطي الفيدرالي في نيويورك. وحُوّل من هذه المبالغ المسروقة مبلغ 20 مليون دولار إلى سريلانكا استعيد لاحقًا وحُوّل المبلغ المتبقي البالغة قيمته 81 مليون دولار فقد حوّل إلى الفلبين ولا يزال معظمه مفقودًا. وقد الدافع المالي الظاهر للهجوم إلى اشتباه الكثيرين بجماعات إجرامية غير حكومية في حين اتّهمت حكومة بنغلادش نفسها مجموعة من الجهات الفاعلة الحكومية وغير الحكومية. وبحلول منتصف عام 2016 لفت محققون من القطاع الخاص إلى أن البنك المركزي قد اخترقته ثلاث جهات فاعلة على الأقل واستخدمت إحداها برمجية خبيثة مرتبطة بمجموعة لازاروس (نوقشت بالتفاصيل في دراسة الحالة 5). وفي آذار (مارس) 2017 أي بعد مرور سنة على الهجوم دعم مسؤولون من الاستخبارات الأمريكية هذه التقارير عبر الإشارة إلى تورط كوريا الشمالية ولكنهم لم يقدّموا أي أدلة (فريق الاستجابة التابع لسيمانتك، 2016؛ ليما (Lema)، 2017؛ غرول (Groll)، 2017).

البنك المركزي في بنغلادش (دراسة الحالة 1 أدناه) ببرمجيات خبيثة عُثر عليها في هجمات أخرى مثل الهجوم على سوني (شيفشينكو ونيش (Shevchenko and Nish)، 2016).

وقد تشير البيانات الوصفية كالأختام الزمنية إلى الوقت الذي جُمعت فيه البرمجية الخبيثة ووقت الإصابة وانتظام جدول عمل المهاجم. وبالإضافة إلى ذلك قد تربط الأختام الزمنية الهجمات ببعضها البعض. على سبيل المثال ارتبطت أختام زمنية مطابقة بترميز الهجمات التي استهدفت اللجنة الديمقراطية الوطنية وهجمات متعددة أخرى استهدفت منظمات دبلوماسية (بوراتوسكي (Buratowski)، 2016).

ويستخدم المهاجمون بنية الأوامر والتحكم (C2) لإيصال البرمجية الخبيثة والحفاظ على قدرة التحكم بها بعد إيصالها. وفي حالة الهجوم الذي استهدف شركة سوني بكتشرز شملت بنية (C2) مضيفات مصابة مستقلة مثل البريد الإلكتروني والألعاب والمؤسسات التعليمية في الولايات المتحدة وتايوان وإندونيسيا والهند والصين. واستفادت أيضًا بنية (C2) في هجوم سوني بكتشرز من الاستخدام "المهمل" لعناوين بروتوكول الإنترنت المرتبطة بالشركات الكورية الشمالية (سانجر وفاكلر (Sanger and Fackler)، 2015).

ومع ذلك، إن توفّر البيانات التقنية التجريمية ليس مضمونًا. وسيحرص الخصوم المتطورون الذين يسعون إلى تجنّب تحديدهم باعتبارهم مصدرًا على تخصيص الموارد لنشر مؤشرات خاطئة وإثارة الشكوك حول أطراف أخرى (برثولوميو وغيريرو – سعادة، 2016). فعلى سبيل المثال استخدمت الجهة الفاعلة المتحدثة بالروسية المرتبطة بالتهديد المتواصل المتطور كلاود أطلس (Cloud Atlas) وثيقة كُتبت على جهاز كمبيوتر تابع لشخص ناطق بالإسبانية وأدخلت سلاسل نصية عربية وأحرفًا وأرقامًا هندية وعناوين متعاقبة لبروتوكول الإنترنت – لتعقيد عملية تحديد المصدر على الأرجح (فاجرلاند وغرانج (Fagerland and Grange)، 2015). ومن المحتمل التلاعب بكل مؤشر من المؤشرات التقنية المستخدمة في تحديد المصدر، أي الأختام الزمنية والسلاسل وإعادة استخدام الترميز إلخ، بطريقة مماثلة لتأخير تحديد المصدر أو تفاديه بالكامل. وبالفعل إذا اعتُبرت بعض المؤشرات التقنية المحددة الدليل الأهم لتحديد المصدر (مثل النظير الأقرب للحمض النووي في الفضاء الإلكتروني) فستخصص إذًا الجهات الفاعلة المتطورة الموارد لإخفاء هذا المؤشّر المحدد أو تمويهه.

المؤشرات السياسية

يتمثل نوع ثان من المؤشرات التي يمكنها المساعدة في التحقيق لتحديد المصدر بالسياق السياسي الذي تقع فيه الحادثة والدوافع ذات الصلة للأطراف القادرة. وفي حال استفادت جهة فاعلة محددة من الهجوم لأسباب سياسية أو اقتصادية أو غيرها فقد يدخل ذلك ضمن تقدير تحديد المصدر. وعلى نحو مماثل قد يكون أيضًا نوع الهدف المختار والمعرفة المتخصصة المطلوبة لاستغلال هذا الهدف بمثابة مؤشرات سياسية ذات صلة.

فمثلًا، اتهمت الصحافة بدرجة كبيرة الولايات المتحدة وإسرائيل بالوقوف وراء هجوم ستوكسنت (Stuxnet) الذي استهدف منشأةً إيرانية لتخصيب اليورانيوم لأسباب متعددة. أولًا استخدم الهجوم مجموعة واسعة من الموارد التقنية بما في ذلك اللجوء إلى هجمات بدون انتظار (zero-day) متعددة والتي لا تملكها إلا الجهات الفاعلة الأكثر تطورًا. وشكّلت الدوافع السياسية مؤشرًا إضافيًا نظرًا إلى أنّ تقهقر البرنامج النووي الإيراني يعود بالنفع على المصالح الأمريكية والإسرائيلية. وعلى نحو مماثل ألقت الحكومة الأوكرانية ووسائل الإعلام باللائمة بدرجة كبيرة على روسيا للهجوم على شبكة الكهرباء الأوكرانية وذلك بسبب الهدف المختار والمعرفة المتخصصة المطلوبة للاختراق والدوافع السياسية الواضحة للجهات الفاعلة الحكومية الروسية. وترتكز أيضًا التكهنات السائدة بأن الصينيين هم من نفّذوا الهجوم على المكتب الأمريكي لإدارة شؤون الموظفين جزئيًا على الادعاء القائل بأن للحكومة الصينية مصلحة فعلية في استخراج هذا النوع من الاستخبارات من الأهداف الأمريكية. ومن الممكن أيضًا تبرير تحديد إيران باعتبارها مصدرًا للهجوم بفيروس شامون (Shamoon) الذي استهدف أرمكو السعودية جزئيًا من خلال تقييم الدوافع السياسية للنظام الإيراني.

وتمامًا كالمؤشرات التقنية التي لا تكون دائمًا كافية لتحديد المصدر بموثوقية عالية، قد لا تكون المؤشرات السياسية قاطعة. فقد يملك الخصوم سببًا لتنفيذ

دراسة الحالة 2

الحادث المموّه في قناة تي في 5 موند

في 8 نيسان (إبريل) 2015 تعرّضت شبكات القناة التلفزيونية العالمية الناطقة باللغة الفرنسية تي في 5 موند للقرصنة ما أدّى إلى انقطاع البث لمدة 18 ساعة (كوريرا (Corera)، 2016). وفي الوقت عينه، هاجم القراصنة أيضًا حسابات تي في 5 موند (TV5Monde) على وسائل التواصل الاجتماعي ونشروا دعاية موالية لـ"داعش" واستبدلوا صور تعريفها الشخصية بشاشة سوداء كُتب عليها "الخلافة الإلكترونية" (CYBERCALIPHATE) و"أنا داعش" (Je suIS IS). وحوّلت الصور جملة "أنا شارلي" (Je suis Charlie) المستخدمة للتعبير عن الوحدة في أعقاب هجمات عام 2015 الإرهابية التي استهدفت الشعب الفرنسي، فبدا الهجوم نهجًا جديدًا اعتمده تنظيم "داعش". وعُزي الهجوم نتيجة ذلك فورًا وبدرجة كبيرة إلى "الخلافة الإلكترونية" (CYBERCALIPHATE) وأثار ذلك المخاوف من قدرات "داعش" الإلكترونية.

ولكن اتّضح في ما بعد أن الخلافة الإلكتروني كان مجرّد تمويه استُخدم في هجوم معقّد غامض الأهداف. وفي الأشهر التي تلت التكهنات الأولية، بدأت التحقيقات التي ترأستها الوكالة الوطنية للأمن الإلكتروني في فرنسا (ANSSI) وشركة فاير آي (FireEye) بتوجيه أصابع الاتهام إلى مصدر آخر. وبحلول حزيران (يونيو) 2015 أفادت شركة فاير آي (FireEye) بأن تحليلها قد تعقّب الهجوم وصولًا إلى مجموعة آي بي تي 28 (APT28) الروسية، وذلك بالاستناد إلى مراجعة المؤشرات التقنية ومن ضمنها البنية التحتية والبرمجية الخبيثة والأختام الزمنية ذات الصلة بالهجوم (لايدن (Leyden)، 2015؛ باغانيني (Paganini)، 2015).

الهجوم حتى لو لم يتّضح علنًا كيف يستفيدون منه. مثلًا اعتُقد في البداية أن الهجوم على قناة تي في 5 موند قد نفّذه تنظيم الدولة الإسلامية ليس بسبب التمويهات التقنية فحسب وإنما بسبب استهداف قناة إخبارية غربية كبرى أيضًا إذ بدا ذلك عملاً يتماشى مع دوافع داعش لزرع الخوف وعدم الاستقرار في المدن الأوروبية (دراسة الحالة 2 أدناه). ولكن بالرغم من التقييم الأولي عزت لاحقًا شركات خاصة متعددة والسلطات الفرنسية الهجوم إلى جهات فاعلة تابعة لمجموعة آي بي تي 28 ومرتبطة بالحكومة الروسية (ويلسون (Wilson)، 2015). وفي حالة سرقة الأموال من البنك المركزي في بنغلادش كانت لمجموعة متنوعة من الجماعات الإجرامية أو حتى دول مثل كوريا الشمالية دوافع لتنفيذ العملية.

المؤشرات الاستخباراتية الشاملة

توفّر القدرات الاستخباراتية أيضًا أدلة قيّمة لتحديد المصدر. وتتضمّن الاستخبارات الشاملة على سبيل المثال لا الحصر استخبارات الإشارات (SIGINT) والاستخبارات البشرية (HUMINT) واستخبارات المصادر المفتوحة (OSINT). وقد لا تكون هذه القدرات واسعة الانتشار على الصعيد العالمي ويُعتقد أن عددًا قليلًا جدًا من البلدان يمتلك قدرات شاملة متطوّرة. ومع بعض الاستثناءات البارزة لا تتم مشاركة هذه القدرات والمعلومات المستقاة منها عن طيب خاطر.[3]

وتنتج استخبارات الإشارات (SIGINT) عن طريق جمع الإشارات والبيانات من أنظمة تكنولوجيا الاتصالات والمعلومات وتحليلها (وكالة الأمن القومي (National Security Agency)، 2016). وإذا توفّرت هذه الأنواع من البيانات للباحثين الإلكترونيين فقد تضطلع بقيمة كبيرة لأنها تعطي لمحةً عن أفعال المهاجمين الإلكترونيين وعن نواياهم أيضًا. فمثلًا إذا تمتّعت الحكومة بالقدرة على جمع الإشارات في الشبكات التي استُخدمت في الهجوم ستتمكن هذه الحكومة من التحقق من الحركة المرتبطة بها للمساعدة على اكتشاف مصدر الهجوم. وفي حال تواصل أيضًا المهاجمون عبر الشبكات عينها تستطيع هذه الحكومة على ما يبدو الحصول على معلومات بشأن الهجوم عبر فحص الاتصالات المتعلقة بالهجوم التي قد تعطي أدلة بشأن المصدر.

وتنتج الاستخبارات البشرية (HUMINT) عن طريق جمع المعلومات من الأشخاص وتحليلها. وفي سيناريو الهجوم الإلكتروني قد يستخلص جامع الاستخبارات البشرية (HUMINT) المعلومات من أشخاص يظن أنهم قد يقدّمون معلومات مفيدة حول الهجوم. مثلًا إذا تمكن جامع الاستخبارات البشرية (HUMINT) من الوصول إلى مصدر في حكومة يشتبه بأنها مسؤولة عن الهجوم الإلكتروني فقد يحمل جامع هذه الاستخبارات المصدر على الإفصاح عن معلومات بشأن الهجوم أو اكتشاف معلومات إضافية لدعم تحديد المصدر.

وتفوق كمية وجودة البيانات التي تجمعها بعض الدول ذات القدرات الاستخباراتية المتطورة تلك التي تجمعها الشركات الخاصة. ولكن من الضروري

[3] يشكّل تحالف فايف آيز (5-Eyes) الذي يقوم على مشاركة المعلومات الاستخباراتية بين الولايات المتحدة وكندا والمملكة المتحدة ونيوزلندا وأستراليا أحد أبرز الاستثناءات. للمزيد من المعلومات انظر فاريل (Farrell) (2015).

الإشارة إلى أن الشركات الخاصة قد تمتلك القدرة على جمع المعلومات المماثلة في سياق عملها. في الواقع قد تتمكن الشركة الخاصة التي تقوم بأعمال حول العالم من الوصول إلى مجموعة أكثر تنوعًا من البيانات والأشخاص عن تلك المتاحة أمام حكومة "متدنية المستوى" قدراتها الاستخباراتية ضعيفة جدًا.[4] وعلى سبيل المثال في تقرير صدر عام 2014 تبيّن لمنظمة اختبار البرمجيات المستقلة آي في كومباراتيفز (AV Comparatives) أن بعض شركات البرمجيات المضادة للفيروسات الرائجة تجمع بيانات متعلقة بالمضيف والشبكة والبرمجيات والملفات حتى عندما لا تكون الملفات خبيثة (آي في كومباراتيفز (AV Comparatives)، 2014). وقد تشبه البيانات التي تجمعها هذه الشركات التي تعمل في مجال مضادات الفيروسات البيانات التي تستهدفها المنظمات الاستخباراتية. وقد تحتل هذه الكيانات التي تنتمي إلى القطاع الخاص مثل مزوّدي خدمة الإنترنت وشركات الاتصالات وشركات وسائل التواصل الاجتماعي مكانة خاصة للوصول إلى أدلة شاملة ذات قيمة ومشاركتها. وقد أطلق موقع فيسبوك (Facebook) في عام 2015 منصّة رحّبت "بالشركات الموثوقة" للإسهام ببيانات عالية الموثوقية حول التهديدات المُكتشَفة في شبكاتها. واعتبارًا من تشرين الثاني (نوفمبر) 2016 ضمّت المنصة أكثر من 450 عضوًا مشاركًا. وبالاستجابة إلى الطلب أطلقت شركات مثل آليين فولت (AlienVault) وسولترا (Soltra) منصات مماثلة لتبادل التهديدات.[5] وبالفعل قد تحتاج الحكومة في الحالات التي تضّطر فيها إلى ملء الثغرات الاستخبارية إلى الاستعانة بالقطاع الخاص للحصول على البيانات سواء عن طريق التعاون الطوعي أو إرغام الشركات على توفيرها.[6]

وفي حين تشمل استخبارات الإشارات والاستخبارات البشرية معلومات غالبًا ما تبقى طي الكتمان تنتج استخبارات المصادر المفتوحة وتُحلّل عن طريق جمع المعلومات من المصادر المتاحة المفتوحة كالإنترنت ومعالجتها. وكما هو الحال مع استخبارات الإشارات والاستخبارات البشرية تستطيع تقنيات جمع استخبارات المصادر المفتوحة وتحليلها دعم تحديد المصدر. ويستطيع الباحثون تحليل ما يُنشر على وسائل التواصل الاجتماعي وتصفّح مواقع الشبكة المظلمة[7] (DarkNet) المتعلّقة بجرائم الإنترنت وخدمات موارد الاستعلام عبر شبكة الإنترنت مثل هو إز[8] (WHOIS) لوضع توصيفات للمهاجمين واكتشاف معلومات تساعد في التحقيق. وقد تجمع منظمات أخرى بالفعل وتحلّل البيانات المتعلقة بالهجمات الإلكترونية وتتيحها للجميع. فعلى سبيل المثال أعلن مؤخرًا محرّك البحث المتاح للعموم شودان (Shodan) عن ميزة تسمح للباحثين

[4] يحدّد مجلس الدفاع المعني بالشؤون العلمية (Defense Science Board) ستة مستويات لتمثيل القدرة المتزايدة على استخدام التدابير الإلكترونية الهجومية والموارد الاستخباراتية لتنفيذ عمليات هجومية. إن تعليقاتنا بشأن قدرات القطاع الخاص مقارنة بالمعلومات الاستخباراتية موجّهة نحو البلدان ذات المستويات المتدنية التي تتمتّع بقدرات محدودة. انظر مجلس الدفاع المعني بالشؤون العلمية (2013).

[5] انظر مثلًا "وثائق تبادل التهديدات" (ThreatExchange Documentation) (غير مؤرّخ)، كينيدي (Kennedy 2016)، و"آليين فولت أوسيم" (AlienVault Ossim) (غير مؤرّخ)، وسولترا (Soltra) (غير مؤرّخ).

[6] إن قانون عام 2008 لمراقبة الاستخبارات الأجنبية (FISA) المعدَّل في الولايات المتحدة هو مثال على ذلك (مجلس النواب الأمريكي، 2008).

[7] للمزيد من المعلومات حول الشبكة المظلمة، انظر مكتب التحقيقات الفيدرالي (2016).

[8] هو إز (WHOIS) هو نظام يوفر معلومات حول أسماء النطاقات وعناوين بروتوكول الإنترنت (هيئة الإنترنت للأسماء والأرقام المخصصة [الآيكان]، غير مؤرّخ).

باكتشاف خوادم البرمجيات الخبيثة.[9] وإذا نجحت الشركات الخاصة في جمع المعلومات المفتوحة المصدر واستغلالها وتعزيز استخباراتها من خلال البيانات من الشبكات والأجهزة والمنظمات التي تقدم لها الخدمات فقد تحظى بقدرات تفوق تلك التي تتمتّع بها بعض الدول لتحليل الأدلة المحتملة بفعالية.

ربط المؤشرات ببعضها

يحتاج التحقيق في تحديد مصدر الهجمات الإلكترونية إلى تفسير الأدلة المتوفرة كافة وتقييمها وتحديد أهميتها. ويحتاج المحققون أيضًا إلى ربط المؤشرات بمختلف الحوادث. فالمعتدون الإلكترونيون يعيدون استخدام الترميز والبنية التحتية من هجوم إلى آخر. ويعني ذلك في حالة بنية (C2) أن عناصر البرمجيات المشتركة مثل أدوات الوصول عن بعد ستُستخدم للحفاظ على روابط دائمة بين مختلف الحوادث. وقد اكتُشفت أشكال متغيّرة لفيروس بلاك إنرجي (BlackEnergy Trojan) من نوع حصان طروادة في هجمات متنوعة شهدتها بلدان مختلفة منذ عام 2008 (بومغارتنر وغارنيفا (Baumgartner and Garnaeva)، 2014؛ غرايت (GReAT)، 2016). وتعني أيضًا إعادة استخدام البرمجيات أن السلاسل والأختام الزمنية وغيرها من المعرّفات التي يتوقع المرء أن تكون فريدة ستظهر في هجمات متعددة وتكون بمثابة دليل على أن الهجمات مصدرها الخصم عينه. وفي أعقاب هجوم عام 2016 الذي استهدف البنك المركزي في بنغلادش اكتشف الباحثون لدى سيمانتك وكاسبرسكي لاب إعادة استخدام لترميز معيّن وربطوه بالتالي بأنشطة مجموعة لازاروس (غرايت، 2017). وربطت التحقيقات التي قامت بها شركة نوفيتا مجموعة لازاروس بهجمات متعددة في الولايات المتحدة وكوريا الجنوبية (أبرزها الهجوم على شركة سوني بيكتشرز) عن طريق روابط مشتركة مثل إعادة استخدام الترميز (فريق الأبحاث المتعلقة بالتهديدات لدى نوفيتا (NovettaThreat Research Group)، 2016). وبالإضافة إلى ذلك شمل هجوم بنغلادش سلاسل متعددة تخلّلتها أخطاء مطبعية مثل كلمة "foundation" التي كُتبت بالشكل التالي "fandation" وكلمة "already" التي كُتبت على النحو الاتي "alreay" ("أخطاء إملائية تحول دون استحواذ القراصنة على مليار دولار في عملية سطو على مصرف" (1Bn in Bank$ Spelling Mistake Prevented Hackers Taking Heist)، 2016)؛ إذا تواجدت هذه الأخطاء المطبعية المتفرّدة عينها في برمجية هجوم آخر فستشكّل دليلًا إضافيًا على هجوم ذي صلة.

ولكن كما أشرنا سابقًا من الممكن التلاعب بالمؤشرات التقنية. ومن الضروري جدًا بالتالي أن يربط محققو تحديد المصدر المؤشرات التقنية بالمؤشرات السياسية والمعلومات الشاملة المصدر بالإضافة إلى ربط المؤشرات التقنية بمختلف الحوادث. ولا بدّ أن يرتكز قرار تحديد المصدر الراسخ على تقييم شامل للأدلة المتوفرة كافة. وقد يزيد هذا الجانب من تحديد المصدر من تعقيد التحقيقات إذ قد لا يضطلع الخبراء القادرون على تقييم المؤشرات التقنية بالخبرة لتقييم المؤشرات السياسية في حين لا يملك معظم الخبراء السياسيين فهمًا كافيًا للأدلة الجنائية التقنية. وقد تبدو هذه الأنواع المختلفة من المؤشرات غير متكافئة وقد تظهر تحديات تتعلّق بالتوفيق بين الأدلة عندما تدلّ المؤشرات إلى اتجاهات مختلفة.

[9] شودان هو محرّك بحث للأجهزة المتصلة بالإنترنت. انظر شودان (Shodan) (غير مؤرّخ).

وتسلّط هذه المناقشة للمؤشرات الضوء على النوع الأول من تحديات تحديد المصدر وكيف سعى محققو تحديد المصدر إلى تخطيها. وننتقل الآن إلى تحد ثان عند تحديد المصدر.

نقل نتيجة تحديد المصدر

يتعلّق التحدي الثاني عند تحديد مصدر الهجمات الإلكترونية بمسألة نقل النتائج على نحو مقنع إلى الجمهور المستهدف. وتزداد أهمية هذا التحدي بالنسبة لمحققي تحديد المصدر الحكوميين وغير الحكوميين الذين يسعون إلى محاسبة الجهات الفاعلة الخبيثة على أفعالها. ونطرح في هذا القسم بعض العناصر المتعلقة بالنقل الموثوق من أجل مناقشة شكل التحدي وسنعود إلى هذه المواضيع لاحقًا.

ويكمن هدف النقل العلني لنتائج التحقيق في الهجوم الإلكتروني في إطلاع الرأي العام على هوية منفذي الهجوم والطرق المستخدمة. ولكن قد ينبع الإعلان عن هذه المعلومات من دوافع وعواقب أخرى. فعلى سبيل المثال قد يشجّع البيان العام لتحديد المصدر الضحايا أو غيرهم من الفئات الضعيفة على تعزيز دفاعات الشبكة. ويمكن استخدامه أيضًا لتحذير الجاني بشأن الرد الوشيك أو لإقناع مجموعة من الأطراف الثالثة بتقديم الدعم للعقوبات. وفي حالات أخرى، يوفّر البيان العام رؤية وتوعية قد تلفت نظر الرأي العام إلى الأنشطة الخبيثة ولكن لن يتم التصرّف على أساسه لغير ذلك (إدواردز وآخرون (Edwards et al.)، 2017). ويمكن تشبيه الأمر بالمدّعي العام الذي يعرض الأدلة في المحكمة لإقناع هيئة المحلّفين بأن القانون قد انتُهك وبالنسبة إلى محكمة أمريكية قد يؤدي الإقناع في تحديد المصدر إلى إدانة هيئة المحلّفين يليها إصدار حكم وإنفاذ العقوبة علمًا أن هذه الإجراءات اللاحقة (مثل إصدار الحكم أو العقوبة) لن تحدث بالضرورة.

وتوخّيًا للفعالية لا بدّ أن يتمتّع البيان العام بالموثوقية. وقد تفشل عملية تحديد المصدر التي تفتقد للموثوقية في تحقيق أي من الأهداف المباشرة أو غير المباشرة المذكورة أعلاه. وبالعودة إلى تشبيه المحكمة قد يفشل تحديد المصدر الذي يفتقد للموثوقية في التوصل إلى قرار من هيئة المحلفين يتوافق مع الأحداث الفعلية والمعايير القانونية بالرغم من تقديم أدلة دقيقة للمحلفين. مثلًا قد يؤدي التعامل غير الكفؤ مع الأدلة أو العجز عن تقديمها بشكل واضح أو أي تحيّز ذاتي ظاهر إلى فقدان واضح للموثوقية.

وتترسّخ الموثوقية من خلال عوامل متعددة. ولعل أبرزها يتمثّل بتوفّر أدلة قوية وواضحة تدعم تبرير نتيجة معينة. وإذا استطاع خبراء مستقلون آخرون مراجعة الأدلة وتقييمها وإثبات قوّتها فسيساعد ذلك على جعل الأدلة قاطعة. فبشكل عام وبمعزل عن الأدلة المحددة المتعلقة بحوادث معينة ترتبط مجموعة من العوامل بالجهة التي تُجري التحقيق. وتشمل هذه العوامل إظهار المعرفة والمهارات اللازمة للتوصّل إلى الاستنتاج الصحيح وسجلًا حافلًا بالعناية والدقة في التحقيقات السابقة وسمعة في التحليل الموضوعي والنزيه ومنهجية شفافة تشمل عملية مراجعة مستقلة. وستعكس نتائج التحقيقات

الفعّالة المتعلقة بتحديد مصدر التهديدات الإلكترونية هذه الاعتبارات وستوحي بالموثوقية في نظر الجمهور المستهدف.

أساليب الاطلاع على النتائج

تستخدم التحقيقات في الهجمات الإلكترونية وتحديد مصدرها مجموعة متنوعة من النهج لإطلاع الرأي العام على النتائج والتحليل. وتتنوّع هذه النهج من ناحية الأسلوب والتفاصيل والتوقيت. ونستعرض هنا بعض النهج المختلفة التي استُخدمت لتحديد مصدر الهجمات علنًا.

تنوّع تحديد الحكومات للمصدر بدرجة كبيرة من ناحية الشكل. فعلى سبيل المثال استُخدمت بيانات عامة رسمية رفيعة المستوى لإطلاع الرأي العام على نتيجة تحديد المصدر في حالات سوني بيكتشرز وشبكة الكهرباء الأوكرانية والهجمات التي استهدفت مجلس النواب الاتحادي الألماني (Bundestag). ونُشرت تقارير رسمية في حالات أخرى. على سبيل المثال نشر مكتب مدير الاستخبارات القومية الأمريكي في أعقاب الهجوم على اللجنة الديمقراطية الوطنية تقريرًا رسميًا يحدد فيه مصدر الهجوم (مكتب مدير الاستخبارات القومية الأمريكي، 2017) وأصدرت وزارة الأمن الوطني الأمريكية ومكتب التحقيقات الفيدرالي تقرير غريزلي ستيب (GRIZZLY STEPPE) (2016) الذي تضمّن تفاصيل تقنية بشأن الهجوم (انظر دراسة الحالة 4 ص. 34). وبالإضافة إلى ذلك أتى تحديد الحكومة للمصدر بمثابة إجراءات انتقامية رسمية في حالات أخرى (مثل اتهام مكتب التحقيقات الفيدرالي لجهات فاعلة حكومية إيرانية بوقوفها وراء هجمات القطع الموزّع للخدمة على مؤسسات مالية أمريكية).

بيد أنه في حالات أخرى لم يتّخذ تحديد الحكومة للمصدر شكل بيانات رسمية وعلنية. فعلى سبيل المثال استخدم المسؤولون الحكوميون لنقل نتائج تحديد المصدر بيانات غير رسمية وسرية وُجّهت لوسائل الإعلام الإخبارية مثل عزو الهجوم على البنك المركزي في بنغلادش إلى كوريا الشمالية في وسائل الإعلام نقلًا عن مسؤولين في مكتب التحقيقات الفدرالي (فنكل (Finkle)، 2017). وفي حالات أخرى مثل الهجمات ضد وزارة الخارجية والبيت الأبيض وستوكسنت كشفت التسريبات الحكومية عن نتائج تحديد المصدر غير الرسمية للرأي العام (غرول، 2016).

وقد اتخذت أيضًا بيانات تحديد المصدر الصادرة عن القطاع الخاص والباحثين المستقلين أشكالًا مختلفة. وقد نُشرت تقارير رسمية في حالة تحليل شركة كراودسترايك المتعلق بالهجوم على اللجنة الديمقراطية الوطنية وتقرير شركة مانديانت (Mandiant) المتعلّق بهجوم مجموعة التهديد المتواصل المتطور 1 (ATP1). وساعد الصحافيون الاستقصائيون ولا سيّما دافيد سانجر (David Sanger) الذي عمل على التحقيق في هجوم ستوكسنت وتحديد مصدره لدى صحيفة نيويورك تايمز (New York Times) على نشر وإتاحة نتائج تحديد المصدر التي تستند إلى البحث المستقل والمحادثات السرية. كذلك قدّم أيضًا الباحثون المستقلون نتائج تحديد المصدر والأدلة بطرق أخرى متنوّعة وغير رسمية بما في ذلك المدونات والنشر على وسائل التواصل الاجتماعي. وبهذه الطريقة حُدّدت المصادر عن طريق الروابط بين التقارير المنشورة والبحث غير

الرسمي. فعلى سبيل المثال بينما ربط تقرير عملية أوبريشن بلوكباستر حول هجوم سوني بيكتشرز الذي أُجري عن طريق تعاون بين شركات خاصة ترأسته نوفيتا الهجوم بمجموعة لازاروس، ربطت في الوقت عينه تقارير غير رسمية هذه المجموعة بكوريا الشمالية. وقد استُخدم النوع عينه من الربط غير الرسمي في أعقاب الهجوم على البنك المركزي في بنغلادش عندما ربط خبر نشرته مدونة سيمانتك الرسمية (2016) الهجوم بمجموعة لازاروس (وبالتالي كوريا الشمالية).

وبالرغم من الغموض الذي يلف الأسباب المحيطة باختلاف طرق الاطلاع ودرجة الموثوقية الضمنية المرتبطة بكل منها يخلّف استخدام طرق الاطلاع المختلفة آثارًا على الثقة العامة في قرارات تحديد المصدر.

الرؤى الرئيسية حول تحديد مصدر الهجمات الإلكترونية

نستخلص من استعراض الحالات المذكورة أعلاه رؤى متعددة حول الوضع الراهن لتحديد مصدر الهجمات الإلكترونية. ويلعب القطاع الخاص دورًا جوهريًا في التحقيق في الحوادث وتقدير مصادرها. إلا أن كيانات القطاع الخاص تمتلك حوافزها المالية المستقلة الخاصة لإصدار تقارير تحديد مصدر رفيعة المستوى. وحتى إذا جمع بين الشركات هدف مشترك في تحديد التهديدات والتخفيف من حدّتها فهي لا تتشارك الأطر التي تسهل مقارنتها ما يؤدي إلى تناقضات مثل التسميات المتنوّعة. وتستخدم أيضًا بعض الحكومات التي تتمتّع بقدرات تحديد المصدر أطرًا بحثية غير شفافة خاصة بها. وفي المناسبات النادرة التي تحدد فيها الحكومات علنًا مصدر التهديدات الإلكترونية المزعومة غالبًا ما تُعتبر بياناتها سياسية بحتة. وبما أنها لا تشارك غالبًا بطريقة رسمية تفاصيل التحقيق التي استندت إليها استنتاجاتها تصبح هذه الاستنتاجات عرضة للتشكيك بسهولة. وفي النهاية لا يشكّل المشهد الحالي المجزّأ لأبحاث الأمن الإلكتروني بيئة صديقة لضحايا الهجمات الإلكترونية. فضحايا الهجمات الكبرى لا يسعون دائمًا للحصول على دعم خارجي مباشرة بعد الحادث لأن عددًا كبيرًا من هؤلاء الضحايا لا يستطيعون تحمّل كلفة المساعدة لتحديد مصدر الهجمات الإلكترونية أو لا يعرفون ممن يلتمسون المساعدة. وقد يزداد هذا التحفّظ في غياب منظمة مستقلّة تسعى إلى توافق الآراء بين الشركات والمنهجيات المتعددة.

نهج الحملة ضروري

كما الضحايا يُعاد استخدام البنية التحتية والثغرات التي استُفيد منها في الهجمات السابقة مرارًا فيتمكن حينها المحقّقون من ربط حوادث مختلفة بالجهات الفاعلة عينها. وبعبارات أخرى تؤثّر التحقيقات السابقة في التقييمات الحالية لتحديد المصدر ولا بد أن تتعقّب التحقيقات الجهات الفاعلة في مختلف مراحل أنشطتها المتنوّعة وربما يستغرق الأمر عدة سنوات. ويشير ذلك إلى ضرورة اتّباع المحقق في تحديد المصدر نهج "حملة" ثابت في تحقيقاته يفرض النظر في حوادث إلكترونية متعددة في خلال عملية تحديد الجهة المسؤولة. وعلى الرغم من أن الجهات الفاعلة المتطورة ستبذل قصارى جهدها لتغيير الطرق والتقنيات التي تعتمدها للثغرات كي تتجنّب كشفها، لن يكون ذلك ممكنًا على الدوام وسيزيد من تكاليف شنّ الهجمات. ونظرًا لأهمية نهج الحملة،

تكتسب كيانات تحديد المصدر الحالية التي تحتفظ بقاعدة بيانات متاحة وسهلة التحديث بدلًا من التئام المحققين المستقلين في كل حالة على حدة قيمة كبرى.

وستؤثّر أيضًا ضرورة اعتماد نهج الحملة في كيفية إدارة منظمة تحديد المصدر للمعلومات المتعلّقة بالهجمات مع مرور الزمن. وستحتاج منظمة تحديد المصدر على وجه الخصوص إلى إنشاء نظام رسمي للتسمية للتمكن من اعتماد الهجمات مرجعًا على الصعيد العالمي في التحقيقات المستقبلية. وبالإضافة إلى ذلك قد يستفيد توصيف الهجمات الإلكترونية من نهج رسمي مخصص لوصف الهجمات من حيث نوع الاستغلال وحدّته وخصائص أخرى. مثلًا قد تعود توصيفات الحدة المتواصلة بالنفع في حال كُلّفت هيئة مستقلة بالتوصية باتخاذ إجراءات عقابية بحق الأطراف المسؤولية.

قد يؤدي التقسيم بين الباحثين إلى الارتباك

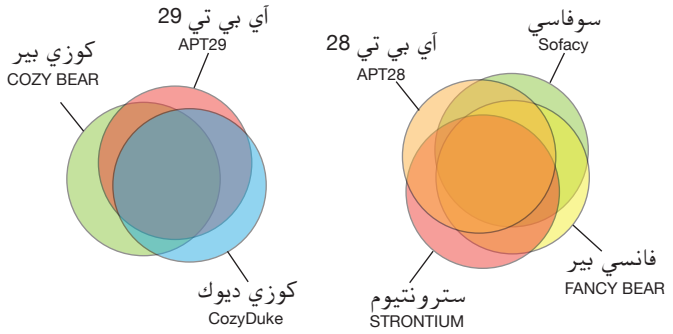
ازداد التعاون وتشارك المعرفة بين الباحثين في مجال الأمن الإلكتروني ولكنه لم يصبح طريقة العمل المعيارية بعد. فقد نتج عن غياب قاعدة معارف مشتركة تناقضات في نهج التحقيق وطرق الشركات المختلفة. فعلى سبيل المثال أشارت شركة كاسبرسكي لاب إلى أن التحليل الذي أجرته شركتا بي آي إي (BAE) وأنومالي (Anomali) للعلاقة بين مجموعة لازاروس المرتبطة بكوريا الشمالية وعملية السطو على البنك المركزي في بنغلادش قد ركّز بشكل دقيق على ترميز أداة "وايبر" (Wiper). وعلى نحو مماثل أشارت كاسبرسكي إلى أن شركة سيمانتك قد ورّطت مجموعة لازاروس عبر تحديد إعادة استخدام لسلسلة برمجية خبيثة في الهجوم على القطاع المالي البولندي (غرايت، 2017). وتُظهر الأمثلة المشابهة أن هيئة البحث الحالية لا تحدد على نحو ثابت هذه الجهات الفاعلة وتكتيكاتها وتقنياتها وإجراءاتها لأن البحث قد أجرته منظمات متعددة أتيحت لكل منها البيانات الهامة والخبرات بمستويات متفاوتة وفصلت أحيانًا بين التقييمات سنوات طويلة. وقد تعود بالتالي المجموعة المشتركة من أدوات وطرق البحث المتعلقة بالأمن الإلكتروني بالنفع على التحقيقات المستقبلية ولا سيّما في الحالات التي تشمل جهات فاعلة إلكترونية تنفّذ هجمات منتظمة.

وتملك الشركات الخاصة مصالح اقتصادية في التحقيق في الحوادث وتحديد مصادر الهجمات وثمة حوافز لنشر النتائج بأسرع وقت ممكن وبطريقة رفيعة المستوى مثل التسويق للعملاء المستقبليين. وقد يكون لشركات أخرى منافسة دوافع لرفض نتائج منافسيهم وتقديم فرضيات أخرى بديلة. وبدون منهجية موحّدة أو حتى التزام على مستوى القطاع بالتقيّد بمنهجية صارمة تشمل مراجعة مستقلة قد يؤدي ذلك إلى تكوين صورة مربكة لدى غير الخبراء.

ويزيد من تعقيد طبيعة مجموعة المعارف الحالية المجزّأة اعتماد شركات القطاع الخاص ووكالات الاستخبارات الحكومية تسميات مختلفة للتهديدات الإلكترونية موضع البحث ما يؤدي إلى مصطلحات تسمية مختلفة للتهديدات المتواصلة المتطورة الشائعة. ويعرض الشكل 1 مصطلحات التسمية المختلفة المستخدمة حاليًا لتهديديْن متواصليْن متطوّريْن رئيسيين. فعلى سبيل المثال يُعرف التهديد المتواصل المتطوّر الذي ربطه بعض الباحثين بمديرية المخابرات

الشكل 1

تسميات متعددة متعارف عليها للتهديدات المتواصلة المتطورة



الرئيسية في روسيا (GRU) باسم سوفاسي (Sofacy) لدى كاسبرسكي وآي بي تي 28 لدى فاير آي وسترونتيوم (STRONTIUM) لدى مايكروسوفت وفانسي بير (FANCY BEAR) لدى كراودسترايك. وتُطلق شركة فاير آي اسم آي بي تي 29 على تهديد متواصل متطوّر آخر ربطه البعض بدائرة الأمن الاتحادي في روسيا (FSB) ولكنه يُعرف باسم كوزي ديوك (CozyDuke) لدى أف سيكيور (F-Secure) وكوزي بير (COZY BEAR) لدى كراودسترايك. ويعدّد تقرير التحليل المشترك غريزلي ستيب حول النشاط الإلكتروني الروسي الخبيث *(GRIZZLY STEPPE—Russian Malicious Cyber Activity)* (وزارة الأمن الوطني الأمريكية ومكتب التحقيقات الفيدرالي، 2016) حوالى 50 اسمًا بديلًا لأجهزة الاستخبارات العسكرية والمدنية الروسية المفاد عنها. ويهدف رسما فين (Venn) البيانيان مع أقسامهما المتداخلة جزئيًا في الشكل 1 إلى الإشارة إلى أن أسماء متعددة للتهديدات المتواصلة المتطورة قد ترتكز على مؤشرات متشابهة ولكنها ليست متطابقة. وحتى لو تداخلت مصطلحات التسمية هذه نوعًا ما فقد تسبّب ارتباكًا في صفوف السياسيين والمحللين السياسيين والرأي العام الذين يواجهون بالفعل صعوبة في تفسير نتائج عملية تحديد المصدر المعقدة من الناحية التقنية.

غالبًا ما تكون المزاعم الحكومية لتحديد المصدر سياسية ومبهمة

قد تعتبر الحكومات الهجمات الإلكترونية التي تستهدف مواطنيها ومنظماتها وقطاعاتها كهجمات تستدعي الردّ. وعلى هذا النحو قد تجري الحكومة الضحية تحقيقًا وتزعم تحديد المصدر من طرف واحد عن طريق تحديد هوية المهاجم المزعوم علنًا في محاولة "لتسميته والتشهير به" ولتجهيز أنشطة دفاعات الشبكة اللاحقة وفرض التكاليف. إلا أن هذه المزاعم العلنية لتحديد المصدر لم تصدر أو تنفَّذ بشكل منتظم. وفي ظل الهجمات الإلكترونية المتعددة حددت الحكومات المصدر علنًا في عدد قليل جدًا من الحالات ليس إلا. وبالرغم من ادّعاء المسؤولين الصينيين بأنهم يتعرّضون لهجمات إلكترونية منتظمة فقد أشاروا إلى أن تحديد المصدر يكاد يكون مستحيلًا (سولمايير وشانغ (Sulmeyer and Chang)، 2017؛ سيغال (Segal)، 2017). وفي الحالات النادرة التي تعلن فيها الحكومات عن تحديد المصدر تصدر البيانات عن مستويات حكومية مختلفة ومع مستويات مختلفة من الرسمية وعن طريق

مجموعة متنوعة من الوسائل. وغالبًا ما ترفض الحكومة مشاركة المعلومات التي دفعتها إلى استنتاجاتها من أجل حماية المصادر والطرق الحساسة. وفي حالات أخرى يتكهّن المسؤولون الحكوميون بشكل عام بشأن مصدر الهجوم وأحيانًا قبل إجراء التحقيق حتى.

وفي أعقاب الهجوم على سوني بيكتشرز والاختراقات التي تعرّضت لها اللجنة الديمقراطية الوطنية حدّدت الحكومة الأمريكية علنًا المصدر عن طريق تصريحات الوزراء أو الرئيس. وتقرر جزئيًا نظرة المرء إلى موثوقية هؤلاء المسؤولين ما إذا كانت هذه التصريحات مقنعة أم لا. وصدرت فضلًا عن ذلك تقارير تحليلية تقنية. ولكن لم تشمل هذه التصريحات معلومات بشأن الأدلة وخضعت للتدقيق العام والمطالبة بمعرفة الأدلة المستندة إليها.[10] فقد صدرت أيضًا بعد مرور أشهر على الحادث الأساسي وبعدما قدّم باحثون آخرون في مجال الأمن الإلكتروني وجهات نظرهم العلنية بوقت طويل. وفي حالات أخرى عزت الحكومة الأمريكية علنًا الحوادث الإلكترونية للجهات الفاعلة الحكومية الصينية والإيرانية والروسية من خلال اتهامات أطلقتها أجهزة إنفاذ القانون ولكنها لم توفّر أيضًا أدلة تُذكر من التي استندت إليها النتائج (وزارة العدل الأمريكية 2014؛ 2016؛ 2017). وبما أن الجهات الفاعلة المتهمة لن تُسلَّم على الأرجح ولن تعتقلها أجهزة إنفاذ القانون الأمريكية تطرح هذه الاتهامات تساؤلات حول الغاية منها وفعاليتها. وفي حالة الهجوم على المكتب الأمريكي لإدارة شؤون الموظفين لم تحدد بعد حكومة الولايات المتحدة علنًا أي مصادر مزعومة بالرغم من التصور الراسخ بشأن مسؤولية الجهات الفاعلة الحكومية الصينية عن الهجوم.

ولا تتفرّد الولايات المتحدة في مسألة نشر تحديد المصدر بدون الكشف عن الأدلة. فالبلدان الأخرى تحدد بانتظام المصادر المزعومة بدون دعم النتائج بأدلة واضحة. في مسألة ألقت دائرة أمن أوكرانيا (SBU) علنًا باللائمة على الحكومة الروسية لوقوفها وراء الهجوم الإلكتروني على شبكة الكهرباء الأوكرانية في عام 2015 حتى قبل أن تشكّل وزارة الطاقة الأوكرانية لجنة خاصة للتحقيق (بوليتيوك (Polityuk)، 2015). واتّهمت عناصر مختلفة من حكومة بنغلادش مجموعة من الجهات الفاعلة بتنفيذ الهجوم على البنك المركزي. ويتسبب تحديد المسؤولين الحكوميين العلني للمصدر بدون أدلة شاملة في تشويش تحديد المصدر المزعوم ويشكّل تشكيكًا في الموثوقية.

ولكن هذا النوع من التحدي الذي تواجهه الموثوقية لا يقتصر على الحكومات فحسب. فقد أفادت تقارير عن ارتباط بعض أبرز شركات الأمن الإلكتروني الخاصة بوكالات حكومية. ومن الأمثلة على ذلك ما تعرضت له شركة كاسبرسكي لاب من اتهامات بالتغاضي عن الهجمات الروسية المشتبه بها (ماتلاك ورايلي وروبرتسون (Matlack, Riley, and Robertson)، 2015؛ وشاكتمان (Shachtman)، 2012). وعلى نحو مماثل حصلت شركة فاير آي على تمويل جزئي من صندوق الاستثمار إن كيو تيل (In-Q-Tel) التابع لوكالة الاستخبارات المركزية (CIA) وقد أعرب رئيسها التنفيذي عن تحفظات بشأن نشر الهجمات المدعومة من الولايات المتحدة (يادرون (Yadron)، 2015).

[10] أثارت مجموعة متنوعة من الخبراء مثل لي (2016) (Lee) وديبرت (2017) (Deibert) المشاكل المحيطة بتقرير غريزلي ستيب. في ما يتعلّق بشكوك الباحثين في مجال الأمن حول سوني انظر روجرز ((Rogers 2014)).

ويؤدي تولّي شركة واحدة فقط التحقيق في هجوم خلّف تداعيات جغرافية سياسية إلى طرح تساؤلات بشأن تحيّز التحديد العلني للمصدر.

واقترح بعض المعلقين أنه ينبغي على الحكومات نشر نتائج تحديد المصدر على نحو منتظم وسريع باعتباره مسألة سياسية روتينية. وعلى الرغم من أن هذا الأمر قد ينظّم مزاعم تحديد المصدر ويجعلها أقل تخصصًا يفتقد الكثير إن لم يكن معظم الحكومات للخبرة التقنية الأساسية والقدرة الاستخباراتية والموارد الأخرى لإجراء تحقيقاتها الخاصة. وبالإضافة إلى ذلك ترددت الحكومات في القيام بتصريحات عامة لأنها ستواجه ضغوطًا للرد بفعالية وبطريقة علنية ما إن تحدد الطرف المسؤول ويشكّل هذا الأمر تحديًا حتى بالنسبة للدول ذات القدرات العالية.

وتشير هذه المسائل إلى أن الحكومات قد لا تكون الخيار الأمثل والأكثر مصداقية للإعلان عن نتائج تحديد المصدر. وتزداد حدّة هذا التحدّي في المناخ الحالي من انعدام ثقة الناس بالمؤسسات السياسية.

التعاون ضمن القطاع الخاص مفيد

غالبًا ما يعتمد ضحايا الهجمات الإلكترونية على شركات القطاع الخاص لإجراء التحقيقات. وعندما تعمل شركات الأمن الإلكتروني التابعة للقطاع الخاص بمفردها لتحديد مصدر الهجوم بالنيابة عن ضحية ما يتمثّل الخطر بأن تحفّزها الدوافع المالية على إصدار الأحكام السريعة في ما يتعلّق بمصادر الهجمات بغض النظر عن الأدلة المستندة إليها. ولا تقوم الشركات التي تعمل بشكل مستقل أيضًا بمراجعة مستقلة وقد تخضع لنفوذ السلطات الحكومية (لين، 2016). وقد يؤدي التعاون بين مجموعة كبيرة من شركات الأمن الإلكتروني في القطاع الخاص إلى تجاوز هذه التحديات من خلال مراجعة خارجية ومراقبة إضافية للجودة. وثمة أمثلة كثيرة عن التعاون الرسمي وغير الرسمي بين الشركات المتنافسة وقد ساعد هذا التعاون ومشاركة المعلومات على تعزيز الأمن الإلكتروني الأوسع نطاقًا. وقد يستفيد التحليل المرتكز على ما سبقه والتعاون الرسمي من الكفاءات الأساسية الموزعة على مختلف الباحثين وإنشاء منصة لدراسة الأدلة على نحو دقيق.

وتشمل حالات التعاون غير الرسمي بين شركات الأمن الإلكتروني اعتماد طرق موّحدة ومشاركة خصائص البرمجيات الخبيثة ودالات التجزئة الخاصة بها. فعلى سبيل المثال ازداد عدد أعضاء قاموس الضعف والتعرّض المشترك (CVE) من 29 عضوًا في عام 2000 إلى أكثر من 150 اليوم.[11] وعلى نحو مماثل تستخدم العشرات من شركات الأمن الإلكتروني الكبرى مثل كراودسترايك وسيمانتك وكاسبرسكي لاب أداة يارا (YARA) (يارا، غير مؤرّخ).

وقد تؤدي حالات التعاون الرسمي أو التعاون المرتكز على ما سبقه إلى تبسيط المهام القائمة على الكفاءات الأساسية وإلى نتيجة نهائية مستندة إلى تحليل متعدد الأطراف. على سبيل المثال اكتشفت شركة أمن صغيرة نسبيًا دودة

[11] وفقًا لموقع الضعف والتعرّض المشترك (CVE) الإلكتروني، شاركت 29 منظمة في إعلانات المطابقة في كانون الأول (ديسمبر) 2000. وفي عام 2017 ضم الموقع الإلكتروني أكثر من 150 منظمة (الضعف والتعرّض المشترك، 2017).

ستوكسنت ولكنّ هذا الاكتشاف تحول إلى جهد عالمي النطاق انتشر بين شركات متعددة ذات كفاءات أساسية مختلفة: أصدرت مايكروسوفت برامج الرقع (Patch) لإصلاح نظام التشغيل وحللت شركات مضادات الفيروسات مثل سيمانتك الترميز ونشرت خصائص البرمجيات الخبيثة ونشرت شركات أمن أخرى تقييمات مفيدة على شبكة الإنترنت. وتشكّل عملية أوبريشن بلوكباستر (انظر دراسة الحالة 5 ص. 42) نموذجًا منفصلًا لا عن كيفية قبول الشركات الخاصة بالعمل معًا لبناء مجموعة معارف حول التهديد الإلكتروني الخطير فحسب بل عن كيفية دعم النهج التعاوني لتحديد المصدر على مستوى الدولة حتى لو لم يكن ذلك الهدف المتوخّى من الجهود (فريق الأبحاث المتعلقة بالتهديدات لدى نوفيتا، 2016).

الانتقال من الرؤية إلى العمل

تشير هذه الرؤى بشأن ممارسة تحديد المصدر إلى صورة فوضوية في ما يتعلّق بالتحديد العلني للمصدر حاليًا. وقد سعت مجموعة متنوعة من الجهات الفاعلة إلى إصدار بيانات حول تحديد المصدر ولكن تحيط الشكوك بكفاءتها التقنية ونزاهتها وموضوعيتها.

ويزيد غياب المنهجية التوافقية والمعايير لتحديد المصدر من صعوبة تقييم مؤهلات مزاعم تحديد المصدر. وفي الماضي صُمّمت المزاعم الحكومية للتحديد العلني للمصدر خصيصًا لتحقيق أهداف محدودة وهي تستند إلى معلومات محدودة نُشرت علنًا. وتمكّن هذه البيئة غير المنظمة الجهات الفاعلة الخبيثة من إخفاء أثرها بسهولة أكبر بين الأحكام المتباينة التي لا تُعدّ ولا تُحصى. وتدلّ هذه الرؤى الرئيسية على أهمية النهج التعاوني والموحّد لتحقيقات تحديد المصدر والإعلان العام كما سيتّضح في الفصل التالي. وسيرتكز الفصل الخامس على هذه الرؤى لاستكشاف السمات الأساسية الخاصة بمنظمة مستقلة لتحديد مصدر الهجمات الإلكترونية.

نحو اتحاد عالمي لتحديد مصدر الهجمات الإلكترونية

وصف

النقاش الآنف مشهدًا مجزأ لتحديد مصدر الهجمات الإلكترونية يشمل مجموعة من الجهات الفاعلة التي تعمل انطلاقًا من عدد من الأطر وتنشر نتائجها على نطاق واسع. وفي حين عملت هذه الجهات الفاعلة بشكل مستقل عمومًا إلاّ أنها تعاونت أيضًا في حالات محددة. وبالإضافة إلى أمثلة فعلية عن التعاون قُدّمت اقتراحات بشأن أنواع جديدة من الآليات الرسمية واقترحت على وجه الخصوص مايكروسوفت ومؤلفو دراسة حول المجلس الأطلسي تأسيس هيئة لتحديد المصدر أشبه بالوكالة الدولية للطاقة الذرية. (سميث (Smith)، 2017؛ هيلي وآخرون، 2014).[1]

برزت اقتراحات متعددة بشأن تأسيس هيئة لتحديد مصدر الهجمات الإلكترونية ومن بينها هيئة أشبه بالوكالة الدولية للطاقة الذرية.

ويعرض الشكل 2 مجموعة من النهج البديلة للتحقيقات التعاونية في تحديد المصدر وكيفية تطبيق هذه النهج على الحوادث الإلكترونية في الماضي أو إمكانية تطبيقها على حوادث إلكترونية في المستقبل. وينقسم المحور العمودي في الشكل إلى ثلاث فئات تمثّل مشاركة الجهات في تحقيق لتحديد المصدر: جهات من الدول (حكومية) جهات غير حكومية أو الاثنتين معًا. ويمثّل المحور الأفقي درجة التعاون المستدام والرسمي بين جهتين أو أكثر تجريان تحقيقًا لتحديد المصدر. ويشمل الشكل أيضًا عيّنة من التحقيقات في تحديد مصدر حوادث إلكترونية مع اسم الحادث وتليه الجهات التي تولّت التحقيق فيه بين هلالين. وبالنسبة إلى كيانات التحقيق غير الموجودة بعد (المقترحة) أو جهات التحقيق التي لم تطبّق على حادث يذكره هذا التقرير، فلا نذكر سوى أسماء الجهاتبين هلالين بدون اسم الحادث المتعلق بها. ونذكر مثلًا التهديد المتواصل المتطور 1 الذي يكاد لا ينطوي على تعاون مستدام ورسمي لأن شركة مانديانت (التي اشترتها لاحقًا فاير آي) أجرت باعتبارها شركة خاصة تحليلها الخاص وأطلقت التسمية على الحادث باعتبارها شركة رسمي محدود (انظر دراسة الحالة 3 صفحة 28). وشمل فيروس ستوكسنت بدرجة كبيرة تحليلًا على يد باحثين من سيمانتك ولكن بما أن الشركة استفادت من اكتشاف الفيروس الذي توصّل إليه سيرغاي أولاسن (Sergey

[1] اقترح عدد من الكتاب في دراسة صدرت عن المجلس الأطلسي في عام 2014 إنشاء مجلس متعدد الأطراف للنظر في تحديد مصدر الهجمات الإلكترونية ويقوم بتوفير آلية دولية من أجل توصل الدول بالإجماع إلى تحديد مصدر الحملات الإلكترونية غير المشروعة فضلًا عن عملية رسمية للنظر في النزاعات بين الدول ذات الصلة (هيلي وآخرون، 2014). ونوقش أيضًا اقتراح مايكروسوفت في شارني وآخرون (Charney et al.) (2016). وتطرّق أيضًا تقرير لمؤسسة RAND في عام 2016 إلى الخيارات والتحديات المتعلقة بآليات تحديد المصدر الرسمية، انظر هارولد وآخرون (2016) (Harold et al.).

الشكل 2
خيارات للتحقيقات التعاونية لتحديد مصادر التهديد

RAND *RR2081-2*

Ulasen) الذي لم يكن موظفًا لديها بالإضافة إلى المدخلات المخصصة من شركات التحكّم الصناعي فقد نقلنا موقعها قليلًا إلى يمين التهديد المتواصل المتطور 1. وفي حين حقّقت الشركات الخاصة المتنوعة في كيفية تنفيذ دودة ستوكسنت أعلن الصحافي الاستقصائي في نيويورك تايمز دايفد سانجر (2012) الذي ارتكز عمله جزئيًا على الأرجح على تسريبات (سُمح بها بشكل غير رسمي ربما) مع غيره من المصادر عن تحديد إسرائيل والولايات المتحدة مصدرًا للهجوم. وتشكّل منظمة أوبريشن بلوكباستر مثالاً آخر إذ أجرت تحقيقًا تعاونيًا في قرصنة شركة سوني بكتشرز ولكن هذا التعاون لم يُطبّق بعد على حادث آخر بشكل علني.

ويشير تحليلنا إلى أهمية النهج التعاوني لتحديد المصدر وإلى أهمية النموذج الرسمي لتسهيل نهج الحملة وإلى أهمية هيئة دائمة تختار الحالات للتحقيق فيها عبر عملية معيارية وشفافة. وأخيرًا يشير تحليلنا إلى أنه على الرغم من توفير الدول قدرات استخباراتية فريدة لتحديد المصدر فإن مشاركتها قد تؤدّي إلى مضاعفات تؤثّر سلبًا في موضوعية النتيجة وشفافيتها واستقلاليتها. لذا نعرض نموذجنا المقترح في أعلى الشكل 2 إلى اليمين والذي يشير إلى مشاركة غير حكومية في تعاون مستدام ورسمي.

ولا يحدد الشكل 2 الأساليب كافة التي استخدمتها الجهات الفاعلة الحكومية وغير الحكومية في العمل على تحديد مصدر الهجمات الإلكترونية. على

سبيل المثال قامت المنظمة الدولية للشرطة الجنائية (الإنتربول) بمجموعة من المبادرات لتسهيل التعاون الدولي من أجل مكافحة الجرائم الإلكترونية بما في ذلك مشاركة الممارسات الفضلى التي تساعد أجهزة إنفاذ القانون على تخطي تحديات تحديد المصدر (الإنتربول، 2016). ولا بدّ أيضًا من ذكر اتفاقية بودابست لمكافحة جرائم المعلوماتية (Budapest Convention on Cybercrime) ودورها في التحقيق في الجرائم الإلكترونية التي طالت دول متعددة. وتنسّق هذه الاتفاقية التي اعتمدتها 56 دولة (اعتبارًا من كانون الأول (ديسمبر) 2016) قوانين الجرائم الإلكترونية المحلية وتسهّل تبادل الأدلة الرقمية عبر الحدود (مكتب المعاهدات بمجلس أوروبا، 2001). ويتمثّل أحد التحديات الأساسية التي تواجهها التحقيقات الإلكترونية الدولية في أن دولًا كثيرة لا تزال تفتقر إلى الأُطر القانونية الموضوعية والإجرائية وإلى القدرات الشرعية للحصول على الأدلة الرقمية. وقد يساعد التعاون الدولي المتزايد حول الجرائم الإلكترونية كالذي أتاحته اتفاقية بودابست والإنتربول في تقديم أدلة للتحقيقات في تحديد المصدر. ولكن اتحادنا المقترح لن يعتمد على انضمام الدول لاتفاقية بودابست ولن يركّز بشكل محدد على استجابات أجهزة إنفاذ القانون للجرائم الإلكترونية المرتبطة بالإنتربول.

المهمة

في ضوء التحديات والرؤى المناقشة هنا نقترح إنشاء منظمة دولية لتحديد مصدر الهجمات الإلكترونية واستكشاف طبيعتها وقد أطلقنا عليها لأغراض هذا التحليل تسمية الاتحاد العالمي لتحديد مصدر الهجمات الإلكترونية (الاتحاد). وتقضي مهمة المنظمة بإجراء فريق واسع من الخبراء الدوليين تحقيقات مستقلة في الحوادث الإلكترونية الكبرى بغية تحديد مصدرها. وسيعمل الاتحاد مع الضحايا أو المدافعين عنهم بناءً على طلبهم وبالتعاون معهم للتحقيق في الحوادث الإلكترونية عن طريق مجموعة متنوعة من المنهجيات وسينشر نتائجه ويتيحها للمراجعة العامة. ويستطيع المجتمع الدولي استخدام نتائج الاتحاد لتعزيز دفاعات الشبكة وإحباط الهجمات المستقبلية وتنفيذ إجراءات المتابعة لمحاسبة مرتكبي الجرائم. وبالإضافة إلى تقدير المصادر بموثوقية وشفافية، ستساعد تحقيقات الاتحاد على توحيد المقاربات المنهجية المنتشرة ومصطلحات التسمية ومقاييس الموثوقية التي تحسّن الفهم المشترك في الفضاء الإلكتروني وتعزّز الأمن الإلكتروني العالمي.

العضوية والشرعية

ومن الضروري جدًا أن يشمل الاتحاد عضوية واسعة النطاق تمتدّ على كافة الخطوط الجغرافية السياسية لتعزيز وجهات النظر المتنوعة وتخفيض احتمال فساد نتائجه من جرّاء النفوذ السياسي. وبالاستناد إلى تحليل حالات تحديد مصدر الهجمات الإلكترونية ومنظمات وعمليات استقصائية لا تُعنى بالهجمات الإلكترونية، نوصي بأن تشمل العضوية ممثلين من قطاعين اثنين: (1) خبراء تقنيون من شركات الأمن الإلكتروني وتكنولوجيا المعلومات ومن الأوساط

دراسة الحالة 3

شركة مانديانت تُعزي هجمات مجموعة التهديد المتواصل المتطور 1 (ATP1) إلى الحكومة الصينية

في شباط (فبراير) 2013 نشرت شركة الأمن الإلكتروني الخاصة مانديانت (التي اشترتها لاحقًا فاير آي) تقريرًا يربط سرقة مئات التيرابايت من البيانات من 141 ضحية على الأقل (ومن بينها 115 ضحية في الولايات المتحدة) في 20 قطاعًا بارزًا على مدى سبع سنوات بأربع شبكات كبرى في الصين. وأطلقت اسم "التهديد المتواصل المتطور 1" على المجموعة المتورطة في الهجمات (وتُعرف أيضًا باسم "مجموعة التعليقات" (Comment Crew) لدى شركات أخرى) ووصفتها بأنها "واحدة من أكثر مجموعات التجسس الإلكتروني نشاطًا من حيث الكم الهائل من المعلومات المسروقة". وخلُصت مانديانت أيضًا بالاستناد إلى مجمل أدلتها إلى أن الحكومة الصينية استخدمت مجموعة التهديد المتواصل المتطور 1 أو على الأقل عرفت بوجودها كما أشارت إلى أن هذه المجموعة هي المكتب الثاني للشعبة الثالثة من هيئة الأركان العامة في جيش التحرير الشعبي والمعروف بالوحدة 61398 (مانديانت، 2013).

ووصفت مانديانت دعمًا لاستنتاجاتها المواقع الفعلية للمباني التي اعتقدت أنّها ضمّت المرافق المستخدمة في الهجمات التي قامت بأبحاث عنها وكشفت عن ثلاث أشخاص اعتقدت أنّهم مرتبطون بالتهديد المتواصل المتطور 1. ونشرت أيضًا أكثر من 3 آلاف مؤشر اختراق (IOC) لأجل "تدعيم الدفاعات بوجه عمليات التهديد المتواصل المتطور 1". وشملت مؤشرات الاختراق التي نشرتها مانديانت أسماء نطاقات وعناوين بروتوكول الإنترنت ودالات تجزئة خوارزمية أم دي 5 (MD5) من برمجيات خبيثة من أكثر من 40 عائلة و13 شهادة تشفير X.509.

وقد اعترفت مانديانت بسليبات نشر استنتاجاتها ومؤشرات الاختراق. واعترفت على وجه الخصوص بأن نشر مؤشرات الاختراق يحدّ من مدى عمرها ويزيد بالتالي من صعوبة عمل الحماة. ولكن برأي مانديانت، فإن إقامة رابط مع الصين سيسلّط الضوء على التهديد المستمر الذي نشأ هناك (وفق مانديانت) وسيؤدّي إلى التنسيق في التصدي لمثل هذه التهديدات.

ولكنّ التقرير لم يخل من الجدل. ففي أحد المؤتمرات الصحفية، وصف الناطق باسم وزارة الخارجية الصينية ادعاء مانديانت بأنّه "انتقاد لا أساس له" وأضاف أنه "غير مسؤول وغير محترف" ("الصين تعارض الادعاءات بالقرصنة: الناطق باسم وزارة الخارجية" (China Opposes Hacking Allegation: FM Spokesman)، 2013). ونفى أيضًا الناطق باسم وزارة الدفاع الصينية استنتاجات مانديانت وادّعى أن التقرير يفتقر إلى الاثباتات التقنية وأن عناوين بروتوكول الإنترنت يمكن سرقتها ("الجيش الصيني لا يؤيّد الهجمات الإلكترونية بتاتًا: وزارة الدفاع" (Chinese Military Never Supports Cyberattacks: Defense Ministry)، 2013، بلانشارد (Blanchard)، 2013). وعلى نحو منفصل انتقد مسؤولون في شركات أخرى التقرير. على سبيل المثال نشر جافري كار (Jeffrey Carr) المدير التنفيذي في تايا غلوبل (Taia Global) بيانًا في مدونة (2013) أشار فيه إلى "عيوب تحليلية خطيرة" في تقرير مانديانت. وادّعى كار أنّ مانديانت لم تستبعد بشكل مُرضٍ الجهات الفاعلة أو التمويهات الأخرى.

الأكاديمية (2) وخبراء في سياسات الفضاء الإلكتروني واختصاصيو قانون وخبراء في السياسة الدولية من أوساط أكاديمية ومنظمات أبحاث متنوعة.[2] وثمة أمثلة على تبادل هذه الجهات الفاعلة المعلومات وتعاونها لتحقيق أهداف إدارة الإنترنت والأمن الإلكتروني.[3] ونتصوّر أن تتضمّن عضوية الاتحاد ما بين 20 و40 ممثلًا خبيرًا من منظمات ضمن هذه القطاعات وأن تتولّى التحقيقات فرق صغيرة تتألّف غالبًا من أقل من 10 محققين تتمثّل مسؤوليتها الرئيسية في مراجعة الأدلة الجنائية التقنية. وقد يضطلع أعضاء مختلفون بأدوار مختلفة في التحقيق بحسب مهاراتهم بما في ذلك التقييم التقني فضلًا عن أدوار في التحقيق أو التقدير. وسيشرف الممثلون الباقون على التحقيق وسيعارضون النتائج الأولية ويقدّمون نصحهم وتعليقاتهم عند الضرورة.

ولا بدّ أن نشدّد في توصياتنا على ألّا يكون ممثلو الدول أعضاءً فاعلين في الاتحاد. ولا تُعتبر الدول ضرورية لتحديد المصدر في جميع الحالات لأن القطاع الخاص والأوساط التقنية تملك بالفعل خبرة واسعة لتحديد المصدر بدرجات متفاوتة في حالات رئيسية بدون الاستفادة من الدول وقدراتها الاستخباراتية الفريدة كما حدث في حالات التهديد المتواصل المتطور 1 وسوني واللجنة الديمقراطية الوطنية. وقد حدد أيضًا باحثون مستقلون المصدر بدون مساعدة الدول في العديد من الهجمات الأصغر نطاقًا.[4] وبالرغم من قدرات بعض الدول على إجراء تحقيقات جنائية وضم استخبارات شاملة فريدة، يركّز تحليلنا على ثلاثة أسباب لضرورة عدم تمثيل الدول رسميًا:

1. غالبًا ما ترتكز ادعاءات الدول في تحديد المصدر على أدلة واستخبارات ليست مستعدة لمشاركتها علنًا ويثير ذلك تساؤلات مستمرة حول كيفية توصلها إلى هذه النتائج وحول موثوقيتها.

2. تنشر الدول ادعاءات تحديد المصدر لأغراض سياسية وتملك باعتبارها أعضاءً دوافع لتشكيل نتائج الاتحاد بطريقة تخدم مصالحها الوطنية.

3. تملك الدول حوافز للتأثير في الحوادث الإلكترونية التي يختار الاتحاد التحقيق فيها وقد تسعى إلى إقناع الاتحاد بعدم قبول حالات قد تسلّط الضوء على عملياتها الإلكترونية أو تهدّدها.

ولهذه الأسباب نعتقد أن موثوقية الاتحاد وشفافيته تتطلّبان أن يعمل بدون مشاركة الدول باعتبارها أعضاءً. وقد تلعب الدول المساعدة دورًا مفيدًا عبر منح الاتحاد معلومات للمساعدة في تحقيق ما، ويستطيع الاتحاد بدوره أن يقرّر طلب هذه المعلومات أم لا وإدخالها في التحقيق أم لا. ولكن العضوية الرسمية يجب أن تقتصر على مجموعة مختارة بعناية من الأطراف غير الحكومية لضمان التمثيل

[2] يُذكر من المنظمات المحتملة مثلًا: كاسبرسكي وسيمانتك وكراودسترايك ومايكروسوفت وهواوي (Huawei) وزد تي إي (ZTE) وفرقة العمل المعنية بهندسة الإنترنت ومعهد مهندسي الكهرباء والإلكترونيات وجمعية الإنترنت ومجموعة الخبراء الدوليين التابعين لدليل تالين (Tallinn Manual International Group of Experts).

[3] الأخذ في الاعتبار مثلًا التعاون المتنوّع بين هيئات إدارة الإنترنت مثل الآيكان وفرقة العمل المعنية بهندسة الإنترنت ومساعي تبادل المعلومات لتعزيز الأمن الإلكتروني في مراكز تبادل المعلومات وتحليلها (Information Sharing and Analysis Centers).

[4] انظر مثلًا مدونة براين كريبس (Brian Krebs)، كيربز والأمن *(Krebs on Security)*، للاطلاع على الأمثلة عن الجرائم الإلكترونية.

العالمي والكفاءة التقنية. وسيتيح أيضًا تقييد العضوية للاتحاد أن يلتأم كهيئة بدون الاعتماد على توصّل القوى الإلكترونية الكبرى إلى اتفاق حول الرغبة في المنظمة وبنيتها إذ قد تمتدّ هذه المفاوضات لسنوات كثيرة بدون التوصل إلى أي نتيجة. إننا ندرك أن بعض الشركات والمنظمات الخاصة ترتبط بحكومات وطنية ولكنّنا نفترض أن التنوع الكافي في الخبرات التقنية وإجراءات التحقيق وآليات الحوكمة المفصّلة أدناه ستخفّف من حدة القلق من قدرة الممثلين الذين توكّلهم الدول على التدخل في نتائج تحديد المصدر أو تعديلها.

ونظرًا إلى التوافق المحدود بين الدول بشأن معايير الفضاء الإلكتروني واستبعاد إقامة معاهدة رسمية للأمن الإلكتروني في المدى القريب لن يستمدّ الاتحاد سلطته من الاتفاقات الدولية القائمة أو الجديدة. بل ستقوم شرعيته على سمعته وموثوقيته اللتين سيكتسبهما من الخبرة التقنية التي يتمتّع بها أعضاؤه العالميون المتنوعون ومن التزامه بالموضوعية والشفافية في نتائج تحديد المصدر. وسيبني الاتحاد سمعته وموثوقيته مع مرور الوقت عبر إجراء تحقيقات علنية في تحديد المصدر واحترام بروتوكل النشر والمراجعة المناقش أدناه.

نعترف أنه سيكون هناك بعض الهجمات الإلكترونية التي تتطلّب استخبارات حكومية من أجل التوصل إلى قرار بشأن تحديد مصدرها. وفي الحالات التي يرى فيها الاتحاد أنه غير مجهّز للتوصل بثقة إلى قرار بشأن تحديد المصدر يستطيع عندئذٍ الإعلان عن حاجته إلى الاستخبارات الحكومية. وقد وقعت في الماضي حالاتٍ أشارت فيها شركات من القطاع الخاص إلى عدم قدرتها على إجراء تحقيق لتحديد المصدر.[5] وبصورة عامة سيربط الاتحاد مستوى الموثوقية بكل قرار يتخذه بشأن تحديد المصدر وقد يُستمدّ مستوى الموثوقية من توفّر الاستخبارات أو عوامل أخرى مثل التمويه أو عدم توفرها. (انظر "معايير الموثوقية في تحديد المصدر" في الفصل الخامس للمزيد من النقاشات حول مستويات الموثوقية).

منظمات دولية مماثلة

استعرضنا مجموعة مختارة من المنظمات الدولية التي تتمتّع بصلاحيات مشابهة نوعًا ما من أجل وضع هيكلية المنظمة المقترحة وتحديد وظائف الاتحاد اللاحقة. ويقدّم الجدول 2 أمثلة عن منظمات دولية مماثلة. وتشكّل المنظمات الدولية ومنظمات أصحاب المصلحة المتعددين والعمليات الاستقصائية غير المتكررة والهيئات الوطنية التالية أمثلة تعطي لمحة عن تنظيم الاتحاد ووظائفه. ويجدر الذكر أن أيًا من هذه المنظمات لا توفّر نموذجًا مثاليًا للاتحاد ولكنها تقدّم دروسًا حول بنيته المحتملة.

وتملك المنظمات الحكومية الدولية مثل تلك المرتبطة بالأمم المتحدة (ومن بينها الوكالة الدولية للطاقة الذرية والاتحاد الدولي للاتصالات) سلطة معترف بها مستمدة من اتفاقات رسمية بين الدول وتشمل مشاركة واسعة النطاق

[5] على سبيل المثال امتنعت نوفيتا عن تحديد دول باعتبارها مصدرًا للهجمات في تقرير أوبريشن بلوكباستر ولكنها أفادت أن عملها قد يعزّز عمل الآخرين في مجال تحديد المصدر (فريق الأبحاث المتعلقة بالتهديدات لدى نوفيتا، 2016).

من الدول وخبرة تقنية. وتتمتّع بدرجات متفاوتة من الفعالية في التعامل مع تحديات دولية معينة وتنسيق الأعمال في المجتمع العالمي فضلاً عن التدقيق والامتثال التقنيين في حالة الوكالة الدولية للطاقة الذرية. ولكن كما ورد سابقًا ثمة أسباب مقنعة لإقصاء الدول من العضوية التنفيذية في الاتحاد. وعلاوة على ذلك ستتم عرقلة سرعة الاتحاد وكفاءته التقنية وقدرته على التوصل إلى نتائج تحظى بإجماع تقريبي بشكل كبير إذا صُمم على شكل هيئات دولية تشمل المجتمع العالمي بأسره وتمتاز بانتظام بإدارتها غير العملية والمبالغة التنظيمية.

وتقدّم لجنة الجزاءات المفروضة على المنظمات الإرهابية التابعة لمجلس الأمن والتي تشمل عضويتها مجلس الأمن مثالاً مفيدًا على هيئة أصغر حجمًا تتعاون لتقييم الأدلة التقنية والتوصل إلى استنتاجات توافقية تُنشر فيما بعد على نطاق واسع. ولكن تركّز هذه الهيئة على تهديدات إرهابية غير حكومية وبالتالي تمكّن ممثلي الدول من التصدي بجهوزية أكبر لمشكلة مشتركة. أمّا الاتحاد فلا بدّ أن ينفتح على عزو الهجمات الإلكترونية إلى جهات فاعلة من الدول وأن يتطلّب بالتالي براعة تقنية من مجموعة من الجهات الفاعلة التي لا تحظى بتمثيل في مجلس الأمن.

الجدول 2

المنظمات الدولية النظيرة

المنظمات الحكومية الدولية	التحقيقات الدولية	هيئات أصحاب المصلحة المتعددين
الوكالة الدولية للطاقة الذرية	التحقيق في غرق تشونان (Cheonan) عام 2010	فرقة العمل المعنية بهندسة الإنترنت
قرار لجنة الجزاءات المفروضة على المنظمات الإرهابية التابعة لمجلس الأمن رقم 1267	إسقاط الرحلة 17 التابعة للخطوط الجوية الماليزية عام 2014	أوبريشن بلوكباستر
منظمة حظر الأسلحة الكيميائية	التحقيق في انتشار فيروس إيبولا بين عامي 2014 و2016	الآيكان
الاتحاد الدولي للاتصالات	–	جمعية الاتصالات المالية بين المصارف على مستوى العالم

وتوفّر منظمة حظر الأسلحة الكيميائية مثالاً مقنعًا على منظمة حكومية دولية مستقلة غير تابعة للأمم المتحدة تستفيد من الخبرة التقنية للحد من المخاطر المرتبطة باستخدام الأسلحة الكيميائية. ولكن منظمة حظر الأسلحة الكيميائية تمامًا مثل الوكالة الدولية للطاقة الذرية والاتحاد الدولي للاتصالات ترتكز على مصادقة الدول على معاهدة رسمية. وعلى الرغم من أن البعض قد اقترح نوعًا مشابهًا من الحد من الأسلحة أو حظرها في ما يتعلّق بالقدرات الإلكترونية، أعلنت الحكومة الأمريكية (وغيرها من الحكومات) صراحة عن عدم تأييدها لتطوير أداة مماثلة. ونتيجة لذلك لا يستطيع الاتحاد الاستفادة من اتفاق دولي دائم يستمدّ منه سلطته ووظائفه.

وتعطي التحقيقات الدولية دروسًا مفيدة حول كيفية تعاون مجموعة متنوعة من الجهات الفاعلة لعزو عمل دولي مشين إلى الجهات المسؤولة ومن بينها الدول. وتظهر التحقيقات مثل التحقيق المتعدد الجنسيات في غرق السفينة الحربية الكورية الجنوبية تشونان *(Cheonan)* عام 2010 قيمة الكشف العلني عن الأدلة التقنية التي دعمت تحديد دولة معينة باعتبارها مصدر الهجوم. وكذلك شارك التحقيق في إسقاط الرحلة 17 التابعة للخطوط الجوية الماليزية الذي ترأسته هولندا تحليلًا تقنيًا مقنعًا وجّه أصابع الاتهام إلى وحدات روسية عاملة في شرق أوكرانيا. وتعززت نتائج الفريق الهولندي وازدادت دقتها من خلال بحث مفتوح المصدر أجرته منظمة بالينغكات (Bellingcat) غير الحكومية، وأظهر ذلك الدور المحتمل الذي تلعبه الأطراف الخارجية في استعراض النتائج الرسمية وتعزيزها (بالينغكات، 2016). وبالرغم من نفي كوريا الشمالية وروسيا على التوالي للنتائج في قضيتَي تشونان والخطوط الجوية الماليزية أسفرت طبيعة التحقيق الدولية ونشر التفاصيل التقنية المقنعة عن إجماع عام حول موثوقية النتائج.

وبالرغم من هذه الدروس القيّمة لا ينبغي تشكيل الاتحاد وفق هذه التحقيقات مباشرة لأن التعاون العملي في هذه الحالات كافة قد يتوقف فور حلّ القضية. وكما ذكرنا سابقًا يتطلّب تحديد مصدر الهجمات الإلكترونية "حملة" وليس نهجًا غير متكرر. ولا بدّ أن يمتلك الاتحاد القدرة والإمكانية على تقييم عدد كبير من الهجمات المرتبطة على الأرجح بدلًا من التعامل معها على نحو منفرد. وبالإضافة إلى ذلك تستطيع هيئة دائمة اختيار الحالات التي ستحقّق فيها عبر عملية منظمة وشفافة.

وتشمل هيئات أصحاب المصلحة المتعددين تمثيلًا من القطاع الخاص والمجتمع المدني – وليس من الدول وحدها – وتؤمّن بهذه الطريقة نموذج عضوية مفيدًا للاتحاد. وقد أظهرت بعض هذه الهيئات أيضًا أن التنوع في صفوف الخبراء التقنيين يؤدّي إلى تعاون ناجح في مسائل الإنترنت والأمن الإلكتروني. ولكن منظمات إدارة الإنترنت مثل هيئة الإنترنت للأرقام والأسماء المخصصة وفرقة العمل المعنية بهندسة الإنترنت تعتمد سياسة عضوية مفتوحة واسعة الانتشار ومجموعة متنوعة من الأهداف التقنية في حين ينبغي أن يتألّف الاتحاد من مجموعة صغيرة دائمة من الأعضاء وأن يصب كامل تركيزه على مهمة تحديد المصدر. وشملت عملية أوبريشن بلوكباستر بقيادة نوفيتا تحالفًا من الشركاء في قطاع التكنولوجيا قدّموا تقييمًا مستقلًا أكّد على النتيجة التي توصّلت إليها الحكومة الأمريكية في تحديد المصدر ولكنه اقتصر على حادث إلكتروني واحد (انظر دراسة الحالة 5 صفحة 42). وشكّل مشروع غراي غوس (Grey Goose) الذي أسّسه جافري كار في عام 2008 منظمة أخرى قامت بتحقيقات في تحديد مصدر الهجمات الإلكترونية (كار، 2012). وارتكزت التحقيقات على تعهيد جماعي لمجموعة كبيرة من المتطوعين المتخصصين الخاضعين للتدقيق (سترلينغ (Sterling)، 2009). وتناول التحقيق الأول لمشروع غراي غوس الهجمات الإلكترونية في خلال الحرب بين روسيا وجورجيا.

الاختلافات بين اقتراحات أخرى لمنظمة عالمية

إن تحليلنا ليس الأول من نوعه في دراسة قيمة منظمة دولية لتحديد مصدر الهجمات الإلكترونية. ومن اللافت أن مايكروسوفت ومجلس الأطلسي يدعوان إلى زيادة التنسيق العالمي في مسألة تحديد مصدر الهجمات الإلكترونية – وبالفعل رعت مايكروسوفت بحثنا. وتتّفق النقاشات الثلاثة على القيمة التي يضطلع بها تأسيس منظمة دولية لتحديد المصدر (شارني وآخرون (Charney et al.)، 2016؛ هيلي وآخرون، 2014). ولكن تحليلنا يتوصّل إلى استنتاجين مختلفين بشأن تصميم المنظمة ووظيفتها. أولًا يشير بحثنا خلافًا لمايكروسوفت ومجلس الأطلسي ولأسباب ذُكرت سابقًا في هذا التقرير إلى وجوب إدارة منظمة تحديد المصدر وتشغيلها باستقلالية عن الدول. وثانيًا ينظر أيضًا الاقتراح الذي تتضمّنه دراسة مجلس الأطلسي في دور تنفيذي للمنظمة بينما يقودنا تحليلنا إلى معارضة هذه الوظيفة. وترد في الفصل التالي مناقشة إضافية لوظائف اقتراحنا الأساسية.

دراسة الحالة 4

العملية متعددة الأوجه لتحديد مصدر الهجمات على اللجنة الديمقراطية الوطنية

تعرّضت اللجنة الديمقراطية الوطنية ابتدءًا من عام 2015 لاختراق إلكتروني في خضم انتخابات رئاسية شرسة. واستخرج المخترقون ملفات ورسائل إلكترونية نشر موقع ويكيليكس (WikiLeaks) الكثير منها ما أدّى إلى ارتباك في صفوف اللجنة الديمقراطية الوطنية واستقالة رئيستها ديبي واسرمان شولتز (Debbie Wasserman Schultz). ومع أنه من الصعب، لا بل من المستحيل، تقدير حجم الضرر الذي تسبب به الهجوم يُعتبر بدرجة كبيرة أنه لعب دورًا في الانتخابات الرئاسية الأمريكية في عام 2016.

وترأست شركة الأمن الإلكتروني الخاصة كراودسترايك التحقيق في الهجوم وأعلنت بعد التقييم في أيار (مايو) وحزيران (يونيو) 2016 عن مسؤولية تهديدين متواصلين متطورين روسيين: فانسي بير (المرتبط بمديرية المخابرات الرئيسية الروسية) وكوزي بير (المرتبط بجهاز الأمن الفيدرالي الروسي) (ألبيروفتش (Alperovitch)، 2016). وقدّمت كراودسترايك أدلة تشير جزئيًا إلى استخدام ثغرات عبر واجهة باورشيل (Powershell) وبنية الأوامر والتحكم عبر امتداد ملف أدوبي آي.آر.أم (AdobeARM) وأختام زمنية وسلاسل ظهرت مسبقًا. على سبيل المثال شملت بعض البرمجيات الخبيثة للجنة الديمقراطية الوطنية وظيفة حذف ذاتي تسمّى سابوكو (seppuku) (بوراتوسكي، 2016). وقد عُثر على هذه الوظيفة المتطابقة الاسم في ترميز استُخدم في هجمات أخرى أيضًا بدأت في عام 2010 وفق سيمانتك (فريق الاستجابة الأمنية التابع لسيمانتك، 2015). وقد شاركت كراودسترايك بياناتها مع شركات أخرى تُعنى بخدمة الخصوصية الإلكترونية ومع وكالات أمريكية أميركية متعددة.

أجرت الحكومة الأمريكية تحقيق متابعة. وفي 7 تشرين الأول (أكتوبر) قبل موعد الانتخابات أصدرت وزارة الأمن القومي ومكتب مدير الاستخبارات القومية الأمريكي بيانًا مشتركًا غير مسبوق يعزو الحادث إلى "كبار المسؤولين" في الحكومة الروسية. ولكن البيان لم يقدّم أي دليل على النتيجة (وزارة الأمن القومي ومكتب مدير الاستخبارات القومية الأمريكي، 2016). وفي خضمّ الجلبة العامة المطالبة بالمزيد من المعلومات أصدرت وزارة الأمن القومي ومكتب التحقيقات الفيدرالي تقريرًا تحليليًا مشتركًا تحت عنوان "غريزلي ستيب" حدّد التفاصيل والأدوات التقنية التي استخدمتها الجهات الفاعلة الروسية (وزارة الأمن القومي ومكتب التحقيقات الفيدرالي، 2016). وتعرّض هذا التقرير أيضًا لانتقادات شديدة من الأوساط التقنية ولم يوفّر إلا أدلة إضافية محدودة على تحديد المصدر. وفي أعقاب الانتخابات والأيام الأخيرة من إدارة أوباما أصدر مكتب مدير الاستخبارات القومية تقريرًا استخباراتيًا منسّقًا تضمّن تفاصيل إضافية حول الحملة الروسية (مكتب مدير الاستخبارات القومية، 2017). ولكن مثل الكثير من البيانات الحكومية الأمريكية لم يقدّم التحليل علنًا أدلة إضافية مهمة بشأن تحديد المصدر وجاء التبرير بالحاجة إلى حماية المصادر والوسائل.

ولم يكشف موقع ويكيليكس عن مصدر معلوماته ولكن بعيد التحديد الأولي للمصادر تبنّت جهة فاعلة مجهولة تُعرف باسم "غوتشيفر 2.0" (Guccifer 2.0) الهجوم. ووجدت التحقيقات أن الاسم المستعار غوتشيفر 2.0 كان على الأرجح حيلة استُخدمت لإخفاء أثر الجهات الفاعلة الحكومية الروسية. مثلًا شمل الادعاء نشر مستند مايكروسوفت وورد يضمّ بيانات وصفية تشير إلى أن المستند روسي المصدر (غودين (Goodin)، 2016). ولكن روسيا عارضت ادعاءات تحديد المصدر.

الفصل الخامس

السمات الأساسية لمنظمة تحديد مصدر الهجمات الإلكترونية

بعد التحليل الذي أجريناه للهيئات والعمليات القائمة تبيّن أن عملية التحقيق الخاصة بالاتحاد العالمي لتحديد مصدر الهجمات الإلكترونية ونتائجها ينبغي أن تتضمن الميزات الست التالية:

- المعايير الرسمية لشروط قبول الحالات
- عملية جمع الأدلة
- إطار تقييم الأدلة
- معايير الموثوقية في تحديد المصدر
- الإبلاغ وإجراءات البيانات العامة
- إجراءات تقييم حدة الهجمات ودرجة تطورها

ولا بدّ أن توجّه المبادئ التالية الاتحاد في إطار هذه السمات الأساسية كافة: ينبغي أن يتمتّع بالكفاءة التقنية والحيادية والشمولية والتركيز المحدد وأن تقوم قراراته على الإجماع.

ينبغي أن يتمتّع الاتحاد بالكفاءة التقنية والحيادية والشمولية والتركيز المحدد وأن ترتكز قراراته على الإجماع.

المعايير الرسمية لشروط قبول الحالات

تتجلّى إحدى ميزات الاتحاد الأساسية بقدرته على اختيار القضايا التي يريدها من مجموعة الحوادث الإلكترونية. وفي عالم تتراوح فيه الهجمات الإلكترونية بين هجمات بسيطة نسبيًا كالقطع الموزّع للخدمة أو هجمات برامج الفدية وبين هجمات تعطّل مفاعلات نووية وتهدّد شبكات الطاقة، ثمة نطاق هائل للحالات المتوفرة للتحقيق. وفي ضوء ذلك تحتاج منظمة تحديد المصدر مثل الاتحاد إلى القدرة على اختيار الحالات التي تستحق المراجعة.

وبهذه الطريقة يُصمَّم الاتحاد باعتباره منظمة تمتلك قائمة تقديرية، أي أنّها وحدها تحدّد الحالات التي تتولّى التحقيق فيها من بين تلك المحالة إليها للمراجعة. ونقترح عملية أساسية شبيهة بتلك التي تعتمدها المحكمة العليا للولايات المتحدة. فيختار القضاة حوالى 80 قضية للاستماع إليها من بين 7 آلاف أو 8 آلاف استدعاء تقريبًا يُقدَّم إلى المحكمة في كل سنة (المحكمة

العليا للولايات المتحدة، غير مؤرخ). وتجدر الإشارة إلى عنصرين من هذه العملية. أولًا يبادر الطرف المتضرر بطلب مراجعة قضيته. ويتمثّل هذا الطرف في ضحية الهجوم في حالات تحديد مصدر الهجمات الإلكترونية. ويحفظ منح الضحية حق المبادرة الحصري خصوصية الضحية واستقلاليتها وقدرتها على تحديد ما إذا كانت ستطلب تحقيقًا لتحديد المصدر ومتى.[1] وتُطرح أسئلة مفتوحة حول التحديد الدقيق "لضحية" الهجوم إلكتروني. على سبيل المثال هل كان مركز مراقبة الشبكة أو الحكومة الأوكرانية أو المستهلكون الذين فقدوا الطاقة أو مطّورو الأجهزة والبرمجيات الذين استُغلّت نقاط ضعفهم هم ضحية الهجوم على شبكة الكهرباء الأوكرانية؟ ونقترح أن يستخدم الاتحاد تقديره الخاص ليقرّر من تنطبق عليه صفة الضحية وبالتالي من يستطيع طرح الحالة. وثانيًا لا يكفي مجرد تقديم طلب المراجعة لبدء العمل. فالاتحاد لن يقبل بالحالة لمجرد أن ضحية طلبت منه المساعدة.

وتؤمّن الطبيعة التقديرية لمجموعة حالات الاتحاد فرصًا لتوضيح مسألتين أساسيتين للتحديد الذاتي: المعايير التي ينبغي استخدامها لتقييم ما إذا كان طلب الضحية بمراجعة الهجوم الإلكتروني (سواء حدث مرة واحدة فقط أم كان عبارة عن سلسلة مطوّلة أو حملة هجمات) مهمًا بما يكفي ليستحقّ المراجعة والأساس الذي يتعيّن على مسؤولي الاتحاد الاستناد إليه ليقرّروا ما إذا كانوا سيقبلون بالحالة. وفي ما يتعلّق بالمعايير التي قد يستخدمها الاتحاد لا بدّ من الأخذ في الاعتبار القيود الداخلية والقيود الخاصة بكل حالة. وتتعلّق القيود الخاصة بكل حالة بطبيعة الهجوم المزعوم: ما هو عدد الأشخاص أو الأنظمة التي تعرّضت للقرصنة وما مستوى الضرر الذي وقع على مستوى الاقتصاد والسمعة إلخ. وتشكّل القيود الداخلية مسائل مؤسسية: توفر الموارد المالية للاتحاد والوقت والقدرات التقنية إلخ. وستحدّ هذه القيود من قدرة الاتحاد على الاستماع إلى الحالات بغضّ النظر عن اهتمامه بها أو أهميتها أو حدة المطالب.

ويتعيّن على الاتحاد أيضًا التفكير في الأساس الذي يستند إليه القرار وعدم التوقف عند القيود المؤسسية والقيود الخاصة بكل حالة: فما هي العملية التي يعتمد عليها مديرو الاتحاد لاتخاذ القرار بشأن قبول الحالة؟ وتساعد هنا أيضًا القياس على المحكمة العليا للولايات المتحدة. ويتطلّب استماع المحكمة إلى القضية الحد الأدنى من أصوات القضاة (أربعة قضاة من أصل تسعة). ويعد ذلك مثالاً على وضع الأقلية لجدول الأعمال علمًا أن الأكثرية هي التي تقرّر المسألة في النهاية. وبالنسبة للاتحاد قد يسمح الأساس الذي يستند إليه القرار والذي يمنح الأقلية حق وضع القائمة بتنوع أكبر في الحالات المطلوب مراجعتها.

عملية جمع الأدلة

يحتاج الاتحاد إلى الوصول إلى كل البيانات ذات الصلة التي يتوفّر معظمها على شبكة كمبيوتر الضحية (مثلا ملفات السجلات وتاريخ المتصفح التي نوقشت

[1] تلعب الضحايا أيضًا دورًا أساسيًا في إتاحة البيانات الداخلية والشبكات التي تحتوي على أدلة حول هوية المهاجمين الإلكترونيين. وإذا رفضت الضحية إتاحة الشبكات التي تعرّضت للاختراق لن تكون على الأرجح مساعي تحديد المصدر مثمرة.

سابقًا) للإتاحة له بتحديد المصدر. ونعتقد أن طلب الضحية التحقيق يقتضي ضمنيًا استعدادها لوضع بيانات شبكة الكمبيوتر وأصولها بمتناول الاتحاد. ويتعارض الاستعداد للتعاون مع الكثير من التحقيقات الحكومية الدولية. ففي بعض الحالات تنشأ علاقة عدائية بين مؤسسة التحقيق والدولة التي تخضع أنشطتها للتحقيق. فعلى سبيل المثال غالبًا ما يحوّل تحدي الحد من الانتشار النووي دور الوكالة الدولية للطاقة الذرية إلى دور حفظ الأمن.

ومع أن العلاقة بين الاتحاد والضحية قد تكون تعاونية إلاّ أنه ينبغي الأخذ في الاعتبار المخاطر وتحديد عملية جمع الأدلة بدقة. فعلى الاتحاد أن يحدد البيانات التي يريد جمعها من الضحية ومن أمكنة أخرى بما في ذلك التفاصيل المتعلقة بنوع الأغراض المراد استعراضها وعملية الوصول إلى هذه الأغراض والمدة التي ستتاح خلالها الأغراض. وسيعتمد نوع البيانات الذي تحدّده عملية جمع الأدلة على الممارسات الحالية للهجمات الإلكترونية وتحقيقات تحديد المصدر وبالتالي ستتطوّر على الأرجح خصائص البيانات مع مرور الوقت ومن المحتمل أن يلعب الاتحاد دورًا في تسجيل هذا التطور في إجراءات جمع الأدلة التي سينشرها.

وستشمل على الأرجح الأدلة المرتبطة بتحقيق معيّن بيانات حساسة قد تتضمّن ملكية فكرية خاصة بالضحية. ولهذا السبب ستُناط باتفاقيات السرية مسؤولية المساعدة على حماية أي معلومات مكتشفة خلال التحقيق لا تتعلّق مباشرة بالخرق الإلكتروني.

وقد تملك أطراف ثالثة أخرى ومن ضمنها مشغلو الشبكات والباحثون في مجال الأمن أو حتى الدول أدلة تساهم بها في التحقيق وسيحتاج الاتحاد إلى عملية لجمع المعلومات ذات الصلة التي تشاركها هذه المصادر طوعًا وحمايتها.

إطار تقييم الأدلة

من أجل تأسيس منظمة دولية مسؤولة عن تسهيل تحديد مصدر الهجمات الإلكترونية ينبغي أن تحدد المنظمة بوضوح الإطار التحليلي الذي ستقيّم عن طريقه الأدلة وتنشره. وبما أن مقارنة الحوادث والوسائل قد تكون مفيدة لدعم تحديد المصدر عبر حملة هجمات فمن المحتمل أيضًا أن يشمل إطار تقييم الأدلة آلية لمقارنة الهجمات.

ولا بدّ أن يتضمّن التحليل درجة معينة من ترجيح الأدلة المنفردة. على سبيل المثال قد يفوق ترجيح المؤشرات التقنية المؤشرات غير التقنية في حين قد يقل ترجيح المؤشرات التقنية التي تُعتبر عرضة للتضليل عن مؤشرات تقنية أخرى. ويساعد ترجيح الأدلة على ترسيخ مستويات الموثوقية في مزاعم تحديد المصدر.

وينبغي أن تتضمّن عملية التقييم الاستعانة بأعضاء من الاتحاد على نحو مستقل لتحليل الأدلة. ويساعد ذلك على الحد من مخاوف الشركات الخاصة بشأن الكشف عن الملكية الفكرية و/أو النهج المسجلة الملكية التي تعتقد أنها ربما تعطيها أفضلية تنافسية. وعند اكتمال البحث المستقل يسعى الاتحاد

إلى التوصل إلى توافق يرتكز على نتائج أعضائه الفردية. وإذا عجز الاتحاد عن التوصل إلى قرار بالإجماع فستُسجّل آراء الأكثرية والأقلية كما يحدث مع قرارات المحكمة العليا للولايات المتحدة. وعلى غرار المحكمة العليا فقد يكون لآراء الأقلية قيمة مستقبلية في الاتحاد. وعلاوة على ذلك قد يسمح الاتحاد لأعضائه بأن يتحفظّوا عن التعليق أو ينأوا بأنفسهم بالكامل إن كان هذا يفيد العضو و/أو الاتحاد.

معايير الموثوقية في تحديد المصدر

تقضي النتيجة النهائية لمساعي الاتحاد بتحديد الجهة المسؤولة عن الحادث أو الهجوم. وبعد عمل الاتحاد باستخدام إطار تقييم الأدلة وعدد من المنهجيات التي أسهم بها أعضاء الاتحاد يتعيّن على المنظمة وضع عمليات لنقل معلومتين أساسيتين هما: الجهة التي يعتقد الاتحاد أنها مسؤولة بالارتكاز على الأدلة والمنهجيات التي استخدمها المحققون، ومدى ثقته بهذا التقييم. وتُعتبر هاتان المعلومتان أساسيتين لصلاحية الاتحاد وسمعته باعتباره منظمة مستقلة لتحديد مصدر الهجمات.

وستؤثّر الأدلة والمنهجيات المتوفرة التي استخدمها المحققون على مساعي تحديد المسؤول عن الحادث أو الهجوم وربما تعرقلها. وكما ذُكر سابقًا قد يشكّل تحديد أفراد معينين باعتبارهم مسؤولين عن الحادث أو الهجوم تحديًا، لا بل قد يكون ذلك مستحيلًا في بعض الحالات. وبالإضافة إلى ذلك تكمن الصعوبة الأكبر في تحديد مصدر الهجوم على أنه تابع بالكامل لأوامر دولة ما وخاضع لسيطرتها (وليس لأفراد ضمن مناطق جغرافية) مع أن هذه الأدلة قد تكون قابلة للاكتشاف في بعض الحالات.

إن القيود التي تحدّ قدرة الاتحاد على تحديد أفراد معينين باعتبارهم مسؤولين عن الحوادث أو الهجمات أو الادعاء برعاية دول لهم عبر بنى الأوامر والتحكم الرسمية تسلّط الضوء على حاجة الاتحاد إلى أن يكون واضحًا بشأن الأدلة التي يملكها وقوة الأدلة التي تدعم استنتاجاته. وبالتالي ينبغي على الاتحاد أن يضع مجموعة معايير تحليلية ويتقيّد بها بصرامة لتفصيل كيف يقوم بتحليلاته ويقيّمها. وتتوفر نماذج عن المعايير التحليلية لدى مكتب مدير الاستخبارات القومية الأمريكي الذي يواجه تحديات مشابهة في نقل موثوقية المعلومات التي تدعم استنتاجاته التحليلية (مكتب مدير الاستخبارات القومية الأمريكي، 2015). وقد صُمّمت هذه المعايير في جوهرها لضمان النزاهة وتسليط الضوء على الفرق بين الافتراضات والأحكام والتحليل المرتكز على الحقائق وإبراز مجالات الضعف أو النقص في الأدلة لمستهلكي التحليل النهائيين وذلك للحد من الأخطاء في الحكم مستقبليًا.

وسيُحكم على الاتحاد بناء على جودة تحقيقاته وتقييماته. وسيساعده الالتزام بالمعايير التحليلية ذات الممارسات الفضلى على اكتساب سمعة باعتباره مصدرًا موثوقًا لتحديد مصدر الهجمات الإلكترونية.

الإبلاغ وإجراءات البيانات العامة

تُبلغ المنظمة الأطراف المعنية بنتائجها الرئيسية قبل إصدار بيان عام أو نشر تقرير عام يفصّل تقييمها. وقبل أن تصدر المنظمة بيانًا عامًا تتوفّر للأطراف المعنية مدة زمنية محددة بوضوح تستطيع خلالها تقديم الرد على النتائج أو انتقادها. وقد تشمل هذه العملية تقديم معلومات إضافية أو تقييمات بديلة.

ونعتقد أنه من الضروري أن يبلغ الاتحاد الرأي العام بجميع النتائج التي توصل إليها. ونظرًا لتعقيد العمليات الإلكترونية وسريتها قد يساعد إطلاع الرأي العام على هوية المعتدين والوسائل المستخدمة لارتكاب الهجمات الإلكترونية على تعزيز نتيجة تحديد المصدر وتفعيل المزيد من آليات المساءلة. ويساعد أيضًا حماة الشبكة على إدخال المعلومات في أنظمتهم الدفاعية للوقاية من الجهة الفاعلة المسؤولة ومعالجة نقاط الضعف المستغلَة وتحديد التكتيكات والتقنيات والإجراءات وإصلاح البنية التحتية المقرصنة.

وبالإضافة إلى الانفتاح والشفافية، يتعيّن على الاتحاد السعي لتحقيق أهداف أخرى عندما يزوّد الرأي العام بالمعلومات. ولا بدّ أن توفّر البيانات والتقارير العامة:

- معلومات واضحة تتوفر للرأي العام في الوقت المناسب حول الإجراءات التي يتخذها الاتحاد لتحديد مصادر الهجمات ومبررات قراراته
- شفافية وإجماعًا يستند إلى الأدلة (أو تقارير الأكثرية/ تقارير الأقلية) من أجل تعزيز شرعية المنظمة (لجنة السوق المفتوحة الاتحادية (Federal Open Market Committee)، 2017)
- تفاصيل تقنية قابلة للنشر من أجل التقييم والمناقشة على نطاق أوسع
- بيانات خطية وشفهية يمكن استخدامها شهادة في المداولات الدولية والوطنية أو في جلسات المحاكمة.

وينبغي أن يختار الاتحاد شكلاً من أشكال التواصل العام التقليدية بما في ذلك البيانات الخطية والشفهية والقرارات والمحاضر والتقارير ونُسخ المحاضر (الباب 12 من مدونة النظم الاتحادية صفحة 271 عام 2016). ولا بدّ أن يتضمّن البلاغ إجراءات التحقيق ومبررات قرارات تحديد المصدر وقد تشمل:

- توليفًا لتحقيقات سابقة
- وصفًا للأدلة التقنية ومساهمتها في تحديد المصدر
- موثوقية تحديد المصدر.

إجراءات تقييم حدة الهجمات تطورها

يساعد أيضًا الاتحاد على الحد من المخاطر في الفضاء الإلكتروني من خلال تقييم حدة الهجوم الإلكتروني وتطوره. وتسهّل عملية موحدة لتقييم حدة الحوادث الإلكترونية مرحلة ما بعد تحديد المصدر. على سبيل المثال قد يفيد مخطط للحدة المؤسسات التي تختار استخدام التدابير الدفاعية الجديدة فحسب ردًا على أدلة تثبت تعرّض كيانات أخرى لهجمات عنيفة. ويمكن قياس الحدة بطرق متعددة. مثلًا يمكن استخدام مقياس الكلفة المادية

لتقييم الحدة في الهجمات التي أدّت إلى ضرر مادي (مثل دودة ستوكسنت أو الهجمات على شبكة الكهرباء الأوكرانية). ويمكن أيضًا استخدام تهديدات استقلال الدول السياسي (مثل الهجمات على اللجنة الديمقراطية الوطنية). وقد تشكّل الخسارة المالية عامل تقييم آخر للحدة (مثل الهجوم على شركة سوني بكتشرز). ويستطيع الاتحاد أن يوصي بمعايير لتقييم الحدة كي يطبّقها الآخرون.

وقد يستوحي تقييم الحدة الذي يوصي به الاتحاد من النماذج ذات الصلة المستخدمة حاليًا. على سبيل المثال يُستخدم التعريف الشائع التالي عند حدوث عطل كبير في شبكات الطاقة: (1) حدث غير مدبر (لا يُحتسب إطفاء الشبكة للصيانة أو التقنين الدوري) (2) يؤثّر في ألف عميل على الأقل (يبلغ العدد في هذه الدراسة 30 ألفًا على الأقل) (3) وتبلغ فيه مدة التوقف عن العمل الإجمالية مليون عميل–ساعة على الأقل (مكلين (McLinn)، 2009). وتحدّد الوكالة الفيدرالية لإدارة حالات الطوارئ معايير حدة الكوارث الكبرى. وقد يشكّل مخطط الحدة المرمّز بالألوان الذي وضعته الحكومة الأمريكية نموذجًا مفيدًا (وزارة الأمن الوطني الأمريكية، 2016).

وقد يستفيد الاتحاد من خبراته ويعزّز الفهم المشترك في الفضاء الإلكتروني من خلال بناء إطار لتقييم مدى تطور الهجوم الإلكتروني. وغالبًا ما يستخدم المعلقون مفهوم تطور الهجوم بطريقة متباينة ويملك الضحايا دوافع للمبالغة في درجة تطور التهديدات التي يواجهونها. وعلى الرغم من أن درجة تطور الهجوم لا تضاهي بالضرورة أثره وكذلك لا تستخدم الدول المتقدمة ذات الموارد الوفيرة التقنيات المتطورة فحسب فقد يساعد إطار التقييم الموحد حماة الشبكة والرأي العام على فهم هذه المسائل المعقدة بشكل أفضل. وقد جرت محاولات لوضع إطار لتقييم درجة تطور الهجمات ويستطيع الاتحاد دراسة النهج السابقة والاستناد إليها.[2] وقد يصبح نهج درجة التطور الذي يستخدمه الاتحاد موحدًا في مختلف أوساط الفضاء الإلكتروني من خلال الاستخدام المنتظم مع مرور الوقت.

التطبيق والمعايير القانونية

من الضروري التأكيد على موقفنا بأن الاتحاد ينبغي أن يركز بدرجة كبيرة على تحديد المصدر وليس على الإجراءات اللاحقة كالتطبيق. وتتمثّل الميزة النسبية في هذا الصدد في ضم الاتحاد خبراء مستقلين يعملون على تحديد المصدر المزعوم بالإجماع عند الإمكان بدعم من الأدلة التي يمكن إتاحتها للرأي العام. وبعد الإعلان عن تحديد المصدر المزعوم لن يقدّم الاتحاد توصيات بإجراءات اللاحقة (مثل التوصيات بإصدار الأحكام). ولن يقدّم بالتالي توصيات بالعقاب أو بإحالات إلى منظمات أخرى (مثل مجلس القانون الدولي ومحكمة العدل الدولية ومجلس الأمن) لأن هذه الإحالات قد تُعتبر بمثابة توصية بالملاحقة القضائية. ولكن في الوقت عينه قد تستخدم الضحية أو دولة أخرى أو منظمة خارجية تحديد المصدر التي توصل إليه الاتحاد أساسًا لاتخاذ تدابير إضافية وفق ما تراه ملائمًا.

[2] للاطّلاع على أحد الأطر المقترحة، انظر بوشانن (2017).

وبالإضافة إلى ذلك ننظر إلى دور الاتحاد بشكل أساسي على أنه يقدّم وجهة نظر محددة ودقيقة ولا يوفّر أدلة يمكن استخدامها في المحاكم (في الولايات المتحدة أو بلدان أخرى). ومع ذلك إذا عُثر على أدلة تنتهك القوانين الدولية السارية المفعول أو المستقبلية لا بدّ من نشر هذه الأدلة لكي تدقّق فيها المحاكم. ولا تكفي البيانات المبهمة من الاستخبارات الحكومية لهذه الأغراض إلّا إذا رُفعت عنها السرية. وسيكون بالتالي الاتحاد في وضع يسمح له بتقديم أدلة عن الهجمات الإلكترونية تستوفي المعايير القانونية للإجرام في حال وُجدت هذه الأدلة.

دراسة الحالة 5

شركة سوني بكتشرز وعملية أوبريشن بلوكباستر

شكّل الهجوم على سوني بكتشرز في تشرين الثاني (نوفمبر) 2014 نقطة تحول في التحديد العلني لمصدر الهجمات الإلكترونية الخبيثة. وقد أدّى الهجوم إلى نشر معلومات حساسة خاصة بالاستديو السينمائي شملت معلومات شخصية ورسائل الموظفين الإلكترونية وأفلامًا لسوني لم تُعرض بعد في الصالات وتعطّلت أعمال سوني بكتشرز بدرجة كبيرة. وتبنّت مجموعة أطلقت على نفسها اسم "حرّاس السلام" (Guardians of Peace) الهجوم وهدّدت بتنفيذ هجمات إضافية بما في ذلك هجمات مادية على صالات العرض إن واصلت سوني خطتها بإطلاق فيلم المقابلة *(The Interview)* الكوميدي الذي تدور أحداثه حول اغتيال القائد الكوري الشمالي كيم جونغ أون (Kim Jong-Un).

وقد فتحت الحكومة الأمريكية تحقيقًا بالتعاون مع سوني بكتشرز خلُص إلى بيان صدر عن مكتب التحقيقات الفيدرالي ومفاده أن "الحكومة الكورية الشمالية هي المسؤولة عن هذه الأعمال." (مكتب التحقيقات الفيدرالي، 2014). وأشار مكتب التحقيقات الفيدرالي إلى ثلاثة أسباب دفعته إلى هذا الاستنتاج وشملت ما يلي:

> "[1] كشف التحليل التقني للبرمجيات الخبيثة الماحية للبيانات المستخدمة في هذا الهجوم عن روابط ببرمجيات خبيثة أخرى يعرف مكتب التحقيقات الفيدرالي أن جهات فاعلة كورية شمالية قد طوّرتها في وقت سابق... [2] تداخل كبير بين البنية التحتية المستخدمة في هذا الهجوم ونشاطات خبيثة أخرى... مرتبطة بكوريا الشمالية [3] الأدوات المستخدمة في الهجوم [على سوني] شبيهة بهجوم إلكتروني... على مصارف كورية جنوبية... نفّذته كوريا الشمالية."

ولكن أشار البيان إلى أن مكتب التحقيقات الفيدرالي لا يستطيع مشاركة الأدلة المستخدمة في التقييم بسبب "الحاجة إلى حماية المصادر والطرق الحساسة."

وقد امتزجت الآراء حول تحديد هذا المصدر وأشار البعض إلى امتلاك كوريا الشمالية الوسائل والدوافع لتنفيذ الهجوم بينما وجد آخرون أسبابًا للتشكيك في ادعاءات الحكومة (مثل شناير (Schneier)، 2014). ولفت الكثيرون إلى أن الولايات المتحدة بحاجة إلى أن تكون أكثر صراحة وشفافية بشأن أدلتها (مثل زيتير، 2014b).

وفي شباط (فبراير) 2016 نشرت شركة نوفيتا للبيانات والتحليل الإلكتروني عملية أوبريشن بلوكباستر وهو تقرير يلخّص المسعى الذي قام به تحالف بين شركات خاصة لتحديد الأدوات والتكتيكات التي استخدمها مهاجمو سوني وتعطيلها (فريق الأبحاث المتعلقة بالتهديدات لدى نوفيتا، 2016). وضمّ التحالف شركات متعددة تُعنى بالأمن الإلكتروني مثل سيمانتك وكاسبرسكي لاب وتراند مايكرو تعاونت لمشاركة مؤشرات التهديدات الإلكترونية المرتبطة بالهجوم وتحليلها. ويطرح التقرير منهجية بحث التحالف ويقدّم مجموعة من الأدلة التقنية التي تربط هجوم سوني بمجموعة لازاروس. وعلى الرغم من أن التقرير امتنع عن اتهام كوريا الشمالية برعاية المهاجمين فإنه يقدّم مثالاً مقنعًا على كيفية تعاون الشركات الخاصة لتحديد مصدر الهجوم وتقديم الأدلة علنًا.

الخاتمة

في ظل مواجهة الهجمات الإلكترونية المتزايدة الوتيرة وارتفاع حدة تأثيراتها أصبح الاهتمام بعملية تحديد المصدر المستقلة والموثوقة والمعوّل عليها في غاية الأهمية. ويتزايد قلق القطاعين العام والخاص حيال طبيعة التهديدات الإلكترونية. وتتطلّب الجهوزية للتصدي للحوادث الإلكترونية والوقاية منها والتحقيق فيها محترفين بارعين وتبادل المعرفة ومنظمات تتمتّع بموثوقية ومسؤولية لكشف المهاجمين الإلكترونيين.

ربما حان الوقت لتأسيس منظمة دولية جديدة لتحديد المصدر

وفي حين بُذلت جهود دولية مخصصة لإقامة اتفاق واسع النطاق يتعلق بقواعد السلوك في مجال النشاطات الإلكترونية – مثل المطالبة باتفاق على عدم المس بالبنية التحتية الحيوية في الهجمات الإلكترونية التي تشنّها الدول – لا تتوفر أنظمة قائمة لمحاسبة الدول. وعلاوة على ذلك وبما أن القدرات الإلكترونية أصبحت بمتناول عدد متزايد من الأفراد بدون دعم الدول بفضل إرساء ديمقراطية التكنولوجيا يزداد تعقيد الدافع للمساءلة والامتثال للقواعد.

ولكن الحاجة إلى معرفة المسؤولين عن الهجمات الإلكترونية عند وقوعها تبقى في صلب هذه الشواغل. وتشكّل المعايير الدولية والوعود بحسن السلوك خطوة إلى الأمام في ترسيخ التوقعات، ولكن بدون القدرة على معرفة تاريخ وقوع الهجوم وهوية الفاعل يستطيع أفضل المجرمين تجاهل المساعي الدولية. لذلك تعتبر القدرة على معرفة المسؤول عنصر المساءلة الأساسي.

ولكن المصالح المتضاربة في السياسة والأعمال والشؤون الدولية تعيق بدرجة كبيرة الوضع القائم لتحديد مصدر الهجمات الإلكترونية وتعرقله. وأحيانًا ما تتعارض الدول بشأن مزاعم تحديد المصدر. وتتنافس الشركات الخاصة ذات منهجيات التحقيق الحديثة في الجرائم الإلكترونية بانتظام – لكنها نادرًا ما تتعاون – لتقديم معلومات دقيقة عن أبرز حالات الهجمات الإلكترونية الرفيعة المستوى. ولا يبدو أن أحدًا يملك كلمة الفصل الموثوقة في التوصل إلى رأي توافقي حول تحديد مصدر الهجمات.

وأشار هذا التقرير إلى أن الوقت قد حان ربما لتأسيس منظمة دولية جديدة لتحديد المصدر. وبالاستناد إلى الدروس المستخلصة من استعراض الهجمات الإلكترونية الكبرى في السنوات الأخيرة ومن الرؤى الرئيسية التي استُمدّت من أحدث طرق تحديد مصدر الهجمات الإلكترونية وتكتيكاته طرحنا نموذجًا أوليًا لمنظمة جديدة هي الاتحاد العالمي لتحديد مصدر الهجمات الإلكترونية. ويمكن تأسيس منظمة كهذه لإجراء تحقيق مستقل في الحوادث

الإلكترونية الكبيرة على يد فريق كبير من الخبراء الدوليين بغية تحديد مصادر الهجمات.

وتتمثّل نقاط قوة الاتحاد في تشكيلته الدولية وقدرته على جمع المنهجيات المتنوعة التي ينشرها أعضاء الاتحاد التأسيسيون باستقلالية وصلاحية تحديد المصدر بالإجماع والإعلان عنه (مع فرص للخلاف) ضمن الحالات التي يقرّر الاتحاد التحقيق فيها. ويعمل الاتحاد مع ضحايا الهجمات الإلكترونية على مسائل تحديد المصدر، وإن سُمح بذلك، قد يضع الضحايا والدول والمجتمع الدولي استراتيجيات لتعزيز دفاعات الشبكة وإحباط الهجمات المستقبلية واختيار إجراءات تنفيذ ملائمة لمحاسبة الجهات المسؤولة. ونظرًا إلى أن اقتراحنا يحذّر من عضوية الدول ستتمثل نقطة الضعف الأبرز في الاتحاد في عدم القدرة على الوصول إلى الموارد الاستخباراتية الحكومية الضرورية لبعض تحقيقات تحديد المصدر.

يعرض هذا التقرير بعض السمات الأساسية التي لا بد أن تأخذها منظمة كالاتحاد في الاعتبار ومنها:

- اقتصار العضوية على خبراء غير حكوميين
- خصائص جوهرية لشروط قبول الحالة
- إطار قائم على جمع الأدلة وتقييمها
- الحاجة إلى معايير موثوقية في تحديد المصدر
- متطلبات نشر النتائج
- وضع مقاييس لحدة الهجوم ودرجة تطوره.

وهذه مجرد بداية الحوكمة والجوانب التشغيلية التي يتعيّن على منظمة كالاتحاد معالجتها. ويشكّل التمويل أحد الجوانب المهمة في الاتحاد والتي يجب وضع مخطط لها قبل الإطلاق الناجح. ونظرًا إلى أن افتراضنا يقضي بألاّ تتألّف العضوية من ممثلي دول فسيواجه الاتحاد تحديًا من ناحية التمويل، وهي مسألة لا تقلق بشأنها منظمات عالمية كثيرة. وعادة ما تموَّل المنظمات المتعددة الجنسيات كالأمم المتحدة ومنظمة حلف شمال الأطلسي (الناتو) عن طريق رسوم تسددها الدول الأعضاء. وفي هذه الحالة من المستبعد أو من غير المحبذ أن تتوفر إيرادات من الدول مع العلم أنّها تستفيد كثيرًا من قرارات الاتحاد. وبالإضافة إلى ذلك ستشكّل على الأرجح العضوية الأساسية المؤلفة من شركات القطاع الخاص تحديًا لأن قوة هذه الشركات المالية النسبية (والقدرة على الدفع المرتبطة بها) تمتدّ على نطاق واسع وقد يعتبرها الناس شكلاً من حكم الأثرياء.

وفي ما يتعلق بخيارات التمويل قد تشكّل المنظمات الخيرية مصدر التمويل الأولي في مراحل الاتحاد الأولى مع تفويض رسمي بطلب التمويل من منظمة دولية كالأمم المتحدة وذلك ضمن مهلة زمنية معينة. وفي حين يواجه هذا النهج خطر التعرّض لنفوذ مفرط من قبل كيان خيري معين إلاّ أنّه يعدّ خارطة طريق لينتقل عبرها الاتحاد إلى سلطة منظمة دولية تشمل تمثيلاً متنوعًا وواسعًا.

وقد تشكّل شركات تكنولوجيا المعلومات والاتصالات مصدرًا آخر لتمويل هذه المنظمة. وتقدّم شركات مثل كومكاست (Comcast) أو فاريزون (Verizon) أو إنتل (Intel) أو مايكروسوفت البرمجيات وأنظمة معدات الشبكة التي تنفَّذ عبرها الهجمات الإلكترونية بالإضافة إلى أدوات التحقيق الجنائي الرقمية لدعم التحليل. ويكون لهذه الشركات مصلحة خاصة، إن لم يكن واجبًا، في تحديد ومنع استخدام شبكاتها لإلحاق الضرر بعملائها. وقد لا يوفّر تجميع الموارد عبر هذه الشركات تمويلًا ملائمًا فحسب بل قد يحسّن موثوقية الاتحاد وصورته أيضًا.

وستثير بدون شك المسائل الإضافية كالتوظيف والإدارة والسرية والأمن وحتى موقع المنظمة مشاكل أعمق في بنية المنظمة ووظائفها. وفي حين يجري العمل على تأسيس أي منظمة دولية لتحديد المصدر يتّضح مبرر هذه المنظمة أكثر فأكثر وتزداد الحاجة إليها إلحاحًا.

الاختصارات

APT	التهديد المتواصل المتطور
C2	بنية الأوامر والتحكم
CEO	المدير التنفيذي
CIA	وكالة الاستخبارات المركزية
DDoS	هجمات القطع الموزّع للخدمة
DNA	الحمض النووي
DNC	اللجنة الديمقراطية الوطنية
DNI	مكتب مدير الاستخبارات القومية الأمريكي
DNS	نظام اسم النطاق
FBI	مكتب التحقيقات الفيدرالي
G20	مجموعة العشرين
IAEA	الوكالة الدولية للطاقة الذرية
ICANN	هيئة الإنترنت للأرقام والأسماء المخصصة (الآيكان)
IETF	فرقة العمل المعنية بهندسة الإنترنت
IP	بروتوكول الإنترنت
ISIS	الدولة الإسلامية في العراق والشام (داعش)
ITU	الاتحاد الدولي للاتصالات
HUMINT	الاستخبارات البشرية
NASA	الإدارة الوطنية للملاحة الجوية والفضاء (ناسا)
OPCW	منظمة حظر الأسلحة الكيميائية
OPM	المكتب الأمريكي لإدارة شؤون الموظفين
OSINT	استخبارات المصادر المفتوحة
SIGINT	استخبارات الإشارات
SWIFT	جمعية الاتصالات السلكية واللاسلكية بين المصارف على مستوى العالم في الميدان المالي المصرفي
TTP	التكتيكات والتقنيات والإجراءات
UN	منظمة الأمم المتحدة

المراجع

"AlienVault Ossim," web page, undated. As of May 26, 2017: https://www.alienvault.com/products/ossim

Alperovitch, Dmitri, "Bears in the Midst: Intrusion into the Democratic National Committee," *CrowdStrike*, blog post, June 15, 2016. As of March 31, 2017: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

AV Comparatives, *Data Transmission in Internet Security Products*, May 20, 2014. As of March 31, 2017: http://www.av-comparatives.org/wp-content/uploads/2014/04/avc_datasending_2014_en.pdf

Bartholomew, Brian, and Juan Andres Guerrero-Saade, *Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks*, Virus Bulletin Conference, October 2016.

Baumgartner, Kurt, and Maria Garnaeva, "BE2 Custom Plugins, Router Abuse, and Target Profiles: New Observations on BlackEnergy2 APT Activity," *SecureList*, Kaspersky Lab website, November 3, 2014. As of March 31, 2017: https://securelist.com/blog/research/67353/be2-custom-plugins-router-abuse-and-target-profiles/

Bellingcat, "MH-17—The Open Source Investigation, Two Years Later," blog post, July 15, 2016. As of March 31, 2017: https://www.bellingcat.com/news/uk-and-europe/2016/07/15/mh17-the-open-source-investigation-two-years-later/

Blanchard, Ben, "China Says U.S. Hacking Accusations Lack Technical Proof," Reuters, Februry 20, 2013. As of March 31, 2017: http://www.reuters.com/article/us-china-hacking-idUSBRE91I06120130220

Buchanan, Ben, *The Legend of Sophistication In Cyber Operations*, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, January 2017. As of March 31, 2017: https://www.belfercenter.org/sites/default/files/files/publication/Legend%20Sophistication%20-%20web.pdf

Buratowski, Michael, "Findings from Analysis of DNC Intrusion Malware; Analyzing the DNC Malware," *Fidelis Cybersecurity*, blog post, June 20, 2016. As of March 31, 2017: https://www.fidelissecurity.com/threatgeek/2016/06/findings-analysis-dnc-intrusion-malware

Carr, Jeffrey, "Announcing Project Grey Goose—Operation Poachers," blog post, May 14, 2012. As of May 12, 2017: http://jeffreycarr.blogspot.com/2012/05/announcing-project-grey-goose-operation.html

———, "Mandiant APT1 Report Has Critical Analytic Flaws," blog post, February 19, 2013. As of March 31, 2017: http://jeffreycarr.blogspot.com/2013/02/mandiant-apt1-report-has-critical.html

Charney, Scott, Erin English, Aaron Kleiner, Nemanja Malisevic, Angela McKay, Jan Neutze, and Paul Nicholas, *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, Microsoft Corporation, June 2016. As of March 31, 2017: https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf

"China Opposes Hacking Allegation: FM Spokesman," *Xinhua*, February 19, 2013. As of March 31, 2017: http://news.xinhuanet.com/english/china/2013-02/19/c_132178666.htm

"Chinese Military Never Supports Cyberattacks: Defense Ministry," *Xinhua*, February 20, 2013. As of March 31, 2017: http://news.xinhuanet.com/english/china/2013-02/20/c_132180420.htm

Code of Federal Regulations, Title 12, Banks and Banking, Chapter II, Federal Reserve System (Continued), Subchapter B, Federal Open Market Committee, Part 271, Rules Regarding Availability of Information, January 1, 2016. As of March 31, 2017: https://www.gpo.gov/fdsys/search/pagedetails.action?sr=397&originalSearch=&st=his&ps=10&na=&se=&sb=re&timeFrame=&dateBrowse=&govAuthBrowse=&collection=&historical=false&packageId=CFR-2016-title12-vol4&fromState=&bread=true&granuleId=CFR-2016-title12-vol4-part271&collectionCode=CFR&browsePath=Title+12%2FChapter+II%2FSubchapter+B%2FPart+271

Common Vulnerabilities and Exposures, "About CVE," web page, February 23, 2017. As of March 31, 2017: https://cve.mitre.org/about/

Corera, Gordon, "How France's TV5 Was Almost Destroyed by 'Russian Hackers,'" BBC News, October 10, 2016. As of March 31, 2017: http://www.bbc.com/news/technology-37590375

Council of Europe, Treaty Office, "Convention on Cybercrime," Budapest, November 23, 2001. As of May 24, 2017: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

CVE—*See* Common Vulnerabilities and Exposures.

DeCianno, Jessica, "Indicators of Attack vs. Indicators of Compromise," *CrowdStrike*, blog post, December 9, 2014. As of March 31, 2017: https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/

Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, Washington, D.C.: U.S. Department of Defense, Task Force Report, January 2013. As of May 26, 2017: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA569975

Deibert, Ronald, "The DHS/FBI Report on Russian Hacking Was a Predictable Failure," *Just Security*, blog post, January 4, 2017. As of March 31, 2017: https://www.justsecurity.org/35989/dhsfbi-report-russian-hacking-predictable-failure/

DNI—*See* U.S. Office of the Director of National Intelligence.

Edwards, Benjamin, Alexander Furnas, Stephanie Forrest, and Robert Axelrod, "Strategic Aspects of Cyberattack, Attribution, and Blame," *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 114, No. 11, March 14, 2017, pp. 2825–2830. As of March 31, 2017: http://www.pnas.org/content/114/11/2825.abstract

Fagerland, Snorre, and Waylon Grange, *The Inception Framework: Cloud-Hosted APT*, Sunnyvale, Calif.: Blue Coat Systems, Inc., 2015. As of March 31, 2017: https://www.bluecoat.com/documents/download/638d602b-70f4-4644-aaad-b80e1426aad4/d5c87163-e068-440f-b89e-e40b2f8d2088

Farrell, Paul, "History of 5-Eyes—Explainer," *The Guardian*, December 2, 2013. As of March 31, 2017: https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer

FBI—*See* Federal Bureau of Investigation.

Federal Bureau of Investigation, "Update on Sony Investigation," press release, December 19, 2014. As of May 24, 2017: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

———, "A Primer on DarkNet Marketplaces," web page, November 1, 2016. As of March 31, 2017: https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces

Federal Open Market Committee, "FOMC Policy on External Communications of Federal Reserve System Staff," Washington, D.C., January 31, 2017.

Finkle, Jim,"Cyber Security Firm: More Evidence North Korea Linked to Bangladesh Heist," Reuters, April 3, 2017. As of May 24, 2017: http://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN1752I4

G20, "G20 Leaders' Communiqué, Antalya Summit, 15–16 November 2015," 2015 Turkey G20 web page, undated. As of March 31, 2017: http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/

Goodin, Dan, "'Guccifer' Leak of DNC Trump Research Has a Russian's Fingerprints on It," *Ars Technica*, June 16, 2016. As of March 31, 2017: https://arstechnica.com/security/2016/06/guccifer-leak-of-dnc-trump-research-has-a-russians-fingerprints-on-it/

GReAT, "BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents," *SecureList*, Kaspersky Lab website, January 28, 2016. As of March 31, 2017: https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

———, "Lazarus Under The Hood," *SecureList*, Kaspersky Lab website, April 3, 2017. As of March 31, 2017: https://securelist.com/blog/sas/77908/lazarus-under-the-hood/

Groll, Elias, "'Obama's General' Pleads Guilty to Leaking Stuxnet Operation," *Foreign Policy*, October 17, 2016. As of May 24, 2017: http://foreignpolicy.com/2016/10/17/obamas-general-pleads-guilty-to-leaking-stuxnet-operation/

———, "NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist," *Foreign Policy*, March 21, 2017. As of March 31, 2017: http://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/

Harold, Scott Warren, Martin C. Libicki, and Astrid Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica, Calif.: RAND Corporation, RR-1335-RC, 2016. As of March 31, 2017: http://www.rand.org/pubs/research_reports/RR1335.html

Healey, Jason, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Atlantic Council Issue Brief, Washington, D.C., 2011. As of March 31, 2017: http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF

Healey, Jason, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd, *Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security*, Washington, D.C.: Atlantic Council, November 2014. As of March 31, 2017: http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf

Hilton, Scott, "Dyn Analysis Summary of Friday October 21 Attack," *Company News*, Dyn blog post, October 26, 2016. As of March 31, 2017: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

Hirschfeld Davis, Julie, "Hacking of Government Computers Exposed 21.5 Million People," *New York Times*, July 9, 2015. As of March 31, 2017: https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

Industrial Control Systems Cyber Emergency Response Team, "Cyber-Attack Against Ukrainian Critical Infrastructure Alert (IR-ALERT-H-16-056-01)," US-CERT web page, February 25, 2016. As of March 31, 2017: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Internet Corporation for Assigned Names and Numbers, "About WHOIS," web page, undated. As of March 31, 2017: https://whois.icann.org/en/about-whois

INTERPOL, "Identifying Cybercriminals at Core of INTERPOL-Europol Conference," web page, September 28, 2016. As of May 30, 2017: https://www.interpol.int/News-and-media/News/2016/N2016-121

Kennedy, John, "The Five-Minute CIO: Alex Stamos, CSO, Facebook," *Silicon Republic*, November 11, 2016. As of May 26, 2017: https://www.siliconrepublic.com/enterprise/alex-stamos-security-facebookfive-minute-cio

Krebs, Brian, *Krebs on Security*, blog, undated. As of March 31, 2017: https://krebsonsecurity.com

Lee, Robert M., "Critiques of the DHS/FBI's GRIZZLY STEPPE Report," blog post, December 30, 2016. As of March 31, 2017: http://www.robertmlee.org/critiques-of-the-dhsfbis-grizzly-steppe-report/

Lema, Karen, "Bangladesh Bank Heist Was 'State-Sponsored': U.S. Official," Reuters, March 29, 2017. As of March 31, 2017: http://www.reuters.com/article/us-cyber-heist-philippines-idUSKBN1700TI

Leyden, John, "Russia's to Blame for Pro-ISIS Megahack on French TV Network," *The Register*, June 10, 2015. As of March 31, 2017: https://www.theregister.co.uk/2015/06/10/russian_trolls_staged_tv5monde_megahack_shocker/

Lin, Herbert, "Thoughts on Threat Assessment in Cyberspace," *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8, No. 2, 2012, pp. 337–355.

———, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Journal of International Affairs*, Winter 2016. As of March 31, 2017: https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents

Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, 2013.

Markoff, John, and David E. Sanger, "In a Computer Worm, A Possible Biblical Tale," *New York Times*, September 29, 2010.

Matlack, Carol, Michael Riley, and Jordan Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies," *Bloomberg Businessweek*, March 19, 2015. As of March 31, 2017: https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies

McLinn, James, "Major Power Outages in the U.S., and Around the World," in *IEEE Reliability Society 2009 Annual Technology Report*, 2009.

Morgan, Steve, "Cybersecurity Market Reaches $75 Billion in 2015; Expected to Reach $170 Billion by 2020," *Forbes*, December 20, 2015. As of March 31, 2017: https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#6d91f47e10c3

National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39, Gaithersburg, Md., March 2011. As of March 31, 2017: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

National Security Agency, "Signals Intelligence," web page, May 3, 2016. As of March 31, 2017: https://www.nsa.gov/what-we-do/signals-intelligence/

Norton-Taylor, Richard, "Titan Rain: How Chinese Hackers Targeted Whitehall," *The Guardian*, September 4, 2007.

Novetta Threat Research Group, "Operation Blockbuster: Unravelling the Long Thread of the Sony Attack," web page, February 24, 2016. As of March 31, 2017: http://www.novetta.com/2016/02/operation-blockbuster-unraveling-the-long-thread-of-the-sony-attack/

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, D.C.: National Academies Press, 2009.

Paganini, Pierluigi, "FireEye Claims Russian APT28 Hacked France's TV5Monde Channel," *Security Affairs*, June 10, 2015. As of March 31, 2017: http://securityaffairs.co/wordpress/37710/hacking/apt28-hacked-tv5monde.html

Perlroth, Nicole, and David E. Sanger, "Hackers Hit Dozens of Countries Exploiting Stolen NSA Tool," *New York Times*, May 12, 2017. As of May 25, 2017: https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html

Polityuk, Pavel, "Ukraine to Probe Suspected Russian Cyber Attack on Grid," Reuters, December 31, 2015. As of March 31, 2017: http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231

Rid, Thomas, and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, Vol. 38, Nos. 1–2, 2015.

Rogers, Marc, "No, North Korea Didn't Hack Sony," *Daily Beast*, December 24, 2014. As of March 31, 2017: http://www.thedailybeast.com/articles/2014/12/24/no-north-korea-didn-t-hack-sony

Sanger, David E., "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012. As of May 24, 2017: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Sanger, David E., and Martin Fackler, "NSA Breached North Korean Networks Before Sony Attack, Officials Say," *New York Times*, January 18, 2015. As of March 31, 2017: https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

Schmitt, Michael N., ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, England: Cambridge University Press, 2013.

Schneier, Bruce, "Did North Korea Really Attack Sony?" *The Atlantic*, December 22, 2014. As of May 24, 2017: https://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/

Segal, Adam, "The Continued Importance of the U.S.-China Cyber Dialogue," *Net Politics*, blog post, Council on Foreign Relations, January 23, 2017. As of March 31, 2017: http://blogs.cfr.org/cyber/2017/01/23/the-continued-importance-of-the-u-s-china-cyber-dialogue/

Shachtman, Noah, "Russia's Top Cyber Sleuth Foils U.S. Spies, Helps Kremlin Pals," *Wired*, July 23, 2012. As of March 31, 2017: https://www.wired.com/2012/07/ff_kaspersky/all/

Shevchenko, Sergei, and Adrian Nish, "Cyber Heist Attribution," *Threat Research*, BAE Systems blog, May 13, 2016. As of March 31, 2017: http://baesystemsai.blogspot.com/2016/05/cyber-heist-attribution.html

Shodan, homepage, undated. As of March 31, 2017: https://shodan.io

Smith, Brad, "The Need for a Digital Geneva Convention," *The Official Microsoft Blog*, February 14, 2017. As of March 31, 2017: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0000lgk5vy1e5he6gzh99xggdxmu5

Soltra, homepage, undated. As of May 26, 2017: https://www.soltra.com/en/

"Spelling Mistake Prevented Hackers Taking $1Bn in Bank Heist," Reuters via *The Guardian*, March 10, 2016. As of March 31, 2017: https://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist

Sterling, Bruce, "The Project Grey Goose Cyberwar Report," *Wired*, August 3, 2009. As of May 12, 2017: https://www.wired.com/2009/08/the-project-grey-goose-cyberwar-report/

Stoll, Clifford, *The Cuckoo's Egg*, New York: Doubleday, 2012.

Sulmeyer, Michael, and Amy Chang, "Three Observations on China's Approach to State Action in Cyberspace," *Lawfare*, blog post, January 22, 2017. As of March 31, 2017: https://www.lawfareblog.com/three-observations-chinas-approach-state-action-cyberspace

Symantec Security Response, "'Forkmeiamfamous': Seaduke, Latest Weapon in the Duke Armory," blog post, July 13, 2015. As of March 31, 2017: https://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory

———, "SWIFT Attackers' Malware Linked to More Financial Attacks," blog post, May 26, 2016. As of March 31, 2017: https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

Thornburgh, Nathan, "The Invasion of the Chinese Cyberspies," *Time*, August 29, 2005.

"ThreatExchange Documentation," web page, Facebook for Developers, undated. As of May 26, 2017: https://developers.facebook.com/docs/threat-exchange/v2.9

UN—*See* United Nations.

United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Report No. A/70/174, July 22, 2015. As of March 31, 2017: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

U.S. Department of Defense, *The DoD Cyber Strategy*, Washington, D.C., April 2015.

U.S. Department of Homeland Security, *National Cyber Incident Response Plan*, Washington, D.C., December 2016. As of March 31, 2017: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

U.S. Department of Homeland Security and the Federal Bureau of Investigation, *GRIZZLY STEPPE—Russian Malicious Cyber Activity*, Joint Analysis Report, December 29, 2016. As of March 31, 2017: https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

U.S. Department of Homeland Security and Office of the Director of National Intelligence, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security," October 7, 2016. As of March 31, 2017: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," No. 14–528, May 19, 2014. As of March 31, 2017: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

———, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 24, 2016. As of March 31, 2017: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

———, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 15, 2017. As of March 31, 2017: https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

U.S. House of Representatives, "FISA Amendments Act of 2008," HR 6304, July 10, 2008. As of March 31, 2017: https://www.congress.gov/bill/110th-congress/house-bill/6304

U.S. Office of the Director of National Intelligence, "Analytic Standards," Washington, D.C., Intelligence Community Directive 203, January 2, 2015. As of March 31, 2017: https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf

———, "Assessing Russian Activities and Intentions in Recent U.S. Elections," Washington, D.C., Intelligence Community Assessment, January 6, 2017.

U.S. Senate, *Foreign Cyber Threats to the United States*, hearing before the Committee on Armed Services, Washington, D.C., January 5, 2017. As of March 31, 2017: http://www.armed-services.senate.gov/hearings/17-01-05-foreign-cyber-threats-to-the-united-states

U.S. Supreme Court, "Frequently Asked Questions—General Information" web page, undated. As of March 31, 2017: https://www.supremecourt.gov/faq.aspx#faqgi9

Wilson, Kara, "In Case You Missed It: The FireEye Top Five Stories of the Week," *FireEye*, blog post, June 12, 2015. As of March 31, 2017: https://www.fireeye.com/blog/executive-perspective/2015/06/in_case_you_missedi0.html

Yadron, Danny, "When Cybersecurity Meets Geopolitics," *Wall Street Journal*, March 23, 2015. As of March 31, 2017: http://blogs.wsj.com/digits/2015/03/23/when-cybersecurity-meets-geopolitics/

YARA, "YARA in a Nutshell," web page, undated. As of March 31, 2017: http://virustotal.github.io/yara/

Zetter, Kim, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, New York: Crown, 2014a.

———, "The Evidence That North Korea Hacked Sony is Flimsy," *Wired*, December 17, 2014b. As of May 24, 2017: https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/

———, "That Insane, $81M Bangladesh Bank Heist? Here's What We Know," *Wired*, May 17, 2016. As of March 31, 2017: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

يتمثل تحديد مصدر الحادث الإلكتروني الخبيث في تحديد الجهة المسؤولة عن هذا النشاط. وتشكّل نتيجة تحديد مصدر الهجمات الإلكترونية شرطًا أساسيًا لمحاسبة الجهة الفاعلة على النشاط الخبيث. وقد حظيت في الآونة الأخيرة حوادث إلكترونية متعددة ذات تبعات جغرافية سياسية ونتائج تحديد المصدر المرتبطة بهذه الحوادث بتغطية صحافية بارزة. وقد عارضت شرائح متعددة من الرأي العام المصادر المُعلن عنها وشكّكت في موثوقيتها. ونستعرض في هذه الدراسة وضع تحديد مصدر الهجمات الإلكترونية وننظر في الآليات البديلة من أجل التوصّل إلى عملية موحّدة وشفافة لتحديد المصدر قادرة على تجاوز المخاوف المتعلقة بالموثوقية. وتتناول هذه الدراسة الاستطلاعية على وجه الخصوص القيمة التي تضطلع بها منظمة عالمية مستقلة تتمثّل مهمتها في التحقيق في الهجمات الإلكترونية الكبرى وتحديد مصدرها علنًا.

$20.00

ISBN-10 0-8330-9840-3
ISBN-13 978-0-8330-9840-5
52000
9 780833 098405

Arabic translation of *Stateless Attribution: Toward International Accountability in Cyberspace*
RR-2081/1-MS