إدارة الخطر السيبراني الوطني

إعداد ميليسا هاثاواي

مُقدمة

على مدى السنوات الثلاثين الماضية، ازداد اعتماد الحكومات والشركات والمواطنين على الإنترنت وعلى تقنيات المعلومات والاتصالات (ICTs) بشكل كبير. نحن نفترض أن الخدمات الأساسية المُقدمة للمواطنين مثل الكهرباء والاتصالات ستبقى تعمل على الدوام وأن البضائع والخدمات والبيانات ورؤوس الأموال ستعبر الحدود بكل سلاسة. ولكن، العديد من الأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر وتتعرض للاستغلال حيث تواجه شتى أنواع المؤسسات خروقات للبيانات وتتعرض لأنشطة إجرامية وتتعطل خدماتها وتُدمّر ممتلكاتها. وإحساسنا جميعاً بانعدام الأمن آخذ بالنمو. تتمتع أكثر من 100 دولة بالإضافة إلى عدد متزايد بسرعة من الجهات غير الحكومية والأفراد بالقدرة على إيذاء البنى التحتية المتصلة بالشبكات التابعة للحكومات ولقطاعات الصناعة. وتختلف أهداف هذه الجهات من جهة لأخرى وتتراوح من النشاط السياسي إلى الاحتيال والجريمة الإلكترونية وسرقة الممتلكات الفكرية (IP) والتجسس وتعطيل الخدمات وتدمير الممتلكات والأصول. تعيش الدول والشركات في عالم يسوده انعدام الأمن السيبراني – فجميع الحكومات والشركات التجارية والأفراد يواجهون مخاطر سيبرانية ويتشاطرون مستوى من المسؤولية في إدارة هذه المخاطر. وكما أكدّت الأحداث الأخيرة، ينبغي على الدول والشركات أن تدرك أولاً أن استراتيجيتها وأجندتها الرقمية ينبغي أن تكون قائمة على منهج منضبط لإدارة المخاطر. فالتراخي وعدم اتخاذ الإجراءات المناسبة له مخاطر جمّة.

يُحدد الخطر من حيث الوقت – أي عندما يكون شيء ما أو شخص ما عُرضة للخطر أو الأذى أو الخسارة[1]. وقد تتغير حالة الخطر بالاعتماد على الإجراءات التي يتخذها عدد لا يقل عن اثنين من الأطراف الفاعلة: أولاً المُهاجم الذي يحصل على القدرة لإحداث الأذى ويستخدمها، وثانياً الجهة المُستهدفة التي يمكنها اتخاذ الاحتياطات لتحمّل أو لإحباط الخطر الذي ينوي المُهاجم إحداثه. اعتمادنا على التقنية الرقمية آخذ بالنمو كل يوم، ولكن فهم المخاطر المرتبطة بهذا الاعتماد لا يزال في مراحله الأولى. مع ذلك، فإن الخطر السيبراني آخذ بالازدياد بسبب توفر سوق للبرامج والأدوات الخبيثة والخدمات غير المشروعة والبيانات الحسّاسة (غير المُتاحة للعامة) وبأسعار ميسورة. فعلى سبيل المثال، يمكن شراء برنامج خبيث مقابل دولار واحد ويمكن إطلاق هجمات الحرمان من الخدمات (DDoS) بأقل من ألف دولار. كما تتوفر هجمات برامج الفدية مقابل مئتي دولار وخدمات الرسائل الإلكترونية غير المرغوبة (سبام) بمبلغ أربعمائة دولار تقريباً. [2] كما يمكن أيضاً تنزيل أسلحة معقدة من خدمات الاستخبارات الحكومية [3]. يمكن لأي شخص ينوي شن هجمات ناجحة وإحداث الأذى الوصول لهذه القدرات. وكما أظهرت أحداث العام 2017، تعرضت حكومات وشركات وأفراد للأذى بفعل مجموعة من الهجمات السيبرانية هي الأكثر تطوراً لغاية يومنا هذا.

ففي مايو 2017، استهدف أحد برامج الفدية بعض الثغرات في أنظمة التشغيل "مايكروسوفت ويندوز" وأصاب الملايين من الحواسيب في 150 دولة في مختلف قطاعات الأعمال. وأدى هذا الهجوم العالمي – وهو عبارة عن برنامج فدية بسيط للغاية يُدعى WannaCry – إلى توقف عمليات التصنيع وأنظمة النقل وأنظمة الاتصالات. وفقاً لمكتب التدقيق الوطني في المملكة

[1] قاموس أكسفورد. المنشور الخاص للمعهد الوطني للمعايير والتقنية 30-800 (المراجعة أ) يُعرف الخطر بـ: الخطر = التهديد x نقطة الضعف. CRM تُعرّف بيانات الخطر بـ: الخطر = الحالة (الاحتمالية) + النتيجة (الأثر).

[2] نيكولاس راب وروبرت هاكيت، "أدوات الهاكرز." مجلة فورتشن 25 أكتوبر 2017. http://fortune.com/2017/10/25/cybercrime-spyware-marketplace/

[3] إدوارد كوفاكس، "شادو بروكرز يطالبون بـ 20,000$ لويكلي ليكس،" مجلة سيكيوريتي، 30 مايو 2017، https://www.securityweek.com/shadow-brokers-want-20000-monthly-leaks؛ وإدوارد كوفاكس، "شادو بروكرز يعدون بالمزيد من الاستغلالات مقابل رسوم شهرية،" مجلة سيكيوريتي، 16 مايو 2017، https://www.securityweek.com/shadow-brokers-promise-more-exploits-monthly-fee؛ ونيكول بيرلوث، "هجوم سيبراني "العالم غير جاهز له،"" نيويورك تايمز، 22 يونيو 2017، https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html?_r=0

المتحدة، أصاب برنامج WannaCry ما لا يقل عن 81 منظمة من منظمات هيئة الخدمات الصحية الوطنية البالغ عددها 236 منظمة مما عطّل المعدات الطبية عن العمل وأثر بشكل كبير على صحة وسلامة عامة الناس. [4]

في يونيو 2017، تم إطلاق NotPetya – وهو برنامج خبيث مُدمر آخر. تم إطلاق NotPetya بين الشركات التجارية العالمية المتصلة بالشبكات بواسطة آلية لتحديث البرامج لأحد برامج المحاسبة شائعة الاستعمال (doc.me). وفي غضون دقائق معدودة، أصاب البرنامج الخبيث عشرات آلاف الأنظمة المتصلة بالإنترنت في أكثر من 65 دولة، من بينها أنظمة تعود لمؤسسات حكومية ومصارف وشركات للطاقة وغيرها من الشركات. فعلى سبيل المثال، أدى هجوم NotPetya على A.P. Moller-Maersk- أكبر شركة للشحن في العالم – إلى تشفير ومسح أنظمة تقنية المعلومات الخاصة بالشركة في جميع أنحاء العالم. وعلى إثر ذلك، اضطرت Maerskلإيقاف عملياتها في معظم محطاتها المينائية الـ76 حول العالم مما أدى إلى تعطيل التجارة البحرية لأسابيع عدة. تجاوزت خسائر Maersk بفعل NotPetya 300 مليون دولار حيث اضطرت لإعادة بناء كامل بنيتها التحتية، بما في ذلك 4000 خادم جديد و45000 حاسوب جديد و2500 تطبيق جديد.[5] وتُقدر الخسائر التي تسبب بها NotPetyaبمليارات الدولارات بسبب تعطل الأعمال وتدمير الممتلكات في جميع أنحاء العالم.[6] وكانت الخسائر الأولية واللاحقة للاقتصاد الرقمي كبيرة واستغرق الأمر عدة أشهر للتعافي من الضرر الذي تعرضت له الخدمات والبنى التحتية الحسّاسة.

وفي حادثة مُقلقة أكثر، أُجبرت أحد مرافق النفط والغاز السعودية في أغسطس 2017 على الإغلاق. حيث وقعت ضحية لفيروس Trisis– وهو عبارة عن فيروس حاسوب متين صُمم لتخريب أنظمة التحكم الصناعية (ICS). صُمم هذا البرنامج – أو السلاح - الخبيث ليصيب العناصر التشغيلية من تقنية المعلومات في المواقع الصناعية مثل مرافق النفط والغاز والمياه وهو يستهدف خصيصاً آليات السلامة المادية (أنظمة إيقاف الطوارئ) الخاصة بأنظمة التحكم الصناعية. وبالرغم من أن هذا هو مثال واحد فقط للاستعمال الناجح لهذا البرنامج المُدمر، إلا أن Schneider Electricقد حذرت عملاء خدماتها الحسّاسة ومالكي البنى التحتية من التأكد من جهوزية أنظمتهم في حال فشل إحدى الأنظمة أو عدة أنظمة بفعل النشاطات الخبيثة في المستقبل.[7]

كان للنشاطات السيبرانية الخبيثة في عام 2017 أثر كبير من حيث الخسائر والأضرار التي تسببت بها، مع ذلك، كانت الأدوات التي استخدمت لإحداث الأذى بسيطة وغير معقدة. لقد تضاعف عدد الهجمات المُستهدفة لأنظمة الطاقة والاتصالات والنقل والأنظمة المالية في السنوات الخمس الأخيرة، ويشكّل هذا الاتجاه خطراً أمنياً اقتصادياً ووطنياً للجميع. لذا، هناك حاجة ماسة لقادة الحكومات والشركات للانخراط في العمليات الفعّالة لإدارة الخطر السيبراني ولمعالجة المخاطر الرقمية ضمن عملياتهم للتخطيط الاستراتيجي.

أطر العمل لفهم الخطر السيبراني

[4] مكتب التدقيق الوطني، "تحقيق: هجوم WannaCry السيبراني وهيئة الخدمات الصحية الوطنية ،" 27 أكتوبر 2017، https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

[5] ريتشارد شيرجون، ""أبطال" تقنية المعلومات ينقذون مايرسك من NotPetya بعد 10 أيام من إعادة تثبيت البرمجيات" ذا ريجستر، 25 يناير 2018، https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.

[6] NotPetya يُعطّل الأعمال ويُدمر أصول رؤوس أموال الشركات في مختلف أنحاء العالم. التقارير العامة من أي.بي. مولي-مايرسك، بالرسدورف، دي اتش ال، دي ال أي بايبر، فيدرال إكسبرس، ميرك، موندوليز، نوانس، ريكت بنكيسر جروب، روسنيفت، سانت جوبين، ودبليو بي بي تُظهر خسائر لا تقل عن 2.5 مليار دولار. تقرير حديث من لويدز لندن يُحذر من أن هجوم سيبراني مُحكم التنفيذ قد يتسبب بأضرار حول العالم تتراوح من 53.1 مليار دولار إلى 121.4 مليار دولار. أنظر لويدز لندن، "هجوم سيبراني خطير قد تبلغ تكلفته نفس تكلفة إعصار ساندي، "17 يوليو 2017، https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report.

[7] كيلي جاكسور هيجينز، "شنايدر إلكتريك: هجوم تريتون/ترايسيس استعمل خلل يوم الصفر في نظامه لمراقب السلامة بالإضافة إلى RAT، "دارك ريدينج، 18 يناير 2018، https://www.darkreading.com/vulnerabilities---threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845.

تعمل الدول والمنظمات الدولية والمؤسسات الأكاديمية على تطوير أطر عمل لمساعدة قادة الحكومات والشركات على تشخيص الخطر السيبراني وعلى خفضه. وهناك حاجة كبيرة لأطر العمل هذه لأنه على مدى العقود الثلاثة الماضية اقتنع نفس هؤلاء القادة بمزايا و "فوائد" تقنيات المعلومات التجارية، بما فيها زيادة الإنتاجية، وزيادة الفعالية، وانخفاض تكاليف المعدات الرأسمالية وتخزين البيانات ومعالجتها والنمو الصافي – ولكنهم أجّلوا الاستثمار في أمن ومرونة بناهم التحتية المتصلة بالشبكات ومؤسساتهم التجارية الرقمية. النشاطات السيبرانية المُدمرة والمُعطلة في يومنا هذا تُحتم على هؤلاء القادة مواجهة انعدام الأمن الذي زرعوه من دون قصد في صلب المجتمع. فالخسائر آخذة بالتراكم، والأذى آخذ بالنمو، والخطر مُحدق.

أطر العمل الحكومية

لقد بدأت الحكومات بتطوير أطر عمل وعلامات استدلالية واستراتيجيات وطنية واسعة لفهم مواضع اعتمادها على البنية التحتية للإنترنت ومواضع الضعف بشكل أفضل ومن أجل تأمين الشبكات والبنى التحتية والخدمات الوطنية التي يعتمد عليها مستقبلها الرقمي ورفاهها الاقتصادي. عندما يتعلق الأمر بالتخطيط وجذب الانتباه للخطر السيبراني لدولة ما يكون السؤال المُلح: كيف يمكن تشخيص وتقليص خطر تراكم على مدى 30 سنة؟ [8] من المهم البدء بفهم الخطة الاستراتيجية للدولة لـ 3-5 سنوات وتحديد الأمور التي يمكن القيام بها لتحقيق ذلك الهدف على المدى البعيد. على سبيل المثال، تشير تقديرات الهولنديين إلى أنه بحلول عام 2020، سيشكل الاقتصاد الرقمي (أي البضائع الرقمية والخدمات الإلكترونية) ما لا يقل عن 25 بالمائة من إجمالي الناتج المحلي للبلاد. وأكدت هولندا أن مستقبلها يعتمد على قدرتها على تأمين اقتصادها الرقمي، وهي تقوم ببعض الاستثمارات والإصلاحات الهيكلية الضرورية للتمكن من تحقيق ذلك الهدف. وتعمل بلدان أخرى، مثل الولايات المتحدة وألمانيا، على تحديد الشركات الكبرى التي تشكّل أكثر من 2 بالمائة من إجمالي الناتج المحلي للدولة وتعمل معها لتكون إدارة المخاطر والمرونة جزءاً من عملياتها الشاملة لتخطيط الأعمال. ولكن معظم الدول الأخرى قد اتخذت نهجاً أوسع وطالبت بحماية "البنى التحتية الحسّاسة" – أي الأصول والأنظمة والشبكات الأساسية التي يُعتقد بأنها أصبحت مع مرور الوقت غير حصينة للخطر دون غيرها من الشبكات من خلال ازدياد الترابط والاعتماد على الإنترنت، وبالتالي، تكون عرضة لفشل المعدات والخطأ البشري والأحوال الجوية والانقطاعات الأخرى الناجمة عن العوامل الطبيعية، والهجمات المادية والسيبرانية.[9] التحدي الذي يواجه هذا النهج هو عدم تحديد المسؤولية بشكل واضح بين الحكومة والقطاع مما يُصعب من تحميل المسؤولية لأي شخص بسبب تقاعسه. في هذه الأثناء، انعدام الأمن آخذ بالنمو في المجتمع نظراً لعدم وجود التزام بخفض الخطر وبزيادة المرونة.

قررت بعض الحكومات أن الوقت قد حان للتدخل في السوق وهي تستخدم أنظمة وقوانين لإلزام بعض القطاعات بتحديد وتقييم وتصحيح مواضع القصور في وضعها الأمني. وتشمل القطاعات الخاضعة للتنظيم: مرافق الكهرباء، الخدمات المالية، الرعاية الصحية، النقل والاتصالات. ومن بين الإجراءات التنظيمية الأخرى التي تتبناها الدول إلزام السلطات المحلية و/أو الوطنية بإرسال الإشعارات والتبليغ عن أي خرق يحدث مع ذكر نوع البيانات التي تعرضت للخطر أو التي فُقدت والتقنية أو الوسيلة المُستخدمة في الخرق، ومعلومات عن أي انقطاع أو تعطل للأعمال (الاتصالات) في حال وقوعه.

يفرض الاتحاد الأوروبي هذه الأنواع من المناهج الإلزامية على بناه التحتية الحسّاسة وعلى مُشغلي الخدمات الأساسية. وفي أغسطس 2016، تبنى الاتحاد الأوروبي نظاماً بعنوان "توجيه الاتحاد الأوروبي حول أمن الشبكات والمعلومات (*NIS*)". وضع هذا النظام قواعداً للأمن السيبراني – أو مجموعة من الضوابط الأمنية – للشركات التي تزوّد الخدمات المُصنفة كخدمات أساسية للمجتمع. وتشمل الخدمات التي يغطيها النظام خدمات الطاقة والنقل والصيرفة والتمويل والمياه والصحة بالإضافة إلى

[8] نطاقات المستوى الأعلى (مثل .mil، .com، .edu، .gov) دخلت حيز العمل في عام 1985 ومكنت إطار العمل للتجارة الإلكترونية العالمية. استمر الابتكار بتقديم تقنيات جديدة مثل إنشاء لغة ترميز النصوص التشعبية (HTML) في 1990 التي وسّعت من نطاق تبادل المعلومات بشكل سهل الاستخدام على الإنترنت – ومن ثم أصبحت تسمى بشبكة الإنترنت العالمية. وظهرت ابتكارات تقنية أخرى مثل: الرسائل القصيرة SMS (1992)، وبروتوكول الصوت على الإنترنت (1996) والوايفاي (1997)، وويكيبيديا (2001)، ومحرك البحث قوقل (1997)، وتقنية التواصل الاجتماعي (2002)، وبروتوكول الصوت والفيديو على الإنترنت مع سكايب (2003). القطاع الخاص يقود عجلة الابتكار وتبني التكنولوجيا ويعد بتخفيض التكاليف وبزيادة الإنتاجية وقابلية الاستعمال للمستهلكين دون نقاش يذكر حول الأمن. أنظر: ميليسا هاثاواي:"الوقوع ضحية للجريمة السيبرانية: المضاعفات على الأعمال والاقتصاد،" في تأمين الفضاء السيبراني: نطاق جديد للأمن الوطني، فبراير 2012، صحافة معهد أسبن.

[9] للعديد من الدول تعريفات مختلفة للبنى التحتية الحساسة. لأغراض إعداد هذا البحث، تم استعمال تعريف واسع النطاق. أنظر: المكتبة الرقمية لوزارة الأمن الداخلي، "توجيه القرار الرئاسي 63، PDD/NSC-63،" 22 مايو 1998، https://fas.org/irp/offdocs/pdd/pdd-63.htm.

القطاعات الرقمية مثل أسواق الإنترنت (مثل إيباي وأمازون)، ومحركات البحث (مثل قوقل) ومزودي الخدمات السحابية. وهناك مهلة لغاية شهر مايو 2018 للدول الأعضاء في الاتحاد الأوروبي لدمج هذا النظام ضمن قوانينها الوطنية. يتطلب توجيه أمن الشبكات والمعلومات من مشغلي الخدمات الأساسية في تلك الدول اتخاذ إجراءات أمنية مناسبة وإخطار السلطة الوطنية ذات الصلة (مثل السلطة المختصة أو فريق الاستجابة لحوادث أمن الحاسوب (((CSIRTحول أي حادث سيبراني خطير. ويفرض هذا النهج المُسائلة وقد يخفض الخطر السيبراني بسبب "إجباره" للقطاع على اتخاذ إجراءات لخفض مواضع الضعف ولزيادة المرونة.

وقد سلكت الصين نهجاً مماثلاً للنهج الذي سلكته أوروبا كما أنها أيضاً أضافت عناصراً من توجيه أمن الشبكات والمعلومات إلى قانونها الجديد الخاص بالأمن السيبراني الوطني الذي تبناه البرلمان الصيني في نوفمبر 2016 والذي أصبح نافذاً بشكل كامل في 31 ديسمبر 2017. يتكون القانون من سبعة فصول ومن 79 مادة، وهو "شامل ومتكامل" بحيث أنه يحدد مسؤوليات الوكالات الحكومية ذات الصلة ومزودي خدمات الإنترنت ومستخدمي الإنترنت. وينص القانون على أن الشركات – بتعريفها العام وغير الدقيق – مُلزمة باتخاذ تدابير تقنية وغيرها من التدابير الضرورية لضمان عمل الإنترنت بشكل آمن ومستقر، وللتعامل مع حوادث الأمن السيبراني بشكل فعال ولمنع النشاطات السيبرانية الإجرامية، وللحفاظ على سلامة وسريّة بيانات الإنترنت بالإضافة إلى قابليتها للاستعمال.[10] ويجبر هذا القانون الشركات على الاستثمار في وسائل حماية جديدة وعلى تركيب مجموعة من الضوابط لضمان هذه الأسس. كما يضم القانون نظاماً للفحص والتدقيق لضمان اتخاذ الشركات للتدابير المناسبة لخفض المخاطر ولإخضاعها للمسائلة في حال تبين عدم اتخاذها للتدابير الكافية.

لقد امتنعت الولايات المتحدة الأمريكية عن تبني نهج تنظيمي في هذا المجال، وبدلاً من ذلك دعت القطاع للاستثمار طوعاً في خفض الخطر السيبراني الذي يمكن أن تتعرض له البنى التحتية والخدمات الحسّاسة في الدولة. وفي فبراير 2013، طلب الرئيس من المعهد الوطني للمعايير والتقنية (NIST) إعداد مجموعة من المعايير والمنهجيات والإجراءات والعمليات التي تعمل على موائمة مناهج السياسات والأعمال والتقنية لمواجهة المخاطر السيبرانية. تم نشر "إطار العمل لتحسين الأمن السيبراني للبنى التحتية الحسّاسة" بعدها بعام واحد في فبراير 2014 وهو يحتوي على مجموعة من المعايير الطوعية التي تساعد المنظمات على تقييم الخطر الأمني السيبراني وعلى إدارته والاستجابة له. ويوجه إطار العمل المنظمات لتقييم الخطر تحت خمسة عناوين هي: التعرّف، الحماية، الكشف، الاستجابة والتعافي. وفقاً لبعض تقديرات القطاع، فإن 30% تقريباً من المنظمات الأمريكية (بما فيها الحكومة) تستخدم إطار العمل هذا للمساعدة في تقييم وضعيتها من الخطر وتتحمل هذه المنظمات قدراً أكبر من المسؤولية لحماية شبكاتها وبياناتها الحسّاسة من التطفّل أو التضرر أو التدمير.[11] علاوة على ذلك، يوضح المُلحق المرفق بهذه الوثيقة عدة معايير متنوعة مُتفق عليها دولياً حسب فئات خفض الخطر لإطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتقنية ((NIST. ولكن الدروس المُستقاة من الخروقات الأخيرة تشير إلى أن المنظمات التي تستعمل إطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتقنية ((NIST تُطبّق الفئات بهدف الامتثال بدلاً من تقييم الخطر على نحو مستمر. على سبيل المثال، قيّمت بعض المنظمات وضعيتها من ناحية الأمن والجاهزية باستعمال إطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتقنية ((NIST وكانت تعتقد بأنها قد حققت مستوى عالٍ من الأمن السيبراني، ولكنها مع ذلك تعرضّت لأذى كبير بفعل WannaCry و NotPetya.[12]

[10] لم يُحدد المسؤولون بعد عدد القطاعات التي سيشملها نطاق القانون. ولكن، العديد من الخبراء يعتقدون بأن هذا القانون يشمل نفس القطاعات التي يشملها توجيه الاتحاد الأوروبي لأمن معلومات الشبكات (مثل الطاقة والنقل والصيرفة والبنى التحتية للسوق المالي والبنى التحتية الرقمية والصحة والماء). أنظر يانشينج هونج، "التقييم الأمني لتدفق البيانات عبر الحدود: جزء هام من حماية الموارد الاستراتيجية الأساسية للصين،" 20 يونيو 2017، كلية القانون في ييل، بحث بول تساي شاينا سنتر، https://law.yale.edu/system/files/area/center/china/document/dataflowssecurity_final.pdf.

[11] المعهد الوطني للمعايير والتقنية (NIST)، ""روزيتا ستون" للأمن السيبراني تحتفل بعامين من النجاح،" 19 فبراير 2018، https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success.

[12] هاثاواي جلوبال ستراتيجيز ال ال سي. رؤى مكتسبة من العمل مع مجالس إدارة وإدارات الشركات المُتأثرة بالهجمات.

في سبتمبر 2017، نشر المعهد الوطني للمعايير والتقنية ((NIST مراجعات لمنشور آخر له حول "إطار عمل إدارة المخاطر لأنظمة المعلومات والمنظمات: منهجية دورة حياة النظام للأمن والخصوصية[13]." ويوصي إطار العمل هذا بعملية للمنظمات لتحديد الأصول عالية القيمة والأنظمة عالية الأثر لتتمكن من تقييم الخطر التشغيلي بشكل أفضل. كما يقدم هيكلاً لتحديد واختيار ضوابط الأمن والخصوصية ولتنفيذ وتقييم فعالية الضبط. ويُشدد إطار العمل على أهمية المراقبة المستمرة للخطر بالوقت الحقيقي بدلاً من الامتثال في نقطة زمنية ما. كما يعترف أيضاً بأن قرارات إدارة المخاطر هي جزء لا يتجزأ من وظائف الأعمال التجارية ومن إنجاز المهمة. ويتمم إطار العمل هذا "إطار العمل لتحسين الأمن السيبراني للبنى التحتية الحسّاسة" وعند تطبيقهما معاً فإنهما قد يزودان المنظمات بنهج أكثر استراتيجية لإدارة المخاطر.

أطر العمل الدولية

تُعبّر المنظمات الدولية عن آرائها في نقاش إدارة المخاطر السيبرانية وهي تعمل لتسريع تبني إجراءات فعّالة للأمن السيبراني باستعمال أطر أعمال وتوصيات خاصة بها. وبرز النقاش الدولي حول إدارة المخاطر بعد مرحلتين متتاليتين (2003 و 2005) من "القمة العالمية حول مجتمع المعلومات" (WSIS) – وهي عبارة عن تجمع عالمي لمجتمع "تقنيات المعلومات والاتصالات للتطوير". في ذلك الوقت، قررت 170 دولة على الأقل ضمان تمكن الجميع من الاستفادة من الفرص التي يمكن أن توفرها تقنيات المعلومات والاتصالات من خلال: تحسين الوصول إلى البنى التحتية وتقنيات المعلومات والاتصالات بالإضافة إلى المعلومات والمعرفة؛ وزيادة الثقة والأمن في مجال استعمال تقنيات المعلومات والاتصالات؛ وتطوير وتوسيع استعمالات تقنية المعلومات والاتصالات؛ وتشجيع التعاون الدولي والإقليمي.[14] ومنذ تلك اللحظة، سعت المؤسسات الدولية لتطوير ونشر أطر الأعمال لإدارة المخاطر التي قد تتعرض لها تقنيات المعلومات والاتصالات ولزيادة الثقة والمشاركة في الاقتصاد الرقمي العالمي.

وكانت منظمة البلدان الأمريكية (OAS) إحدى أوائل المنظمات الدولية التي تولت هذه المهمة. ففي عام 2004، بدأت منظمة البلدان الأمريكية (OAS) من خلال لجنة البلدان الأمريكية لمكافحة الإرهاب (CICTE) وبرنامج أمنها السيبراني برعاية تطوير أجندة الأمن السيبراني في القارتين الأمريكيتين. وتتعاون منظمة البلدان الأمريكية (OAS) مع مجموعة واسعة من الجهات الوطنية والإقليمية من القطاعين الحكومي والخاص حول كل من المسائل السياسية والتقنية، وتسعى لبناء وتقوية قدرات الأمن السيبراني في الدول الأعضاء من خلال المساعدة والتدريب التقنيين، واجتماعات المائدة المستديرة حول السياسات، وتمارين إدارة الأزمات، وتبادل الممارسات المُثلى المتعلقة بتقنيات المعلومات والاتصالات. وتستعمل منظمة البلدان الأمريكية (OAS) أطر عمل حكومية وأكاديمية للمساعدة في تعزيز بناء قدرات الأمن السيبراني وهي تساعد في تغيير الخطاب الوطني في الدول الأعضاء للاعتراف بوجوب تأمين اتصال الإنترنت – والبنية التحتية لتقنية المعلومات والاتصالات التي ترتكز عليها. في حال عدم استثمار الدول بشكل متساوٍ في أمن بناها التحتية الأساسية وفي مرونة أنظمتها، فإن التكاليف التي ستفرضها النشاطات السيبرانية الشنيعة ستشكل عبئاً ثقيلاً على نموها الاقتصادي.

في عام 2007، أعلن الاتحاد الدولي للاتصالات (ITU) – وهو وكالة مُتخصصة من وكالات الأمم المتحدة مسؤولة عن مسائل تقنية المعلومات والاتصالات – عن أجندته للأمن السيبراني العالمي (GCA) ونشر إطار عمل يُشجع على التعاون بين الأطراف. تضم أجندة الأمن السيبراني العالمي (GCA) خمس ركائز لإرشاد الدول في مجال بناء القدرات من أجل مجابهة الأمن السيبراني بشكل مسؤول. وتشمل هذه الركائز: (1) التدابير القانونية؛ (2) التدابير التقنية والإجرائية (3) الهياكل التنظيمية (4) بناء القدرات و (5) التعاون الدولي. وأدى إطار العمل هذا لاحقاً إلى إعداد الدليل الوطني للأمن السيبراني للاتحاد الدولي للاتصالات ((ITU في عام 2011 الذي يُركز على القيم والثقافة والاهتمامات الوطنية بكونها الركيزة الأساسية لإعداد استراتيجية وطنية فعّالة. كما يناقش إطار الدليل أيضاً مسائل هامة ينبغي على جميع الحكومات التصدي لها عند العمل على تحويل مسألة الأمن السيبراني من مجرد نقاش أو مشكلة تقنية إلى مجال إستراتيجي للسياسة الوطنية. بناءاً على هذه الجهود

[13] المعهد الوطني للمعايير والتقنية (NIST)، "المنشور الخاص للمعهد الوطني للمعايير والتقنية (NIST) 37-800 (المراجعة 2) مسودة – إطار عمل إدارة المخاطر لأنظمة المعلومات والمنظمات: : منهجية دورة حياة النظام للأمن والخصوصية (مسودة نقاش)، "سبتمبر 2017، https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf.

[14] القمة العالمية حول مجتمع المعلومات (WSIS)، جنيف 2003 – تونس 2005، "التزام تونس،" 18 نوفمبر 2005، http://www.itu.int/net/wsis/docs2/tunis/off/7.html.

الأولية، أطلق الاتحاد الدولي للاتصالات (ITU) مؤشر الأمن السيبراني العالمي (GCI) لمساعدة الدول على مقارنة برامجها الخاصة بالأمن السيبراني باستثمارات وبرامج الدول الأخرى. ويهدف هذا المؤشر إلى قياس مدى تطور الدولة أو مستوى "عافيتها" في الفئات الخمس لأجندة الأمن السيبراني العالمي (GCA) ألا وهي: التدابير القانونية، التدابير التقنية، التدابير التنظيمية، بناء القدرات والتعاون.[15] وكانت هذه المنهجية وهذا المؤشر إحدى أولى أطر العمل الدولية المتوفرة للقادة الدوليين ليعتمدوا عليها في إعداد استراتيجياتهم الوطنية ولقياس الخطر السيبراني بمصطلحات غير تقنية.

في عام 2015، تبنّى مجلس منظمة التعاون الاقتصادي والتنمية (OECD) ونشر توصية المنظمة حول إدارة مخاطر الأمن الرقمي لتحقيق الازدهار الاقتصادي والاجتماعي[16] من أجل توفير المعلومات اللازمة لتطوير الاستراتيجيات الوطنية التي تهدف لإدارة الأمن الرقمي ولتحسين الفوائد الاقتصادية والاجتماعية المتوقعة من الانفتاح الرقمي. يشجّع إطار العمل هذا الدول على تبني منهج يرتكز على إدارة المخاطر ويعتمد على إطار عمل مكوّن من ثمانية مبادئ عالية المستوى مترابطة ومتكاملة ومتممة لبعضها الآخر وهي (1) زيادة الوعي، واكتساب المهارات والتمكين؛ (2) مسؤولية أصحاب المصلحة؛ (3) حقوق الإنسان والقيم الأساسية؛ (4) التعاون؛ (5) تقييم المخاطر ودورة العلاج؛ (6) التدابير الأمنية المناسبة والمتناسبة مع الخطر والنشاط الاقتصادي والاجتماعي المُعرّض للخطر؛ (7) الابتكار؛ و (8) الجاهزية وتخطيط الاستمرارية. وفقاً لتوصيات منظمة التعاون الاقتصادي والتنمية (OECD) فإنه في حال نفّذ القادة هذه المبادئ الثلاثة إلى جانب أطر عمل دولية أخرى، فإن الدول ستكون قادرة على إعداد سياسات (واستراتيجيات) أفضل تقوم على إدارة المخاطر الأمنية الرقمية. المبادئ الثمانية هي ليست إطار عمل بحد ذاتها، بل هي عناصر رئيسية يمكن فيها تأسيس أو تحسين آليات التنسيق داخل الحكومة ومع أصحاب المصلحة غير الحكوميين. كما تعترف منظمة التعاون الاقتصادي والتنمية (OECD) بأن التعاون بين القطاعين الخاص والحكومي أساسي لخفض المخاطر السيبرانية.

في عام 2018، نشر المنتدى الاقتصادي العالمي ((WEFدليل المرونة السيبرانية للتعاون بين القطاعين الحكومي والخاص [17] - وهو عبارة عن أداة تهدف لتقديم إرشادات للتعاون بين القطاعين الحكومي والخاص داخل الدول حول إعداد سياسة للأمن السيبراني. يتطرق القسم 4.7 من الدليل، على وجه الخصوص، إلى الحاجة لتأسيس إطار عمل وطني واضح للحوكمة السيبرانية، بما في ذلك الأدوار والمسؤوليات والقدرات المتوقعة من القطاعين الحكومي والخاص. يهدف إطار العمل ذو الطبقات الثلاث والمقترح من قبل المنتدى الاقتصادي العالمي (WEF) إلى مساعدة الحكومات الوطنية على تعيين المسؤوليات وإلى موائمة الأدوار والمسؤوليات المُحددة بشكل أفضل مع ثلاث قدرات أمنية مميزة هي: المتانة والمرونة والدفاع – حيث كل واحدة منها تقوي القدرات الأخرى. تُعرّف المتانة بأنها "القدرة على منع وصد واحتواء التهديدات". وتُعرّف المرونة بأنها "إدارة الخروقات الناجحة والتعامل معها". بينما يُعرّف الدفاع بأنه "القدرة على استباق الهجمات وتعطيلها والاستجابة لها." [18] يبني إطار العمل هذا على مبادرات تعود لمجلس الأجندة الوطنية حول المخاطر والمرونة للمنتدى الاقتصادي العالمي ((WEFلعام 2014 وعلى الورقة البيضاء "فهم الخطر السيبراني النظامي" لعام 2016. وقدّم المنتدى الاقتصادي العالمي ((WEFنقاشات حول المخاطر السيبرانية وأجرى روابط مباشرة مع الآثار الاقتصادية والتبعات التجارية لانعدام الأمن السيبراني.

أطر عمل المجتمع التقني والأكاديمي

لقد بدأت المؤسسات الأكاديمية ومراكز البحوث والمجتمع التقني بالمساهمة وقد اقترحت منهجيات متنوعة لتسريع الجاهزية السيبرانية للدول والمنظمات بالإضافة إلى مستويات نضوجها.

---

[15] الاتحاد الدولي للاتصالات (ITU) (2014)، المؤشر العالمي للأمن السيبراني، https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx .

[16] مجلس منظمة التعاون الاقتصادي والتنمية (OECD) (2015)، إدارة مخاطر الأمن الرقمي لتحقيق الازدهار الاقتصادي والاجتماعي: توصية مجلس منظمة التعاون الاقتصادي والتنمية (OECD) والوثيقة المرفقة، نشر مجلس منظمة التعاون الاقتصادي والتنمية (OECD)، باريس، https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

[17] المنتدى الاقتصادي العالمي (WEF) (2018) دليل المرونة السيبرانية للتعاون بين القطاعين الحكومي والخاص ص. 33-36، https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration.

[18] نفس المصدر.

تم نشر مؤشر الجاهزية السيبرانية 2.0 (CRI 2.0)[19] بواسطة فريق من الخبراء في معهد بوتوماك للدراسات السياسية في عام 2015، وهو يبني على مؤشر الجاهزية السيبرانية 1.0 الذي صدر عام 2013 والذي قدّم إطار عمل منهجي لتقييم الجاهزية السيبرانية. يُقدّم مؤشر الجاهزية السيبرانية 2.0 منهجية شاملة ونسبية وقائمة على التجارب لتقييم التزام الدول ومستوى نضجها في سد الفجوة بين وضعها الحالي بالنسبة للأمن السيبراني وبين القدرات السيبرانية الوطنية اللازمة لدعم مستقبلها الرقمي. ويستخدم مؤشر الجاهزية السيبرانية 2.0 أكثر من سبعين مُؤشر فريد من نوعه موزعين على سبعة عناصر أساسية لتمييز النشاطات الجاهزة من الناحية التشغيلية ولتحديد المجالات التي ينبغي تحسينها في الفئات التالية: (1) الاستراتيجية الوطنية؛ (2) الاستجابة للحوادث؛ (3) الجريمة الإلكترونية وتطبيق القانون؛ (4) تبادل المعلومات؛ (5) الاستثمار في البحث والتطوير؛ (6) الدبلوماسية والتجارة؛ و (7) الدفاع والاستجابة للأزمات. ويوفر المخطط الناتج والقابل للتنفيذ خريطة طريق لخفض المخاطر لتتبعها الدول. والأهم من ذلك، يربط مؤشر الجاهزية السيبرانية 2.0 بين النمو الاقتصادي والتنمية وبين سياسات الأمن الوطني. كما يقر بأن تحقيق القدرة الكاملة لاقتصاد الإنترنت من ناحية نمو الناتج المحلي الإجمالي، وزيادة الإنتاجية والكفاءة، وتحسين مهارات القوى العامة، وتحسين الوصول للأعمال التجارية والبيانات يتطلب الموائمة بين استراتيجيات التنمية الاقتصادية وبين أولويات الأمن الوطني. بمعنى آخر، تقنيات المعلومات والاتصالات لا يمكنها تحقيق النمو الاقتصادي في حال عدم وضع سياسات وعمليات وتقنيات لحماية وتأمين البنية التحتية السيبرانية والخدمات التي يعتمد عليها مستقبل الدولة الرقمي ونموها. ويُركّز مؤشر الجاهزية السيبرانية 2.0 على الأدوات التي يمكن لقادة العالم الاستفادة منها، بما في ذلك السياسات، والتشريعات، والأنظمة، والمعايير، وحوافز السوق، والمبادرات الأخرى لحماية قيمة استثماراتهم الرقمية ولمعالجة التآكل الاقتصادي المستمر الناجم عن انعدام الأمن السيبراني .

تم نشر نموذج أوكسفورد لنضج قدرات الأمن السيبراني ((CMM في عام 2016 بواسطة مركز قدرات الأمن السيبراني (GCSCC) في جامعة أوكسفورد، وهو يصوّر مستويات متفاوتة لنضج الأمن السيبراني لدى الدول المختلفة بالاعتماد على خمسة أبعاد للقدرات هي: (1) سياسة واستراتيجية الأمن السيبراني؛ (2) الثقافة السيبرانية والمجتمع؛ (3) الأمن والتعليم والتدريب والمهارات السيبرانية؛ (4) أطر العمل القانونية والتنظيمية؛ و (5) المعايير والمنظمات والتقنيات. وكل واحدة من هذه الأبعاد ينقسم إلى عوامل ومؤشرات أكثر تحديداً تدل، عند النظر إليها جميعاً، على مستوى نضج قدرات الأمن السيبراني الخاصة بالدولة. يستخدم نموذج أوكسفورد لنضج قدرات الأمن السيبراني ((CMMوسيلتين للمساعدة في تشخيص الجاهزية السيبرانية. تستخدم الوسيلة الأولى أداة للاستقصاء (شبيهة بالاتحاد الدولي للاتصالات (ITU)) حيث يمكن للدول تشخيص جاهزياتها بنفسها. ومن ثم تتم مراجعة إجابات الاستقصاء وتشارك إحدى الفرق في ورشة عمل تقنية مع أصحاب المصلحة السيبرانيين الرئيسيين من الحكومة والمؤسسات الأكاديمية ومن القطاعين الحكومي والخاص لتقييم مستوى القدرات السيبرانية بشكل أفضل على خمس مستويات من النضج السيبراني (هي: المستوى الابتدائي، المستوى التكويني، المستوى القائم، المستوى الاستراتيجي، والمستوى الديناميكي). نموذج أوكسفورد لنضج قدرات الأمن السيبراني ((CMM هو عبارة عن أداة ممتازة لقياس مستوى فهم أصحاب المصلحة الرئيسيين للوضع الحالي للقدرات السيبرانية ولمستوى نضج الدولة مما يوفر أساساً لأهداف السياسات المستقبلية ولنتائج خفض المخاطر.

في الختام، أطلقت أكاديمية الحوكمة الإلكترونية في استونيا المؤشر الوطني للأمن السيبراني (NCSI) خلال مؤتمر تالين للحوكمة الإلكترونية في شهر مايو 2016 وقامت بتحديث وتعديل المنهجية لتُصدر إصداراً جديداً في شهر يناير 2018.[20] تتضمن المنهجية الدروس التي استقتها استونيا كواحدة من أوائل الدول المتبنية للحوكمة الإلكترونية لمجتمع بأكمله. ويتضمن الإصدار 2.0 من المؤشر الوطني للأمن السيبراني (NCSI) اثني عشر من مجالات القدرات و46 مؤشراً للمساعدة في تقييم قدرة الدولة، على المستوى الوطني، على بناء دولة إلكترونية "آمنة" تعمل على تأمين البيانات والمعاملات وفي الوقت نفسه تقلص من مستوى الخطر الذي تتعرض له الدولة. مجالات التقييم الاثني عشر هي: (1) القدرة على إعداد سياسات وطنية للأمن السيبراني؛ (2) القدرة على تحليل التهديدات السيبرانية على الصعيد الوطني؛ (3) القدرة على تقديم التعليم في مجال الأمن

---

[19] مؤشر الجاهزية السيبرانية 2.0 يبني على الإصدار السابق من مؤشر الجاهزية السيبرانية 1.0 الذي قدّم إطار عمل منهجي لتقييم الجاهزية السيبرانية من خلال خمسة عناصر أساسية هي: الاستراتيجية السيبرانية الوطنية، والاستجابة للحوادث، والجريمة الإلكترونية والقدرات القانونية، وتبادل المعلومات، والبحث والتطوير السيبراني. طبّق مؤشر الجاهزية السيبرانية 1.0 هذه المنهجية على مجموعة أولية مكونة خمسة وثلاثين دولة. للمزيد من المعلومات حول مؤشر الجاهزية السيبرانية 1.0 أنظر: ميليسا هاثاواي، "مؤشر الجاهزية السيبرانية 1.0،" هاثاواي جلوبال ستراتيجيز ال ال سي (2013)، *http:// belfercenter.ksg.harvard.edu/ les/ cyber-readiness-index-1point0.pdf.*

[20] المؤشر الوطني للأمن السيبراني (NCSI)، "منهجية المؤشر الوطني للأمن السيبراني ((NCSI، http://ncsi.ega.ee/methodology " (1.0) و (2.0) http://ncsi.ega.ee/ncsi-methodology-2-0-launched/

السيبراني؛ (4) القدرة على تأمين خط قاعدي للأمن السيبراني؛ (5) القدرة على توفير بيئة آمنة للخدمات الإلكترونية؛ (6) القدرة على تقديم خدمة إلكترونية لإثبات الهوية والتواقيع الإلكترونية؛ (7) القدرة على حماية البنى التحتية للمعلومات الحسّاسة؛ (8) القدرة على الكشف عن الحوادث السيبرانية والاستجابة لها 24 ساعة في اليوم 7 أيام في الأسبوع؛ (9) القدرة على إدارة أزمة سيبرانية واسعة النطاق؛ (10) القدرة على محاربة الجرائم السيبرانية؛ (11) القدرة على إجراء العمليات العسكرية للدفاع السيبراني و (12) القدرة على توفير الأمن السيبراني العالمي. يتضمن المؤشر الوطني للأمن السيبراني (NCSI) العديد من العناصر المماثلة لأطر العمل الأخرى ولكنه يحتوي على أقسام مميزة خاصة بتجربة استونيا في مجال الحوكمة الإلكترونية مثل كيفية بناء بيئة آمنة للخدمات الإلكترونية وكيفية توفير الخدمة الإلكترونية لإثبات الهوية والتواقيع الإلكترونية.

مُلخّص إطار العمل

لكل إطار عمل منهج مختلف للمساعدة في تعزيز الوضعية العامة للدولة من ناحية الأمن السيبراني ولإدارة الخطر السيبراني على المستوى الوطني. وهناك قواسم مشتركة عديدة بين أطر العمل هذه مثل: الاعتراف على نطاق واسع بأن الأمن الوطني للدول ورفاهها الاقتصادي، في العصر الحديث، يعتمدان بشكل كبير على القدرة على تأمين بناها التحتية السيبرانية الوطنية واقتصاداتها الرقمية؛ والحاجة لتعزيز الأمن السيبراني على أعلى مستويات قيادات الحكومات والمؤسسات؛ ومُتطلب البدء بحماية البنى التحتية والخدمات الأساسية الأكثر حساسية؛ ومتطلب تطوير أطر العمل القانونية والتنظيمية المناسبة لحماية المجتمع من الجريمة السيبرانية ومن تعطل الخدمات وتدمير الممتلكات؛ والحاجة للتعاون بين القطاعين الحكومي والخاص بالإضافة إلى المجتمعات الدولية والإقليمية من أجل ضمان تبني استراتيجيات فعّالة لإدارة المخاطر والمرونة؛ والالتزام بتطوير القدرات الوطنية الضرورية لزيادة الثقة والأمن في مجال استعمال تقنيات المعلومات والاتصالات، وتصحيح النقائص، والاستجابة لمخاطر الأمن السيبراني الهامة.

التمتع بالجاهزية السيبرانية – إدارة الخطر

بالرغم من توفر العديد من النماذج وأطر العمل في وقتنا هذا لقادة الدول ليقوموا بتشخيص وخفض الخطر السيبراني في بلادهم، وبالرغم من الدعوات العديدة من أخصائيي هذا المجال ومن خبراء الأمن السيبراني لاتخاذ الإجراءات المناسبة، إلا أن تحسين مستوى الأمن السيبراني على المستوى الوطني لا يزال يشكل تحدياً. على سبيل المثال، اعترفت هولندا بأن صحة الاقتصاد في المستقبل تعتمد على الاقتصاد الرقمي الموثوق وحسن الأداء، وبالتالي خصصت الأموال المناسبة وقامت بتأسيس مركز لضمان تحقيق الدولة لأهدافها بشكل آمن. في شهر يوليو 2015، أجرى المنسق الوطني للأمن ومكافحة الإرهاب "مراجعة لسياسة البنى التحتية الحسّاسة". وفي تلك المراجعة، عرّفت الحكومة البنى التحتية الحسّاسة بأنها "مجموعة من المنتجات والخدمات والعمليات التابعة الضرورية لعمل الدولة [وأنها] ينبغي أن تكون آمنة وأن تتمكن من الصمود ومن التعافي بسرعة من جميع المخاطر."[21] ولكن، عندما تأثر ميناء روتردام – أكبر ميناء في أوروبا – بشكل كبير وانشلت خدماته بفعل NotPetya في 2017، بدأ المسؤولون بفحص وضعية الميناء من حيث مواضع اعتماده على الإنترنت واكتشفوا أن البنية التحتية للميناء لم تكن تُعتبر من بين البنى التحتية الحسّاسة في استراتيجيتهم الوطنية للأمن السيبراني وفي سياساتهم لحماية البنى التحتية.

وفي الوقت نفسه، حتى المملكة المتحدة التي حددت قطاعات حسّاسة مُعينة مثل قطاع الرعاية الصحية – الذي ينبغي أن يتماشى مع معيار مُحدد للرعاية – لم تعتقد بأن مزودي خدمات الرعاية الصحية فيها مستعدين للاستثمار لتحديث برمجياتهم ولحماية خدمات المرضى الحسّاسة من المخاطر السيبرانية. وبالتالي، عندما وقعت أكثر من 81 منظمة من منظمات هيئة الخدمات الصحية الوطنية البالغ عددها 236 منظمة ضحية لبرنامج الفدية البسيط - WannaCry- أدت هذه الحادثة البسيطة التي كان بالإمكان تفاديها بكل باسطة إلى تعريض حياة الناس للخطر. ونتيجة لذلك، أُجبرت المملكة المتحدة على التأكد فيما إن كان برنامجها السيبراني كافياً وإن كانت هناك حاجة للمزيد من التدخل والاهتمام الحكوميين لإدارة الخطر الذي قد تتعرض له الدولة ومواطنيها.

[21] المُنسّق الوطني للأمن ومكافحة الإرهاب، "مراجعة حول البنى التحتية الحسّاسة،" يوليو 2015؛ وميليسا هاثاواي وفرانشسكا سبيدالييري، "نظرة على الجاهزية السيبرانية في هولندا،" مايو 2017، معهد بوتوماك للدراسات السياسية، http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf

كما ذُكر سابقاً، حددّت ألمانيا والولايات المتحدة مجموعة من الشركات التي تُساهم بما لا يقل عن 2 بالمائة من الناتج المحلي الإجمالي للدولة والتي تستحق المزيد من الحماية والتعاون/تبادل المعلومات مع الحكومة، ولكن مع ذلك، لم يحمي تبادل المعلومات بين الحكومة والقطاع هذه الشركات من الوقوع ضحية للطبيعة المُدمرة لـ .NotPetyaفبالرغم من أن الدولتان لديهما عمليات لتبادل المعلومات حول التهديدات والمعلومات الاستخبارية – وبالتالي "تحذير" القطاع الذي قد يكون عُرضة للهجوم، إلا أنه لم يتم إرسال أي تحذير بالخطر الوشيك في هذه الحالة. ونتيجة لذلك، تأثرت الشركات التي تقع مقراتها في كلتا الدولتين بشكل كبير وتعرّضت التجارة الإلكترونية العالمية لتأخيرات لمدة أسابيع وأشهر بسبب نقص جاهزية هذه الشركات وعدم توفر الدعم المناسب من حكوماتها. وأخيراً، أجبرت شركات الطاقة الرئيسية في السعودية – والتي توفّر الطاقة لحوالي 25 بالمائة من أنظمة النقل العالمية العاملة بالغاز الطبيعي السائل والوقود – على التوقف عن العمل بسبب نشاطات سيبرانية خبيثة أثرّت في نهاية المطاف على أنظمة النقل العالمية وعلى الاقتصاد العالمي.

وكما توضح هذه الأمثلة، لا توجد أي دولة تتمتع بالجاهزية السيبرانية. وينبغي أن تبدأ الجاهزية من خلال منهجية مُنضبطة لإدارة المخاطر. الإدارة الفعّالة للمخاطر تتطلب من قيادة الدولة قبل كل شيء فهم الأصول الأعلى قيمة في البلاد وتحديد الأصول الأهم والأجدر بالحماية، وإثبات استعدادها لاستثمار رأس المال السياسي والوقت التنفيذي والمال والموارد اللازمة لحمايتها.

على سبيل المثال، أطلقت كولومبيا منهجية لإدارة المخاطر لتقييم جاهزيتها السيبرانية ولتعزيز ثقة المجتمع باستعمال البيئة الرقمية. وكانت هذه الجهود نتيجة المهام الواردة في السياسة الكولومبية الوطنية للأمن الرقمي (الاستراتيجية الوطنية للأمن السيبراني) التي تمت الموافقة عليها في أبريل 2016 من قبل المجلس الوطني للأمن الرقمي من خلال إصدار وثيقة CONPES 3854 عام 2016. وتبنت كولومبيا إرشادات منظمة التعاون الاقتصادي والتنمية (OECD) لإدارة المخاطر واستخدمت إطار العمل ذلك إلى جانب توصيات من منظمة البلدان الأمريكية (OAS) والاتحاد الدولي للاتصالات (ITU) ومنظمة حلف شمال الأطلسي (NATO) لتقييم التهديدات الرقمية التي تواجه الدولة وفهم الأصول الحسّاسة المعُرضة للخطر. [22] ودفعت الدراسة بالدولة لتقييم المخاطر السيبرانية الأكثر إلحاحاً وللتعرّف على كيفية تأثير الحوادث السيبرانية على المنظمات الكولومبية في كل من القطاعين الخاص والعام، ولجعل الأمن السيبراني أولوية وعنصراً قوياً في تنميتها الاجتماعية والاقتصادية. كما ساعدت أيضاً في زيادة الوعي بين مختلف أصحاب المصلحة في الدولة حول الأنواع الشائعة والفريدة من الحوادث والتهديدات والهجمات السيبرانية التي تصيب مؤسسات القطاع العام والشركات وبدأت بحساب التكاليف التي يتكبدها اقتصاد الدولة بفعل هذه الحوادث. اعترفت كولومبيا بأن إدارة المخاطر السيبرانية على المستوى الوطني هي متطلب أساسي لرقمنة القطاع وللتحول الرقمي للدولة.

تبرز تجربة كولومبيا أن إدارة المخاطر تبدأ بالقيادة والحوكمة. وكما هو حال معظم أطر العمل والمؤشرات والأدلة الصادرة عن مختلف المنظمات بين الحكومية، تُشدد المجتمعات الأكاديمية والتقنية في السنوات الأخيرة على أهمية تقييم الأمور المعُرضة للخطر وعلى وضع الأمن السيبراني على قمة سلّم أولويات الاستراتيجية الأمنية للدولة. ولكن، من غير الكافي إعطاء الأولوية للأمن السيبراني في فئة واحدة دون غيرها والتعامل مع الأمر على أنه مسألة أمن وطني. فالأمن السيبراني، في الواقع، متشابك بشكل وثيق مع الاتصال بالإنترنت ومع التبني السريع لتقنيات المعلومات والاتصالات التي – عندما تكون آمنة ومرنة – تؤدي إلى النمو والازدهار الاقتصاديين. بالتالي، فإن موائمة المبادرات الاقتصادية مع الأمن والتنمية والمرونة – تقييم القيمة المعرضة للخطر ووضع سياسة وطنية تدير نشاطات خفض المخاطر - له نفس القدر من الأهمية.

تقييم الخطر

ينبغي على قادة الدول ذكر نيتهم بوضوح للاستفادة من البيئة الرقمية لتحقيق الازدهار الاقتصادي والاجتماعي من خلال خفض المستوى العام لخطر الأمن الرقمي داخل الحدود وعبرها. وينبغي أن يدركوا أن الخطر يتغير مع مرور الوقت بالاعتماد على الإجراءات التي يتخذهما طرفان على الأقل هما: المهاجم الذي يحصل على القدرة لإحداث الأذى ويستخدمها، والطرف المُستهدف الذي يمكنه أخذ الاحتياطات لتحمل أو لإحباط الخطر الذي يتسبب به المهاجم. ينبغي على قادة الدول ابداء التزامهم

[22] OAS, MINTIC, IDB (2017)، آثار حوادث الأمن الرقمي في كولومبيا 2017، https://publications.iadb.org/handle/11319/8552.

بخفض المخاطر وبزيادة المرونة من خلال إجراء تقييمات مستمرة للخطر على الصعيدين الوطني والقطاعي وتبني الإجراءات والسياسات والعمليات المناسبة لإدارة المخاطر التي يتم تحديدها.

من أجل تحقيق هذه الأهداف الشاملة، ينبغي على قادة الدول وعلى صانعي السياسات وأصحاب المصلحة المعنيين الآخرين في كل دولة العمل معاً لتقييم الخطر. التخطيط الاستراتيجي والتفكّر يساعدان على تحديد حالة الجاهزية:

- ما هي الاستراتيجية طويلة وقصيرة الأمد للدولة، بما في ذلك السياسات الصناعية والأهداف الاقتصادية وأولويات الأمن الوطني؟
- ما الذي قد يُعرّض هذه الأهداف للخطر؟ بمعنى آخر، ما نقاط الضعف التي يمكن استغلالها؟ (أي الأصول عالية القيمة المُهملة) التي قد تُعطّل تنفيذ هذه الأهداف؟
- هل توجد خطوط واضحة للمسائلة والمسؤولية لضمان تنفيذ أهداف الدولة وتطبيق إجراءات خفض المخاطر؟
- هل كانت اعتبارات الأمن السيبراني والمرونة جزءاً أساسياً من عملية التخطيط؟

هذا التقييم الشامل والمتكامل سيُبرز مواضع الاعتماد الرقمي الأكثر حساسية في الدولة (أي الشركات والخدمات والبنى التحتية والأصول) التي إن تعرضت للأذى، سيكون لذلك عواقب وخيمة على اقتصاد وأمن الدولة. لن يتمكن صنّاع القرار من اتخاذ الإجراءات التصحيحية لإحباط أو خفض المخاطر إلا بعد تحديد الأمور غير الحصينة، وما قد يُهدد أثمن أصول الدولة، واحتمالية تعرّضها للخطر أو الأذى أو الضياع.

خفض المخاطر من خلال التخطيط الدقيق

بعد الانتهاء من إجراء تقييم المخاطر، يمكن للدولة وضع خطة لخفض المخاطر لسد الفجوة بين وضعيتها الحالية من ناحية الأمن السيبراني وبين القدرات السيبرانية الوطنية اللازمة لتصحيح مواضع القصور ولدعم مستقبل الدولة الاقتصادي وأولوياتها الأمنية. وينبغي أن تكون جهود خفض المخاطر بقيادة سلطة وطنية كفوءة ومُختصة في مجال الأمن السيبراني – أي قائد (شخص أو مؤسسة على حد سواء) ذو مكانة عالية وراسخة في أعلى درجات الحكومة لتقديم التوجيهات ولتنسيق الإجراءات ولمراقبة تنفيذ الخطة بحيث يكون خاضعاً للمسائلة بالنسبة لمواضع القصور وللنتائج المُتحققة. بما أن الأمن السيبراني يتقاطع مع العديد من المجالات الأخرى (مثل حقوق الإنسان، والتنمية الاقتصادية، والتجارة، وضبط الأسلحة والاستعمال المزدوج للتقنيات، والأمن، والاستقرار، والسلام وحل النزاعات)، من الهام ضمان تمتع السلطة الوطنية المُختصة بالسلطة الموضعية وبالمسائلة وبالتمكين لضم وتوجيه العدد اللازم من أصحاب المصلحة.

بالرغم من كثرة التوجيهات المتعلقة بنشاطات خفض المخاطر كما يتضح من أطر العمل المتنوعة الموضحة في الأقسام السابقة، إلى أنه ينبغي على قادة الدول بذل جهود أكبر لفهم طبيعة الخطر السيبراني والتهديدات المُحددة التي تواجه البنى التحتية المتصلة بالشبكات – والتي ينبغي أن توصف بدقة ووضوح في استراتيجياتهم للأمن السيبراني الوطني وفي تقييم/تقييمات الخطر السيبراني الوطني – ومن ثم العمل مع جميع أصحاب المصلحة المعنيين لتخطيط دفاعاتهم بشكل أفضل ولتعيين الموارد البشرية والمالية لخفض تلك المخاطر. وتشمل الاستراتيجيات الشائعة لخفض المخاطر السيبرانية بشكل فعّال:

- تحديد الأمور المُعرضة للخطر وزيادة الوعي العام بالمخاطر في جميع المستويات – من قادة الحكومات إلى المواطن العادي. لا يمكن للناس إعطاء الأهمية للأمن من دون أن يفهموا أولاً مدى تعرض نشاطاتهم اليومية (وليس مجرد معلوماتهم الشخصية) للخطر. بالتالي، ينبغي أن تبادر الحكومة بإنشاء حملة وطنية لزيادة الوعي العام وتعزيز التعليم والتدريب وتنمية المهارات وتمكين مواطنيها ليصبحوا جزءاً من الحل ببناء ثقافة قوية للأمن السيبراني.
- تحديد الموارد اللازمة وترتيبها حسب الأولويات المطلوبة وتركيزها على الأصول عالية القيمة وعلى الأنظمة ذات الأثر العالي التي تتطلب مستويات إضافية من الحماية وعلى الجهات الأكثر حساسية في الدولة المعتمدة على التقنية الرقمية (مثل الشركات والبنى التحتية والخدمات والأصول)؛ وفهم نقاط ضعفها، وإعطاء الأولوية للإجراءات الأمنية المناسبة والمتناسبة مع الخطر الاقتصادي المجتمعي.
- إعداد أطر عمل قانونية وتنظيمية مناسبة لحماية المجتمع من الجريمة السيبرانية ومن انقطاع الخدمات وتدمير الممتلكات.

- استعمال نطاق واسع من الأدوات، بما فيها السياسات والتشريعات والأنظمة والمعايير وحوافز الأسواق ومشاريع الامتثال الطوعي وغيرها من المبادرات من أجل زيادة مستوى الأمن والثقة باستخدام تقنيات المعلومات والاتصالات بالإضافة إلى تصحيح مواضع القصور في العمليات والمنتجات (مثل توجيه الشبكات وأنظمة المعلومات (NIS) وقانون الصين للأمن السيبراني وإطار عمل المعهد الوطني للمعايير والتقنية (NIST)).
- تحسين الوعي الظرفي، ومؤشرات التهديدات، والتحذيرات من خلال المراقبة المستمرة للكشف عن التهديدات التي قد تصيب المجتمع الشبكي واستعمال أحدث التقنيات للكشف عن مثل هذه التهديدات ولصدها واحتوائها.
- تطوير القدرات الوطنية اللازمة لزيادة الجاهزية، وإجراء تخطيط الاستمرارية والاستجابة لمخاطر الأمن السيبراني الكبيرة عند ظهورها والاستجابة لها والتعافي منها (مثل الأزمات السيبرانية واسعة النطاق).
- حث المجتمع الدولي على تحسين أمن وموثوقية ومرونة الشبكات البينية بشكل عام (الشبكات المالية والاتصالات والطاقة إلخ) من خلال تطوير معايير عالمية للأمن وتشجيع الاتفاقيات متعددة الأطراف.
- توقع التطورات التقنية المستقبلية وتقييم إمكانية تسببها بتشكل نقاط ضعف جديدة للدولة، أو من جهة أخرى، إمكانية تحويلها لفرص لبناء مستوى إضافي من الأمن والموثوقية والمرونة في الجيل التالي من البنى التحتية والأصول.

التنفيذ الفعّال لهذه المهام وللأنشطة الأخيرة سيتطلب تحديد وتوضيح الأدوار والمسؤوليات وحقوق اتخاذ القرار وآليات المسائلة بشكل واضح. وستستفيد النتائج الناجحة من وضع أهداف للأداء للأفراد أو الدوائر أو المؤسسات الوزارية أو الحكومية المختلفة المسؤولة عن مهام مُحددة في خطة العمل.

بطبيعة الحال، تتطلب نشاطات خفض المخاطر أيضاً تخصيص الموارد المُخصصة والمناسبة لتنفيذها. فموارد وآليات التمويل غير الفعّالة قد تقوّض النتائج المرجوة وتخفض من مستوى مسائلة الجهات الموكلة بالأمن السيبراني للدولة والمزودة بموارد غير مناسبة لأداء مهامها. ينبغي تحديد الموارد من الناحية النقدية (أي ميزانية مُخصصة)، والناس، والمواد، بالإضافة إلى العلاقات والشراكات المطلوبة للتنفيذ الناجح لخطط خفض المخاطر ولنجاح نتائجها. وينبغي عدم النظر إلى توفير الموارد لأهداف ومهام استراتيجية الأمن السيبراني على أنها مبادرة لمرة واحدة فقط. فالتمويل الكافي والثابت والمستمر يشكل أساساً فعالاً لوضعية الدولة من ناحية الأمن السيبراني. بالإمكان تخصيص الموارد حسب المهمة أو الهدف، أو حسب الجهة الحكومية. ويمكن للحكومة أيضاً التفكير في إعداد موازنة مركزية للأمن السيبراني تديرها آلية مركزية لحوكمة الأمن السيبراني. سواء تم جمع موارد تمويل مختلفة وتم دمجها في برنامج موحد ومتكامل أو تم إنشاء موازنة موحدة داخل الحكومة، فينبغي أن تتم إدارة البرنامج العام وتتبعه من خلال علامات مرحلية وأطر زمنية مُحددة بشكل واضح لضمان التنفيذ الناجح للاستراتيجية.

التقييم المستمر للخطر

عند تحول جهود الأمن السيبراني لتقييم في نقطة زمنية مُحددة (إطار عمل الامتثال) – بدلاً من تقييم الخطر على نحو مستمر – فسيكون مآلها الفشل. تتطلب إدارة المخاطر التوقع الاستباقي للتهديدات والتقييم المستمر لنقاط الضعف في الجهات الأكثر حساسية في الدولة والمعتمدة على التقنية الرقمية (مثل الشركات والبنى التحتية والخدمات والأصول). كما ذكر أعلاه، هناك عدد من أطر العمل القائمة التي تُشدد على أهمية التقييم المستمر للمخاطر والمعالجة المستمرة لمواضع عجز الضبط. ينبغي أن تكون مراقبة وقياس الأداء والتنفيذ الناجح لمبادرات الأمن السيبراني (نشاطات خفض المخاطر) جزءاً من آليات الحوكمة التي تضعها الدولة ضمن بنيتها الوطنية للأمن السيبراني. التقييم المستمر لخطة التنفيذ (أي الأمور التي تجري بشكل جيد وتلك التي تجري بشكل سيء) يساعد على معرفة المواضع التي تحتاج للتعديلات وعلى حشد المزيد من التأييد للاستراتيجية الشاملة. تُحدد آليات الحوكمة الجيدة المسائلة والمسؤولية بشكل واضح لضمان التنفيذ الناجح وينبغي استخدام مقاييس قابلة للتنفيذ وقابلة للتكرار وهادفة ومعتمدة على الزمن أو المؤشرات الرئيسية للأداء (KPI) من أجل تعزيز الأهداف والجداول الزمنية الواقعية. وينبغي أن تتماشى المقاييس أو المؤشرات الرئيسية للأداء مع المعايير التالية:

- مُحددة – استهداف مجال مُحدد لتطويره.
- قابلة للقياس – تحديد الكمية أو على الأقل اقتراح مؤشر ما للتقدم.
- قابلة للتحقيق – ذكر النتائج التي يمكن تحقيقها بشكل واقعي، والموارد المتوفرة.

- قابلة للتنفيذ – وجود إجراءات واضحة يجب تنفيذها.
- مسؤولة – تحديد الجهة التي ستقوم بها.
- مرتبطة بالوقت – تحديد موعد تحقيق النتيجة/النتائج.

بالرغم من عدم تمتع ولا دولة بالجاهزية السيبرانية الكاملة وبالرغم من استحالة التخلص من المخاطر السيبرانية بشكل كامل إلا أنها قابلة للمعالجة وتنبغي معالجتها. تبدأ الجاهزية السيبرانية من خلال منهج فعّال لإدارة المخاطر يشمل فهماً واضحاً للأصول عالية القيمة في الدولة والأنظمة ذات التأثير العالي التي تتطلب مستويات عالية من الحماية - مواضع الاعتماد الرقمي الأكثر حساسية في الدولة (أي الشركات والخدمات والبنى التحتية والأصول). بعد فهم ذلك، يمكن لتحليل المخاطر وتقييم نقاط الضعف تحديد الإجراءات الأمنية وترتيبها وفقاً للأولويات من أجل تصحيح مواضع النقص المناسبة والمتناسبة مع الخطر الاقتصادي والمجتمعي.

لن يكون من الممكن خفض الخطر السيبراني بشكل كبير وضمان أمن وسلامة الدولة في المستقبل إلا من خلال جهد مشترك ومُنسّق بين أصحاب المصلحة الوطنيين.

الخاتمة

شعورنا بانعدام الأمن آخذ بالتنامي. فحجم ومستوى ونطاق التهديدات السيبرانية التي تُحدق بالخدمات والبنى التحتية الحسّاسة للدول يزداد بشكل متسارع يفوق الإجراءات الدفاعية. النشاطات السيبرانية المُدمرة والمُعطلة في يومنا هذا تستلزم معالجة الحكومات لها بشكل عاجل بالإضافة إلى استثمار الحكومات لنقل الدول من حالة انعدام الأمن السيبراني إلى حالة الجاهزية السيبرانية. الخسائر آخذة بالتراكم؛ والأذى آخذ بالتنامي؛ والخطر مُحدق.

ينبغي على قادة الدول وضع استراتيجيات شاملة للأمن الوطني السيبراني تشمل جهة مُختصة مسؤولة عن الوضعية العامة للدولة من ناحية الأمن السيبراني. وينبغي على الدول فهم المخاطر التي تواجهها على جميع المستويات – من قادة الحكومات إلى المواطنين العاديين. ينبغي على الجميع فهم نقاط ضعف البيئة الرقمية للدولة ومعرفة دورهم في تخفيف تلك المخاطر. خريطة الطريق الاستراتيجية هذه تسمح بتبني الإجراءات والسياسات والعمليات المناسبة لتصحيح مواضع العجز ولخفض المخاطر التي تُحدق بالمجتمع والاقتصاد والدولة. ولا يمكن تحقيق ذلك دون موارد مُخصصة ومناسبة لتمويل المبادرات التي تعمل على خفض المخاطر وزيادة المرونة. إن تبني استراتيجية وطنية للأمن السيبراني هي واحدة من أهم الخطوات لتأمين البنى التحتية والخدمات السيبرانية الوطنية التي يعتمد عليها المستقبل الرقمي والرفاه الاقتصادي للدولة الحديثة.

نبذة عن المؤلفة

ميليسا هاثاواي هي خبيرة بارزة في مجال سياسات الفضاء السيبراني والأمن السيبراني. وقد خدمت في فترة إدارتين رئاسيتين أمريكيتين حيث ترأست مراجعة سياسة الفضاء السيبراني للرئيس باراك أوباما وقادت المبادرة الشاملة للأمن السيبراني الوطني (CNCI) للرئيس جورج دبليو بوش. وبصفتها رئيسة شركة هاثاواي غلوبال ستراتيجيز ال ال سي، هي تقدم المشورة للعملاء من القطاعين العام والخاص من خلال خبرتها الفريدة من نوعها التي تجمع بين الخبرة السياسية والخبرة التقنية بالإضافة إلى خبرتها في مجالس الإدارة لمساعدة الآخرين على فهم التداخلات التي تربط بين السياسة الحكومية، وتطور الاتجاهات التقنية والصناعية والمُحركات الاقتصادية التي تؤثر على الاستحواذ وعلى استراتيجية تطوير الأعمال في هذا المجال. وقد قامت بتطوير منهجية فريدة من نوعها لتقييم وقياس مستوى الجاهزية لبعض مخاطر الأمن السيبراني وُتعرف هذه المنهجية باسم "مؤشر الجاهزية السيبرانية". وبالامكان الاطلاع على مؤشر الجاهزية السيبرانية 2.0 هنا:

http://www.potomacinstitute.org/academic-centers/cyber-readiness-index. ولها منشورات مُنتظمة حول مسائل الأمن السيبراني التي تؤثر على الشركات والدول. ويمكن الاطلاع على معظم مقالاتها على المواقع التالية: http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html و https://ctm.columbia.edu/people/melissa-hathaway