HM Government

الاستراتيجية الوطنية لأمن المعلوماتية
2021-2016

المحتويات

افتتاحية

المملكة المتحدة واحدة من الدول الرائدة في بمجال الاتصالات الرقمية. والكثير من ازدهارنا يعتمد على قدرانا على ضمان أمن تقنيتنا وبياناتنا وشبكاتنا في مواجهة الكثير من التهديدات التي أمامنا.

إلا أن وتيرة الهجمات الإلكترونية باتت متزايدة وأكثر تطورا وتتسبب بأضرار أكبر في حال نجاحها. وبالتالي نتخذ إجراءات حاسمة لحماية كل من اقتصادنا وخصوصية مواطنينا.

استراتيجيتنا الوطنية لأمن المعلوماتية تشرح خطتنا الرامية لجعل بريطانيا واثقة وقادرة وصامدة في عالم رقمي سريع التطور.

وعلى مدى هذه الاستراتيجية الممتدة خمس سنوات، سوف نستثمر 1.9 مليار جنيه استرليني في الدفاع عن أنظمتنا وبنيتنا التحتية، وردع المعادين لنا، وتطوير قدرات تشمل مجتمعنا ككل – من أكبر الشركات وحتى المواطنين الفرديين.

ونحن بحاجة لاستجابة أكثر شمولا، من أبسط إجراءات الوقاية من الهجمات الإلكترونية، وحتى توفير الرادع الأكثر تطورا.

وسوف نركز على رفع تكلفة شن اعتداء ضد أي أحد في المملكة المتحدة، وذلك من خلال توفير دفاعات أقوى وتطوير المهارات الإلكترونية على حد سواء. وذلك لم يعد مجرد مسؤولية إدارة المعلوماتية، بل كذلك مسؤولية كافة العاملين. حيث لا بد من أن يتمتع كل العاملين، في كافة المهن، بمهارات إلكترونية.

والمركز الوطني لأمن المعلوماتية الذي افتتحناه مؤخرا سيكون بمثابة مركز لتجربة عالمية المستوى ويسهل تطبيقها بالنسبة لكل من الشركات والأفراد، إلى جانب آلية للاستجابة سريعا لدى وقوع حوادث إلكترونية كبيرة.

تتولى الحكومة دورا قياديا واضحا، لكننا سوف نرعى كذلك بيئة تجارية أوسع، ونتعرف على المجالات التي يمكن أن يكون الابتكار بهذا القطاع فيها أسرع مما يمكننا نحن. ذلك يشمل التوجه إلى توظيف أفضل العقول الشابة في مجال أمن المعلوماتية.

إن التهديدات الإلكترونية تؤثر على مجتمعنا ككل، وبالتالي نريد أن نوضح بشكل جلي بأن كل فرد في مجتمعنا له دور في استجابتنا الوطنية. لهذا السبب تعتبر هذه الاستراتيجية تجربة في الشفافية لا سابق لها. حيث لم يعد بإمكاننا عقد هذا النقاش خلف أبواب مغلقة.

وفي نهاية المطاف، هذا تهديد لا يمكن القضاء عليه تماما. فالتقنية الرقمية ناجحة بسبب كونها منفتحة، وذلك الانفتاح يحمل في طياته المخاطر. لكن ما يمكننا عمله هو خفض التهديد إلى مستوى يكفل أن نظل في طليعة الثورة الرقمية. وهذه الاستراتيجية تشرح كيف يمكننا عمل ذلك.

فيليب هاموند، وزير الخزانة

تمهيد

مسؤوليتنا الأساسية هي الحفاظ على أمن بلدنا وأن تكون لدينا حكومة تتمتع بالكفاءة. وهذه الاستراتيجية تعكس هذه الواجبات. إنها مقاربة جريئة وطموحة للتصدي للكثير من التهديدات التي يواجهها بلدنا في مجال المعلوماتية. وإدارة وتخفيف هذه التهديدات هي مسؤولية تقع على عاتقنا جميعا، لكن الحكومة تدرك مسؤوليتها الخاصة بقيادة الجهود الوطنية اللازمة.

والحكومة ملتزمة بضمان تنفيذ الالتزامات المبينة في هذه الاستراتيجية، وأن نراقب بدقة ما نحرزه من تقدم في تنفيذها وإعداد تقارير منتظمة بشأنها. كما سنُبقي مقاربتنا هذه قيد المراجعة المستمرة ونستجيب للتغييرات في مستوى التهديد الذي نواجهه، وكذلك للتطورات في تقنيات الأمن.

وتضطلع الحكومة أيضا بمسؤولية خاصة تجاه المواطنين والشركات والمؤسسات العاملة في المملكة المتحدة، وتجاه حلفائنا وشركائنا الدوليين. وسيكون باستطاعتنا طمأنتهم بأننا بذلنا كل الجهود الممكنة كي تكون أنظمتنا الرقمية آمنة، ولحماية ما لدينا من بيانات وشبكات من أي هجوم أو تدخّل. وبالتالي من واجبنا أن نضع لأنفسنا أعلى معايير لأمن المعلوماتية، وضمان التزامنا بها كأساس للأمن القومي لبلدنا ولضمان سلامة اقتصادنا، وكذلك كنموذج يحتذيه الآخرون. وسوف نعد تقارير سنوية بشأن ما حققناه من تقدم.

إنني عازم، من واقع منصبي كوزير في شؤون مجلس الوزراء مسؤول عن أمن المعلوماتية وأمن الحكومة، على أن أرى تطبيق هذه الاستراتيجية بالكامل. سوف أعمل عن قرب مع الزملاء في أنحاء الحكومة البريطانية، والشركاء في الحكومات المفوضة في المملكة المتحدة، ومع القطاع العام على نطاق أوسع، ومع قطاع المعلوماتية والمؤسسات الأكاديمية لضمان تحقيق طموحنا هذا.

بِن غَمر، عضو البرلمان، وزير شؤون مجلس الوزراء وأمن المعلوماتية

1 الموجز التنفيذي

1-1 إن مستقبل أمن المملكة المتحدة ورفاهها يرتكزان على أسس رقمية. والتحدي الذي يواجه جيلنا هو بناء مجتمع رقمي مزدهر لديه القدرة على الصمود أمام التهديدات الإلكترونية ومزود بالمعرفة والقدرات المطلوبة من أجل الاستفادة من الفرص للحد الأقصى ولإدارة المخاطر.

2-1 أصبحنا متكلين على الإنترنت لدرجة كبيرة جدا. إلا أن ذلك يحمل الخطر في طياته، إذ ستكون هناك دائما محاولات لاستغلال نقاط الضعف من أجل شن هجمات إلكترونية. ولا يمكن التخلص من هذا التهديد بشكل كامل، غير أنه بالإمكان تقليل الخطر لحد بعيد وإلى مستوى يمكن فيه للمجتمع أن يستمر في الازدهار وأن يستفيد من الفرص الهائلة التي توفرها التكنولوجيا الرقمية.

3-1 الاستراتيجية الوطنية لأمن المعلوماتية لعام 2011، التي يدعمها برنامج الحكومة البريطانية الوطني لأمن المعلوماتية، والذي تبلغ تكلفته 860 مليون جنيه إسترليني، قد أدت إلى إدخال تحسينات كبيرة على أمن المعلوماتية في المملكة المتحدة. فقد حققت الاستراتيجية نتائج هامة من خلال تطلعها إلى السوق من أجل تشجيع سلوكيات آمنة في استخدام الإنترنت. إلا أن تلك المقاربة لم تحقق التغيير بالسرعة والمستوى اللازمين لكي تظل المملكة المتحدة متقدمة على التهديدات المتطورة بسرعة. وعلينا الآن أن نبذل جهودا لأبعد من ذلك.

4-1 تتلخص رؤيتنا لسنة 2021 في **أن تكون المملكة المتحدة في مأمن من التهديدات الإلكترونية ولديها القدرة على الصمود في وجهها، وأن تكون مزدهرة ومفعمة بالثقة في العالم الرقمي.**

5-1 لتحقيق تلك الرؤية، سنعمل لتحقيق الأهداف التالية:

- **الدفاع**: أن تكون لدينا الوسائل للدفاع عن المملكة المتحدة ضد التهديدات الإلكترونية الآخذة في التطور، والاستجابة بفعالية للحوادث، وضمان أن الشبكات والبيانات والأنظمة في المملكة المتحدة محمية وقادرة على الصمود. وأن تكون لدى المواطنين والشركات والقطاع العام المعرفة والقدرة للدفاع عن أنفسهم.
- **الردع**: أن تصبح المملكة المتحدة هدفا عسيرا لكل أشكال الاعتداء في الفضاء الإلكتروني، بحيث نكتشف أي عمل عدائي موجه ضدنا ونفهم طبيعته ونحقق به ثم نعرقله، كما نطارد المعتدين ونقدمهم للمحاكمة. كما ستكون لدينا سبل القيام بعمل هجومي في الفضاء الإلكتروني، في حال رغبنا بذلك.
- **التطوير**: أن يصبح لدينا قطاع أمن معلوماتية مبتكر ومتنامي، تسانده أعمال بحث وتطوير علمي رائدة عالميا. كما يتوفر لدينا مورد مستدام من المواهب يوفر المهارات اللازمة للاستجابة لاحتياجاتنا الوطنية في كافة جوانب القطاعين العام والخاص. وخبرتنا وقدرتنا على التحليل المتفوقة ستمكن المملكة من التصدي للتهديدات والتحديات المستقبلية والتغلب عليها.

6-1 لدعم تلك الأهداف، سوف نعكف على **العمل الدولي** ونمارس تأثيرنا من خلال الاستثمار في شراكات من شأنها أن تحدد معالم التطور العالمي للفضاء الإلكتروني بطريقة تعزز مصالحنا الاقتصادية والأمنية الأعم. وسوف نعمق روابطنا القائمة حاليا مع أقرب شركائنا الدوليين، لإدراكنا أن ذلك سوف يعزز أمننا المشترك. كما أننا سنبني علاقات مع شركاء جدد لنمكنهم من رفع مستويات أمن المعلوماتية لديهم، ولحماية مصالح المملكة المتحدة في الخارج. وسنقوم بذلك على المستويين الثنائي والدولي، بما في ذلك من خلال الاتحاد الأوروبي وحلف الناتو والأمم المتحدة. وسوف نبث رسائل واضحة فيما يخص العواقب التي يواجهها الأعداء الذين يهددون بإلحاق الضرر بمصالحنا، أو بمصالح حلفائنا، في الفضاء الإلكتروني.

7-1 لتحقيق تلك النتائج خلال السنوات الخمس القادمة، تعتزم حكومة المملكة المتحدة أن تتدخل بفاعلية أكبر وأن تستعين بمزيد من الاستثمارات، بينما تستمر بنفس الوقت في دعم قوى السوق كي ترفع من معايير أمن المعلوماتية في أرجاء المملكة المتحدة. وستعمل الحكومة البريطانية، بالشراكة مع الحكومات المفوضة في اسكتلندا وويلز وإيرلندا الشمالية، مع القطاعين الخاص والعام لضمان تبنّي الأفراد والشركات والمنظمات للسلوك اللازم للحفاظ على أمنهم على الإنترنت. وسوف نتخذ إجراءات للتدخل (عندما تستدعي الضرورة، وضمن نطاق صلاحياتنا) للدفع بتحسينات تصب في مصلحتنا القومية وخاصة فيما يتعلق بأمن المعلوماتية للبنية التحتية الوطنية الحيوية.

8-1 ستعتمد الحكومة البريطانية على قدراتها وعلى قدرات قطاع المعلوماتية من أجل تطوير وتطبيق إجراءات دفاع إلكتروني فعالة لكي تعزز إلى درجة كبيرة مستويات أمن المعلوماتية في كافة شبكات المملكة المتحدة. وتتضمن تلك الإجراءات تقليل أكثر أنواع هجمات التصيد الإلكتروني شيوعا إلى الحد الأدنى، وفلترة عناوين الإنترنت الضارة المعروفة، وحجب أنشطة الإنترنت الخبيثة بشكل فعال. ومن شأن التحسينات في أمن المعلوماتية الأساسي أن ترفع من قدرة المملكة المتحدة على الصمود في وجه التهديدات الإلكترونية الأكثر انتشارا.

9-1 أسسنا المركز الوطني لأمن المعلوماتية ليكون الجهة المرجعية لأمور بيئة أمن المعلوماتية في المملكة المتحدة، حيث يضطلع بمهام تقاسم المعلومات، ومعالجة نقاط الضعف المنهجية، وتولّي الدور القيادي بالنسبة للمسائل الأساسية المتعلقة بأمن المعلوماتية الوطني.

10-1 سوف نضمن أن قواتنا المسلحة قادرة على الصمود ولديها الدفاعات الإلكترونية القوية التي تحتاجها لحماية شبكاتها ومنصاتها والدفاع عنها، وأن تستمر في عملها وفي المحافظة على حريتها على مستوى العالم للمناورة رغم التهديدات الإلكترونية. وسيعمل مركز عمليات أمن المعلوماتية العسكري لدينا بشكل وثيق مع المركز الوطني لأمن المعلوماتية، وسوف نضمن أن يكون باستطاعة القوات المسلحة أن تساعد في حال وقوع هجوم إلكتروني كبير على مستوى البلاد.

11-1 ستتوفر لدينا السبل للاستجابة للهجمات الإلكترونية بنفس الطريقة التي نستجيب بها لأي هجوم من نوع آخر، باستخدام القدرة الأكثر ملاءمة، بما في ذلك قدرة الهجوم الإلكتروني.

12-1 سوف نستخدم سلطة حكومة المملكة المتحدة ونفوذها للاستثمار في برامج لمعالجة النقص في مهارات أمن المعلوماتية في المملكة المتحدة، من المدارس إلى الجامعات وعلى كافة مستويات قوى العمل.

13-1 سوف نطلق مركزين جديدين للابتكار الإلكتروني للدفع نحو تطوير أحدث المنتجات الإلكترونية وشركات حيوية جديدة في مجال أمن المعلوماتية. كما سنخصص جزءا من صندوق الدفاع والابتكار الإلكتروني البالغ 165 مليون جنيه إسترليني لدعم المشتريات المبتكرة في مجالي الدفاع والأمن.

14-1 سوف نستثمر ما يصل إلى 1.9 مليار جنيه استرليني خلال السنوات الخمس التالية لإحداث نقلة كبيرة بمجال أمن المعلوماتية في المملكة المتحدة.

2 مقدمة

1-2 لقد تطورت تقنيات المعلومات والاتصالات خلال العقدين الماضيين، وهي تدخل اليوم فعليا ضمن كافة أوجه حياتنا. وقد أصبحت المملكة المتحدة مجتمعا رقميا. وبفضل ذلك أصبح اقتصادنا وحياتنا اليومية أكثر ازدهارا.

2-2 التحول الناجم عن شيوع التقنيات الرقمية يؤدي إلى حالات جديدة من الاتكالية. فاقتصادنا وإدارة الحكومة وتوفير الخدمات الرئيسية تعتمد الآن على سلامة الفضاء الإلكتروني، وعلى البنية التحتية والنظم والبيانات التي تدعمه. وفقدان الثقة بسلامة الفضاء الإلكتروني سوف يفسد فوائد تلك الثورة التكنولوجية.

3-2 الكثير من الأجهزة والبرامج التي تم تطويرها أصلا لتسهيل هذه البيئة الرقمية المترابطة فيما بينها قد أعطت الأسبقية للكفاءة وقلة التكلفة وراحة المستخدم، إلا أن الأمن لم يكن دائما داخلا في تصميمها منذ البداية. ويمكن لأصحاب النوايا الخبيثة – من دول معادية ومنظمات إجرامية أو إرهابية وأفراد – استغلال الفجوة القائمة بين راحة المستخدم والأمن. لذا، فإن تضييق تلك الفجوة أولوية وطنية.

4-2 انتشار الإنترنت لأبعد من الكمبيوترات والهواتف المحمولة ليشمل أنظمة أخرى إلكترونية متكاملة أو "ذكية" يوسع مخاطر الاستغلال عن بعد ليشمل مجموعة كاملة من التقنيات الحديثة. إن الأنظمة والتقنيات التي تقوم عليها حياتنا اليومية - كمحطات الكهرباء، وأنظمة المراقبة الجوية في المطارات، والأقمار الصناعية، والتقنيات الطبية، والمصانع، وإشارات المرور - متصلة بالإنترنت، وبالتالي فهي معرضة لاحتمال التدخل الخارجي.

5-2 أكدت استراتيجية الأمن القومي لعام 2015 ان التهديد الإلكتروني يشكل خطرا من الدرجة الأولى على مصالح المملكة المتحدة. وتشير الاستراتيجية إلى تصميم الحكومة على معالجة التهديدات الإلكترونية "وأن تضع إجراءات صارمة ومبتكرة باعتبارها رائدة عالميا في مجال أمن المعلوماتية". وستفي هذه الاستراتيجية الوطنية لأمن المعلوماتية بهذا الالتزام.

6-2 بإعدادها لهذه الاستراتيجية الجديدة، فإن الحكومة تُؤسس على إنجازات وغايات وتقديرات الاستراتيجية الوطنية الخمسية الأولى لأمن المعلوماتية التي صدرت 2011. وقد استثمرت الحكومة 860 مليون جنيه إسترليني خلال تلك الفترة، وهي فخورة بما تم إنجازه. فالسياسات والمؤسسات والمبادرات التي تم تطويرها خلال السنوات الخمس الماضية قد أسهمت في إرساء مكانة المملكة المتحدة كلاعب عالمي رائد في مجال أمن المعلوماتية.

7-2 هذه أساسات صلبة، لكن مثابرة أولئك الذين يشكلون تهديدا لنا وطرقهم المبتكرة، ووجود نقاط ضعف وفجوات في قدراتنا ودفاعاتنا، يعني أن علينا بذل جهود أكبر لكي نواكب الخطر. ويتطلب الأمر مقاربة شاملة إن أردنا أن نحمي مصالحنا الإلكترونية بشكل فعال. إن تصميمنا على المضي قدما في استثمارات ومداخلات جديدة يرتكز على المعطيات التالية:

- مستوى التهديدات وطبيعتها الحيوية، بالإضافة إلى نقاط ضعفنا واعتمادنا على الأنظمة الإلكترونية، يعني أن الاستمرار في اتباع المقاربة الحالية لن يكون بحد ذاته كافيا لحمايتنا؛
- المقاربة القائمة على معطيات السوق بشأن الترويج لاتخاذ تدابير وقائية إلكترونية لم ينتج عنها الوتيرة والمستوى المطلوبين للتغيير، لذلك فإن على الحكومة أن تضطلع بالقيادة وأن تتدخل بشكل مباشر أكثر بأن تسخر نفوذها ومواردها من أجل مواجهة التهديدات الإلكترونية؛
- لا تستطيع الحكومة بمفردها أن تتحمل أعباء كافة أوجه أمن المعلوماتية في البلد. فهناك حاجة إلى مقاربة راسخة ومستدامة يكون فيها المواطنون والقطاعات والشركاء الآخرون في المجتمع والحكومة يؤدون دورهم كاملا في حماية شبكاتنا وخدماتنا وبياناتنا؛
- المملكة المتحدة بحاجة إلى قطاع أمن معلوماتية حيوي، وإلى قاعدة من المهارات المساندة التي يمكنها أن تواكب التهديدات المتغيرة بل وأن تكون متقدمة عليها.

نطاق الاستراتيجية

8-2 الغرض من هذه الاستراتيجية هو صياغة سياسة الحكومة، وبنفس الوقت لتوفير رؤية متماسكة ومقنعة يتم تشاطرها مع القطاعين الخاص والعام والمجتمع المدني والجامعات وعامة المواطنين.

9-2 تغطي الاستراتيجية المملكة المتحدة بكاملها. وسوف تسعى الحكومة البريطانية لضمان تنفيذ الاستراتيجية في كافة أرجاء البلاد، مع الأخذ بعين الاعتبار أننا سنعمل بشكل وثيق على تطبيقها مع الحكومات المفوضة في اسكتلندا وويلز وايرلندا الشمالية بقدر ما تمس الاستراتيجية مسائل تقع تحت مسؤولية هذه الحكومات (مع احترام الأنظمة القانونية المنفصلة الثلاثة والأنظمة التعليمية الأربعة في المملكة المتحدة). وحيث تكون المقترحات المطروحة في الاستراتيجية ذات صلة بمسائل تقع تحت مسؤولية الحكومات المفوضة، فإن تطبيق تلك المقترحات يكون بالاتفاق مع تلك الحكومات بالشكل الملائم، ووفقا للتسويات المتعلقة بالتفويض.

10-2 تحدد الاستراتيجية إجراءات مقترحة أو موصى بها موجهة إلى كافة قطاعات الاقتصاد والمجتمع، من مؤسسات الحكومة المركزية إلى قيادات القطاعات المختلفة وحتى المواطن الفرد. وتهدف الاستراتيجية إلى زيادة أمن المعلوماتية على كافة المستويات لمصلحتنا الجماعية، وستكون حجر الأساس لما تقوم به المملكة المتحدة دوليا لنشر الحوكمة الرشيدة للإنترنت.

11-2 تشير عبارة "أمن المعلوماتية " في هذه الاستراتيجية إلى حماية نظم المعلومات (من أجهزة وبرامج وبنية تحتية مصاحبة)، والبيانات المختزنة فيها، والخدمات التي توفرها بحيث لا يصل إليها من ليس مرخصا له ذلك، وأيضا حمايتها من الأذى أو إساءة الاستخدام. ويشمل ذلك الضرر المتعمد من جانب من يشغل النظام، أو الأذى العَرَضي الناجم عن عدم اتباع إجراءات الأمن.

12-2 انسجاما مع تقديراتنا للتحدي الذي نواجهه، وتأسيسا على منجزات استراتيجية عام 2011، فإن هذه الاستراتيجية الجديدة تعرض ما يلي:

- تقييمنا المُحدّث للسياق الاستراتيجي، بما في ذلك التهديدات الحالية والمتغيرة باستمرار: أولئك الذين يمثلون أخطر تهديد لمصالحنا، والأدوات التي تحت تصرفهم؛
- مراجعة لنقاط الضعف وتطورها خلال السنوات الخمس الماضية؛
- رؤية الحكومة لأمن المعلوماتية في عام 2021، والأهداف الرئيسية لتحقيق تلك الغاية، ويشمل ذلك المبادئ الإرشادية والأدوار والمسؤوليات، وكيف وأين يمكن لتدخل الحكومة أن يكون مفيدا؛
- كيف نعتزم تطبيق سياستنا: تحديد المجالات التي ستلعب فيها الحكومة دورا قياديا، وتلك التي نتوقع أن نعمل بشأنها بالشراكة مع آخرين؛
- كيف نعتزم تقييم تقدمنا نحو تحقيق أهدافنا.

3 السياق الاستراتيجي

1-3 عندما نُشرت الاستراتيجية الوطنية السابقة لأمن المعلوماتية في 2011، كان مستوى التغير التكنولوجي وتأثيره باديا بالفعل. والتوجهات والفرص التي أشير إليها وقتها قد تسارعت منذ ذلك الحين. وقد برزت تقنيات وتطبيقات جديدة، كما إن الإقبال على التقنيات القائمة على الإنترنت في كافة أرجاء العالم، وخاصة في الدول النامية، قد وفر المزيد من الفرص للتنمية الاقتصادية والاجتماعية. وهذه التطورات جلبت، أو أنها ستجلب، فوائد جمة للمجتمعات التي تستخدم الإنترنت كما هي حالنا. ولكن مع تزايد اعتمادنا على الشبكات الإلكترونية في المملكة المتحدة وفي الخارج، تزداد أيضا الفرص لأولئك الذين يسعون لإلحاق الضرر بأنظمتنا وبياناتنا. وبنفس القدر، تغير كذلك المشهد الجيوسياسي. فالأنشطة الإلكترونية الخبيثة لا تعترف بالحدود الدولية. والأطراف التي تمثل الدول عاكفة على تجريب قدرات إلكترونية هجومية. ومجرمو الإنترنت باتوا يوسعون نطاق جهودهم وأساليب عملهم الاستراتيجية لتحقيق مردود مادي أعلى من المواطنين والمنظمات والمؤسسات في المملكة المتحدة. أما الإرهابيون ومناصروهم فينفذون هجمات منخفضة المستوى، ويطمحون إلى القيام بعمليات أكبر. وهذا الفصل يعرض تقييمنا لطبيعة تلك التهديدات، ونقاط ضعفنا، وكيف أنها لا تزال تتطور.

التهديدات

مجرمو الإنترنت

2-3 تتناول هذه الاستراتيجية جرائم الإنترنت في سياق نوعين متداخلين من النشاط الإجرامي:

- الجرائم المعتمدة على الإنترنت - وهي الجرائم التي يمكن ارتكابها فقط من خلال استعمال أجهزة تكنولوجيا المعلومات والاتصالات، حين تكون الأجهزة هي أداة ارتكاب الجريمة وهي المستهدفة من الجريمة في آن معا (مثلا لتطوير وترويج برامج ضارة من أجل الكسب المالي، أو القرصنة بقصد سرقة البيانات و/أو الشبكات أو اتلافها أو تحريفها أو تدميرها، و/أو تدمير الشبكة أو عملها).
- الجرائم التي تتم بواسطة الإنترنت - وهي الجرائم التقليدية التي يمكن أن تزداد في نطاقها أو مداها باستخدام الكمبيوتر أو شبكات الكمبيوتر أو أشكال أخرى من تكنولوجيا المعلومات والاتصالات (كالاحتيال بالاستعانة بالإنترنت وسرقة البيانات).

3-3 الكثير من الجرائم الإلكترونية الأكثر خطورة - كالاحتيال والسرقة والابتزاز بشكل أساسي - المرتكبة ضد المملكة المتحدة مازالت ترتكبها على الغالب جماعات الجريمة المنظمة الناطقة باللغة الروسية والمدفوعة بالكسب المالي في أوروبا الشرقية، حيث أن تلك الدول تستضيف الكثير من خدمات سوق جرائم الإنترنت. إلا أن التهديد يأتي أيضا من دول ومناطق أخرى، ومن داخل المملكة المتحدة نفسها، فضلا عن التهديدات الناشئة من جنوب آسيا وغرب أفريقيا التي تسبب قلقا متزايدا.

4-3 حتى عندما يتم التعرف على الأشخاص الرئيسيين المسؤولين عن القيام بأنشطة إلكترونية إجرامية والذين تسببوا بأكبر الضرر للمملكة المتحدة، فغالبا ما يكون من الصعب على أجهزة تطبيق القانون البريطانية والدولية أن تحاكم هؤلاء حين يتواجدون في بلدان تكون فيها إجراءات تسليم المطلوبين إما محدودة أو غير موجودة أصلا.

5-3 إن جماعات الجريمة المنظمة تلك مسؤولة بصورة أساسية عن تطوير ونشر برامج ضارة أصبحت متقدمة بشكل متزايد، والتي تصيب كمبيوترات وشبكات المواطنين والقطاعات والحكومة في المملكة المتحدة. والاضرار الناجمة موزعة على مختلف مناطق المملكة المتحدة، ولكن أثرها التراكمي ضخم. وقد أصبحت تلك الهجمات شرسة وتعتمد المواجهة بشكل متزايد، كما يوضحه الاستخدام المتزايد لبرامج طلب الفدية (ransomware) والتهديدات باعتداء الحرمان من الخدمة المُوزَع (DDoS) لأغراض الابتزاز.

6-3 وفي حين أن جماعات الجريمة المنظمة قد تشكل تهديدا كبيرا لازدهارنا ولأمننا الجماعي، فإنه من المقلق بنفس الدرجة استمرار التهديدات من جرائم إلكترونية أقل تعقيدا ولكنها واسعة الانتشار تُرتكب بحق الأفراد أو المؤسسات الأصغر.

حالات الاحتيال المصرفي عبر الإنترنت، التي تشمل مدفوعات أعمل النصب المسحوبة من الحساب المصرفي للعميل باستخدام قنوات الإنترنت المصرفية، قد زادت بنسبة 64% لتصل إلى 133.5 مليون جنيه إسترليني في 2015. وقد ازداد عدد الحالات بنسبة أقل بلغت 23%، والذي قال عنه مركز مكافحة الاحتيال المالي في المملكة المتحدة أنه دليل على الاتجاه المتنامي لدى المجرمين لاستهداف الشركات والعملاء الأثرياء.

التهديدات من جانب دول وأطراف ترعاها دول

7-3 نتعرض بشكل منتظم لمحاولات تقوم بها دول وجماعات ترعاها دول لاختراق شبكات المملكة المتحدة من أجل مكاسب سياسية وديبلوماسية وتكنولوجية وتجارية واستراتيجية، مع تركيز أساسي على القطاعات الحكومية والدفاعية والمالية والطاقة والاتصالات اللاسلكية.

8-3 تتفاوت قدرة وتأثير هذه البرامج الإلكترونية للدول. وتستمر الدول الأكثر تقدما في تحسين قدراتها بسرعة، بحيث تدمج خدمات التشفير وإخفاء هوية مستخدمي البيانات في أدواتها لكي تبقى مستترة. وفي حين أن لديها القدرة الفنية لشن هجمات معقدة، يمكنها غالبا أن تحقق أغراضها باستخدام أدوات وتقنيات بسيطة ضد أهداف ضعيفة لأن دفاعات ضحاياها ضعيفة.

9-3 ليس هناك سوى عدد ضئيل من الدول التي لديها القدرات الفنية لكي تشكل تهديدا حقيقيا لأمن المملكة المتحدة وازدهارها بشكل عام. ولكن دولا كثيرة أخرى ماضية في تطوير برامج إلكترونية معقدة يمكنها أن تشكل تهديدا لمصالح المملكة المتحدة في المستقبل القريب. وبإمكان دول عديدة ممن تسعى لتطوير قدرات التجسس الإلكتروني أن تشتري أدوات لاستغلال شبكات الكمبيوتر "متوفرة في السوق" وأن تعيد توجيه عمل تلك الأدوات بحيث تستخدمها لأغراض التجسس.

10-3 فيما هو أبعد من خطر التجسس، لجأ عدد من الأجانب المعادين العاملين في هذا المجال إلى تطوير واستخدام قدرات إلكترونية هجومية، ومنها ما هو مُدمِر. تلك القدرات تهدد أمن البنية التحتية الوطنية الحيوية وكذلك أنظمة التحكم الصناعية في المملكة المتحدة. وقد تستخدم بعض الدول تلك القدرات بما يخالف القانون الدولي لاعتقادها أنه بإمكانها أن تفعل ذلك بحصانة نسبية، ما يشجع الآخرين أن يحذوا حذوها. وفي حين أن الهجمات المدمرة في أنحاء العالم لا تزال نادرة، إلا أن أعدادها وأضرارها في ازدياد.

الإرهابيون

11-3 لا تزال الجماعات الإرهابية تطمح لتنفيذ عمليات إلكترونية مدمرة ضد المملكة المتحدة ومصالحها. القدرات الفنية للإرهابيين تعتبر منخفضة حاليا. لكن رغم ذلك، فحتى الأعمال ذات القدرة الفنية المنخفضة التي تمت لتاريخه ضد المملكة كان ضررها أكبر من المتوقع: فعمليات بسيطة كتشويه موقع إلكتروني واستقاء معلومات شخصية (doxing - حيث المعلومات الشخصية التي تعرضت للقرصنة "تُسرَّب" على الإنترنت) تُمكّن الجماعات الإرهابية ومن يدعمها من جذب اهتمام الإعلام وترهيب ضحاياها.

"إن استخدام الإرهابيين للإنترنت لخدمة أغراضهم لا يوازي الإرهاب الإلكتروني. ولكن بانخراطهم أكثر فأكثر في الفضاء الإلكتروني، ونظرا لتوفر الجريمة الإلكترونية كخدمة، فيمكن الافتراض بأنه سيكون بمقدور الإرهابيين أن يشنوا اعتداءات إلكترونية".

تقرير الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA) عن حالة التهديدات لعام 2015

12-3 التقييم الحالي هو أن الهجمات الإرهابية المادية، لا الإلكترونية، سوف تظل الأولوية بالنسبة للمجموعات الإرهابية في المستقبل المنظور. ومع انخراط جيل مُلمّ بشكل متزايد بأمور الكمبيوتر في أعمال التطرف، ومع إمكانية تبادل المهارات الفنية المتقدمة، فإننا نتوقع قدرا أكبر من العمليات التخريبية منخفضة التعقيد (مثل تشويه المواقع الإلكترونية أو اعتداءات الحرمان من الخدمة الموزّع) ضد المملكة. وسيزداد احتمال بروز عدد المهاجمين المنفردين من المتطرفين الماهرين، وكذلك سيزداد خطر أن تسعى منظمة إرهابية لأن تجند شخصا متمرسا من الداخل. ومن المرجح أن يستخدم الإرهابيون أية قدرات إلكترونية لتحقيق أكبر تأثير ممكن. وبذلك، فحتى زيادة بسيطة في قدرات الإرهابيين قد تشكل تهديدا كبيرا للمملكة ومصالحها.

قراصنة الإنترنت

13-3 جماعات القراصنة منظمة بطريقة لا مركزية، وتوجهاتها قائمة على قضايا معينة. فهي تتشكل وتختار أهدافها كردة فعل على ما ترى أنه مظالم حاقت بها. وهي تضفي على العديد من أعمالها طابع أخذ العدالة بيدها. وبينما أن معظم أنشطة القراصنة تخريبية بطبيعتها (تشويه المواقع الإلكترونية واعتداءات الحرمان من الخدمة الموزّع) إلا أن القراصنة الأكثر تمكنا قد استطاعوا أن يُلحقوا أضرارا أكبر وطويلة الأمد بضحاياهم.

التهديد من الداخل

تظل التهديدات التي مصدرها شخص من الداخل (insider) تشكل خطرا إلكترونيا على المؤسسات في المملكة المتحدة. فالمتآمرون من الداخل، الذين هم موظفون موثوقون في المؤسسة ومخولون لاستخدام الأنظمة والبيانات، يشكلون التهديد الأكبر. فبإمكانهم إلحاق الضرر بالوضع المالي للمؤسسة وسمعتها عن طريق سرقة البيانات الحساسة والممتلكات الفكرية. كما يمكنهم أن يشكلوا تهديدا إلكترونيا مدمرا إن استخدموا المعرفة المتاحة لهم بحكم مناصبهم، أو صلاحيتهم للدخول على الأنظمة الإلكترونية، لتسهيل أو شن هجوم بقصد التخريب أو إلحاق الضرر بخدمات حساسة على شبكة المؤسسات التي يعملون بها، أو لمحو بيانات من الشبكة.

وما يشكل مصدر قلق مماثل هم أولئك الأشخاص من الداخل أو الموظفون الذين يتسببون عرضيا بالضرر حين يفتحون عن غير قصد رسالة إلكترونية تتضمن رابطا للتصيّد (phishing)، أو يُدخلون قرص تخزين ملوث على الكمبيوتر، أو حين يتجاهلون إجراءات أمن المعلوماتية ويُنزلون مواد غير آمنة من الإنترنت. وفي حين أنه ليس في نيتهم أن يتعمدوا الإضرار بالمؤسسة، إلا أن قدرتهم على الوصول إلى الأنظمة والبيانات تعني أن تصرفاتهم يمكنها أن تسبب الضرر تماما بقدر ما يسببه شخص داخلي سيئ النية. وغالبا ما يكون هؤلاء الأفراد ضحايا لما يُعرف بالهندسة الاجتماعية (social engineering) - وبإمكانهم، عن دون قصد، أن يوفروا للآخرين إمكانية الوصول إلى شبكات مؤسساتهم، أو أن ينُفذوا، بحسن نية، تعليمات تفيد المحتالين.

إن مجمل الخطر الإلكتروني على مؤسسة ما من التهديدات الداخلية لا يقتصر على الوصول غير المصرح به لأنظمة المعلومات ومحتوياتها. فضوابط الأمن المادي التي تحمي الأجهزة من أن يصل إليها الشخص الخطأ، ونقل بيانات حساسة أو معلومات سرية للمؤسسة على أشكال مختلفة من الوسائط، هي أيضا بنفس الأهمية. وبالمثل فإن وجود ثقافة راسخة بشأن أمن العاملين تكون واعية للتهديدات التي يشكلها العاملون الساخطون، وللاحتيال في قوة العمل والتجسس الصناعي وغير ذلك من التهديدات، يعتبر عنصرا هاما في المقاربة الشاملة بشأن الأمن.

"صبيان النص الجاهز" (Script Kiddies)

14-3 **إن** من يُطلق عليهم "صبيان النص الجاهز" - وهم عادة ذوو مهارات محدودة ويستخدمون برامج طورها آخرون لشن هجمات إلكترونية - لا يُعتبرون مصدر تهديد كبير للاقتصاد والمجتمع على النطاق الأوسع. إلا أنهم تتوفر لديهم إرشادات وموارد وأدوات قرصنة على الإنترنت. ونظرا لنقاط الضعف الموجودة في أنظمة تطبيقات الإنترنت التي تستخدمها مؤسسات عديدة، فإن ما يقوم به هؤلاء المهاجمون يمكنه في بعض الحالات أن يحدث ضررا أكبر من المتوقع على المؤسسة المعنية.

دراسة حالة 1: الهجوم على شركة TalkTalk للاتصالات

بتاريخ 21 أكتوبر 2015، أعلنت شركة الاتصالات البريطانية TalkTalk أنها تعرضت لهجوم إلكتروني ناجح وأنه أدى لكشف بيانات العملاء. وقد أشارت التحقيقات اللاحقة إلى أن المهاجمين قد تمكنوا من الوصول إلى قاعدة بيانات تحتوي تفاصيل عن العملاء عن طريق خوادم إنترنت عامة، ما جعل سجلات حوالي 157,000 عميل في خطر، وهي تشمل الأسماء والعناوين وتفاصيل الحسابات المصرفية.

وفي نفس اليوم، تلقى العديد من العاملين في هذه الشركة رسالة إلكترونية تطالب بدفع فدية بعملة بيتكوين Bitcoin. وقد سرد المهاجمون تفاصيل هيكل قاعدة البيانات كبرهان ملموس على أنهم قد اطلعوا عليها.

تقرير هذه الشركة بشأن انكشاف البيانات أفاد الشرطة، بدعم من خبراء من الوكالة الوطنية لمكافحة الجريمة، في القبض على المشتبه بهم الرئيسيين، وجميعهم داخل المملكة المتحدة، وذلك في أكتوبر ونوفمبر 2015.

يُظهر هذا الهجوم أن نقاط الضعف يمكن أن تبقى موجودة، حتى في الشركات الكبرى التي لها دراية وافية بالأمور الإلكترونية. ويمكن لاستغلال تلك النقاط أن يُحدث تأثيرا أكبر من المتوقع من حيث الضرر الذي سيلحق بسمعة المؤسسة وتعطيل عملياتها. وقد لاقت تلك الحادثة اهتماما واسعا من جانب الإعلام. وبفضل سرعة شركة TalkTalk في الإبلاغ عن انكشاف البيانات، تمكنت الجهات الأمنية من أن تستجيب دون تأخير، وأتاح ذلك للحكومة وعامة الناس تخفيف وقع الخسارة المحتملة لبيانات حساسة. تلك الحادثة كلفت الشركة ما يقدر بنحو 60 مليون جنيه إسترليني وخسارة 95,000 عميل، بالإضافة إلى هبوط حاد في سعر أسهم الشركة.

دراسة حالة 2: الاعتداء على نظام سويفت في بنك بنغلادش

جمعية الاتصالات اللاسلكية المالية للتعاملات بين البنوك بأنحاء العالم، وتعرف اختصارا باسم "سويفت"، توفر شبكة تُمكن المؤسسات المالية من أنحاء العالم من أن ترسل وتستقبل معلومات عن التعاملات المالية بطريقة آمنة. وحيث أن نظام سويفت يرسل أوامر الدفع التي يجب أن تسدد من حسابات مقابلة موجودة فيما بين المصارف، يسود قلق منذ زمن طويل حول احتمال أن تتعرض تلك العملية للضرر من جانب مجرمي الإنترنت أو أية أطراف خبيثة أخرى الذين يسعون لضخّ أوامر دفع غير مشروعة في ذلك النظام أو، في أسوأ الأحوال، يسعون لتخريب سير عمل شبكة سويفت نفسها.

وفي أوائل فبراير 2017، تمكن مهاجم من الدخول إلى شبكة سويفت في بنك بنغلادش وأصدر تعليمات للبنك المركزي في نيويورك بأن يحول أموالا من حساب بنك بنغلادش إلى حسابات في الفلبين. وكانت قيمة محاولة الاحتيال تلك 951 مليون دولار أمريكي. وقد استطاع النظام المصرفي تعطيل 30 عملية تحويل تبلغ قيمتها 850 مليون دولار أمريكي، إلا أنه مرت خمس تحويلات بقيمة 101 مليون دولار أمريكي. وجرى لاحقا استرداد مبلغ 20 مليون دولار كان قد تم تعقبه إلى سريلانكا. أما مبلغ 81 مليون دولار المتبقي والذي تم تحويله إلى الفلبين فقد جرى غسله من خلال الكازينوهات، بينما أُرسلت بعض المبالغ بعد ذلك إلى هونغ كونغ.

وقد كشف التحقيق الجنائي الذي أجراه بنك بنغلادش أنه جرى زرع برامج خبيثة في أنظمة البنك، ومن ثم استخدامها لجمع المعلومات عن الإجراءات التي يتبعها البنك في المدفوعات وتحويلات الأموال الدولية. كما كشف تحليل أجرته شركة BAE Systems على البرنامج الخبيث ذي الصلة بالهجوم عن وجود خاصية معقدة من أجل التفاعل مع البرنامج المحلي لتبادل الرسائل مع نظام سويفت (SWIFT Alliance Access) الذي يدخل في البنية التحتية الإلكترونية لبنك بنغلادش. والنتيجة التي خلصت إليها هذه الشركة هي "أن المجرمين أصبحوا يشنون المزيد من الهجمات المعقدة ضد المؤسسات التي يستهدفونها، وخاصة في مجال اختراق الشبكات".

دراسة حالة 3: الاعتداء على شبكة الكهرباء في أوكرانيا

الاعتداء الإلكتروني على شركتي توزيع الكهرباء في غرب أوكرانيا، بريكارباتيا أوبلنيرغو وكييف اوبلنيرغو يوم 23 ديسمبر 2015 أدى إلى انقطاع كبير في الكهرباء بتعطّل ما يزيد عن 50 محطة فرعية من شبكات التوزيع. وأفادت التقارير أن المنطقة شهدت انقطاعا في الكهرباء لعدة ساعات، وأن الكثير من العملاء والمناطق الأخرى تعرضوا لانقطاع الكهرباء بدرجة أقل، وقد تأثر من جراء ذلك ما يزيد عن 220,000 مستهلك.

رأى البعض أن استخدام البرنامج الإلكتروني الضار بلاك إنيرجي 3 هو الذي تسبب في وقوع الاعتداء بعد كشف عينات على الشبكة. وقبل الهجوم بستة أشهر على الأقل، أرسل المعتدون رسائل تصيّد إلكترونية إلى مكاتب شركات الكهرباء في أوكرانيا تحتوي على وثائق مايكروسوفت أوفيس ضارة. إلا أن تلك البرامج لم تكن على الأرجح هي المسؤولة عن فتح قواطع الدوائر الكهربائية الذي أدى إلى انقطاع الكهرباء. بل من المحتمل أن البرنامج الخبيث مكّن المهاجمين من جمع معلومات سرية أتاحت لهم أن يتحكموا عن بعد بوظائف الشبكة، الأمر الذي جعلهم يتمكنون لاحقا من التسبب بانقطاع الكهرباء.

وهذه الحادثة في أوكرانيا هي أول مثال مؤكد على هجوم تخريبي إلكتروني استهدف شبكة كهرباء. ويظهر هذا المثال مجددا الحاجة إلى إجراءات أمن معلوماتية جيدة تشمل كافة أوجه بنيتنا التحتية الوطنية الحيوية لمنع وقوع أية حوادث مشابهة في المملكة المتحدة.

نقاط الضعف

توسع نطاق الأجهزة

15-3 عندما نُشرت الاستراتيجية الوطنية السابقة لأمن المعلوماتية في 2011، كان ما يعرفه معظم الناس عن أمن المعلوماتية هو من منظور حماية أجهزتهم كالكمبيوتر المكتبي أو المحمول. ومنذ ذلك الوقت أصبحت الإنترنت متداخلة في حياتنا اليومية بشكل متزايد وبطرق عديدة نحن غافلون عنها لحد بعيد. إن مفهوم "إنترنت الاشياء" (Internet of Things) يخلق فرصا جديدة للاستغلال ويزيد من التأثير المحتمل للهجمات التي يمكنها أن تحدث أضرارا مادية وإصابات للأشخاص وقد تؤدي، في أسوأ الأحوال، إلى الموت.

16-3 الانتشار السريع لتطبيقات الإنترنت في عمليات التحكم الصناعية في الأنظمة الحيوية، وعلى نطاق واسع من القطاعات كالطاقة والتعدين والزراعة والطيران، قد خلق مفهوم إنترنت الاشياء الصناعي. وبذات الوقت، ذلك يفسح المجال لإمكانية أن تتعرض الأجهزة ومراحل العمل الصناعي للقرصنة والعبث بها وبنتائج قد تكون كارثية، علما أنها لم تكن يوما عرضة للتدخل الخارجي في السابق.

17-3 لذلك، فنحن لم نعد معرضين فقط للأذى الإلكتروني الذي يسببه غياب أمن المعلوماتية في أجهزتنا، بل إننا معرضون أيضا للتهديدات لأنظمتنا المتصلة ببعضها والتي هي جوهرية لمجتمعنا وصحتنا ورفاهنا.

ضعف الإجراءات الوقائية الإلكترونية والامتثال

18-3 لا شك أن الوعي قد ازداد خلال السنوات الخمس الماضية فيما يخص نقاط الضعف في البرامج والشبكات، والحاجة إلى إجراءات وقائية إلكترونية في المملكة المتحدة. ويعود ذلك جزئيا لعدد من المبادرات، كمبادرة الحكومة التي بعنوان "10 خطوات نحو أمن المعلوماتية"، ولكنه أيضا نتيجة لزيادة الاهتمام الشعبي بالحوادث الإلكترونية التي لها تأثير على الحكومات والشركات. والاعتداءات الإلكترونية ليست بالضرورة معقدة وحتمية الحدوث، وهي في الغالب نتيجة لنقاط ضعف تم استغلالها، ولكنها نقاط ضعف قابلة للتصحيح بسهولة وغالبا ما يمكن اتقاؤها. وفي معظم الحالات، لا يزال ضعف الضحية، وليس براعة المهاجم، هو العامل الحاسم في نجاح الاعتداء الإلكتروني. وتقرر الشركات والمنظمات أين وكيف تستثمر في أمن المعلوماتية بناء على تقييم للتكلفة والمنفعة، ولكنها في نهاية الأمر هي المسؤولة عن أمن بياناتها وأنظمتها. ولن تقلل الشركات من احتمال تعرضها للأذى الإلكتروني إلا من خلال الموازنة بين الخطر على أنظمتها الحيوية وبياناتها الحساسة من الهجمات الإلكترونية، وبين الاستثمار الكافي في الأفراد والتكنولوجيا وإدارة الأنظمة الإلكترونية.

"لا يمكن تصور وجود نظام أمن معلومات يمكنه أن يمنع واحدا من مئة شخص من فتح رسالة تصيّد إلكترونية، وهذا يمكن أن يكون كل ما يتطلبه الأمر".

كيرن مارتن، المدير العام لأمن المعلوماتية في القيادة المركزية الحكومية للاتصالات (GCHQ)

نقص التدريب والمهارات

19-3 تعوزنا المهارات والمعرفة للاستجابة لحاجاتنا من أمن المعلوماتية في كل من القطاعين العام والخاص. ففي الشركات، يفتقر العديد من الموظفين إلى الوعي بأمن المعلوماتية، وهم لا يدركون مسؤولياتهم في هذا المجال، ويعود ذلك جزئيا لعدم توفر التدريب الرسمي، كما إن القطاع العام هو أيضا يفتقر إلى الوعي الإلكتروني.

"أقل من خُمس الشركات تقريبا وفرت التدريب لموظفيها على أمن المعلوماتية في العام الماضي."

استقصاء حوادث انتهاك أمن المعلوماتية 2016

20-3 نحتاج أيضا لتطوير المهارات المتخصصة والقدرات التي ستمكننا من مواكبة التكنولوجيا المتطورة بسرعة، وإدارة المخاطر الإلكترونية المصاحبة لها. تمثل هذه الفجوة في المهارات نقطة ضعف لا بد من إيجاد حل لها.

الأنظمة القديمة وغير المُحدّثة

21-3 سيستمر الكثير من الشركات في المملكة المتحدة في استعمال أنظمة كمبيوتر قديمة وغير مُحدّثة حتى يحين موعد التحديث التالي لأنظمة تكنولوجيا المعلومات لديها. وغالبا ما تعتمد البرامج في تلك الأنظمة على نسخ قديمة وغير مُحدثة. وهذه النسخ القديمة تعاني غالبا من نقاط ضعف يتصيدها المهاجمون ولديهم الأدوات لاستغلالها. والأمر الآخر هو أن بعض المؤسسات تستخدم برامج لا يتوفر دعم فني لها ولا توجد أنظمة لتحديثها.

"حللنا مؤخرا 115,000 جهاز سيسكو (Cisco) على الإنترنت وفي العديد من مقرات العملاء من أجل لفت الانتباه للمخاطر الأمنية التي تمثلها البنى التحتية المتقادمة - وقلة الاهتمام بنقاط الضعف بسبب عدم التصحيح... وتبين لنا أن 106,000 من بين 115,000 جهاز فيها نقاط ضعف معروفة في البرامج التي تشغلها."

التقرير الأمني السنوي لشركة سيسكو عام 2016

توفر موارد القرصنة

22-3 إن سهولة توفر معلومات حول القرصنة وأدوات قرصنة سهلة الاستخدام عبر الإنترنت أصبحت تُتيح لمن يرغبون في تطوير قدراتهم على القرصنة أن يفعلوا ذلك. والمعلومات التي يحتاجها القراصنة لكي ينجحوا بالإيقاع بضحاياهم غالبا ما تكون متوفرة بوضوح ويمكن جمعها بسرعة. إن كل شخص، من الرجل العادي في بيته إلى المسؤول التنفيذي في أية مؤسسة، يحتاج لأن يكون مدركا لدرجة انكشاف بياناته الشخصية وأنظمته على الإنترنت وللدرجة التي يمكن لذلك الانكشاف أن يجعلها عرضة للاستغلال الإلكتروني الخبيث.

"99.9% من نقاط الضعف التي تم استغلالها قد تعرضت للهجوم بعد أكثر من سنة من الإعلان عنها."

تقرير تحقيقات مؤسسة فيريزون (Verizon) عن انكشاف البيانات 2015

الاستنتاجات

23-3 اتبعت المملكة المتحدة سياسات وأسست مؤسسات عززت دفاعاتنا وخففت من بعض المخاطر التي نواجهها في الفضاء الإلكتروني.

24-3 إلا أننا لم نتجاوز الخطر بعد. فأنواع مجرمي الإنترنت الذين علينا أن نتعامل معهم، ودوافعهم، ما زالت قائمة لحد بعيد، بل إن كمية البرامج الضارة وأعداد المجرمين قد ازدادت بسرعة فائقة. وقدرات أعدائنا الأكثر كفاءة من الناحية الفنية، وتحديدا عدد من الدول المحددة ونخبة من مجرمي الإنترنت، قد تعاظمت. والتحدي المشترك الذي نواجهه هو ضمان أن تكون دفاعاتنا متطورة وقادرة على التكيف بما يكفي لمواجهتهم، والحد من قدرة هؤلاء الأشرار على مهاجمتنا، ومعالجة مسببات نقاط الضعف آنفة الذكر.

4 ردنا الوطني

1-4 لكي نخفف من التهديدات المتعددة التي نواجهها ونحمي مصالحنا في الفضاء الإلكتروني، نحتاج لمقاربة استراتيجية تساند كافة تحركاتنا الفردية والجماعية في المجال الرقمي خلال السنوات الخمس القادمة. وهذا الفصل يستعرض رؤيتنا ومقاربتنا الاستراتيجية.

رؤيتنا

2-4 تتلخص رؤيتنا لسنة 2021 في **أن تكون المملكة المتحدة في مأمن من التهديدات الإلكترونية ولديها القدرة على الصمود في وجهها، وأن تكون مزدهرة ومفعمة بالثقة في العالم الرقمي.**

3-4 لتحقيق تلك الرؤية، سنعمل لأجل تحقيق الأهداف التالية:

- **الدفاع**: أن تكون لدينا الوسائل للدفاع عن المملكة المتحدة ضد التهديدات الإلكترونية الآخذة في التطور، والاستجابة بفعالية للحوادث، وضمان أن الشبكات والبيانات والأنظمة في المملكة المتحدة محمية وقادرة على الصمود. وأن تكون لدى المواطنين والشركات والقطاع العام المعرفة والقدرة للدفاع عن أنفسهم.
- **الردع**: أن تصبح المملكة المتحدة هدفا عسيرا لكل أشكال الاعتداء في الفضاء الإلكتروني، بحيث نكتشف أي عمل عدائي موجه ضدنا ونفهم طبيعته ونحقق به ثم نعرقله، كما نطارد المعتدين ونقدمهم للمحاكمة. كما ستكون لدينا سبل القيام بعمل هجومي في الفضاء الإلكتروني، في حال رغبنا بذلك.
- **التطوير**: أن يصبح لدينا قطاع أمن معلوماتية مبتكر ومتنامي، تسانده أعمال بحث وتطوير علمي رائدة عالميا. كما يتوفر لدينا مورد مستدام من المواهب يوفر المهارات اللازمة للاستجابة لاحتياجاتنا الوطنية في كافة جوانب القطاعين العام والخاص. وخبرتنا وقدرتنا على التحليل المتفوقة ستمكن المملكة من التصدي للتهديدات والتحديات المستقبلية والتغلب عليها.

4-4 ولدعم تلك الأهداف، سنتبع سياسة **العمل الدولي** ونمارس نفوذنا عن طريق الاستثمار في الشراكات. وسوف نرسم جوانب التطور العالمي للفضاء الإلكتروني بشكل يحقق التقدم لمصالحنا الاقتصادية والأمنية الأعم.

المبادئ

5-4 من خلال العمل لتحقيق تلك الغايات، ستطبق الحكومة المبادئ التالية:

- ستكون جهودنا وسياساتنا مدفوعة بالحاجة إلى حماية مواطنينا وتعزيز رفاهنا في آن معا؛
- سنتعامل مع أي اعتداء إلكتروني على المملكة المتحدة بنفس الجدية التي نتعامل بها مع هجوم تقليدي يعادله، وسندافع عن أنفسنا كما تقتضي الضرورة؛
- سنتصرف وفقا للقوانين الوطنية والدولية، ونتوقع من الآخرين أن يفعلوا ذلك أيضا؛
- سنحمي قيمنا الأساسية بقوة ونعمل على نشرها. وهي تشمل الديمقراطية، وسيادة القانون، والحرية، وحكومات ومؤسسات منفتحة وتخضع للمساءلة، وحقوق الإنسان، وحرية التعبير؛
- سوف نحافظ على خصوصية مواطني المملكة المتحدة ونحميها؛
- سنعمل بالشراكة مع الآخرين. وفقط من خلال العمل مع الحكومات المفوّضة، وكافة مكونات القطاع العام، والشركات والمؤسسات، والمواطن الفرد سنتمكن من حماية المملكة المتحدة بنجاح في الفضاء الإلكتروني؛
- ستضطلع الحكومة بمسؤوليتها، وتقود جهود الرد الوطني على الاعتداءات. ولكن تقع على عاتق الشركات والمؤسسات والمواطنين الأفراد مسؤولية اتخاذ خطوات مناسبة لحماية أنفسهم على الإنترنت، وضمان أنهم قادرين على الصمود وعلى الاستمرار في العمل في حال وقوع حادث؛

- تقع مسؤولية أمن المؤسسات في كامل القطاع العام، بما في ذلك أمن المعلوماتية وحماية بيانات وخدمات الإنترنت، على عاتق الوزراء المعنيين، ووكلاء الوزارة الدائمين، ومجالس الإدارات؛
- لن نقبل أن يتعرض المواطنون والبلاد بمجملها لخطر نتيجة لفشل الشركات والمؤسسات باتخاذ الإجراءات اللازمة لإدارة المخاطر الإلكترونية؛
- سنعمل بشكل وثيق مع الدول التي تشاركنا وجهات النظر والتي يتداخل أمننا مع أمنها، لإدراكنا أن التهديدات الإلكترونية لا تعترف بالحدود. كما سنعمل بشكل أعم مع نطاق واسع من الشركاء الدوليين للتأثير على قطاع أكبر من المجتمع الدولي، مع إدراكنا لقيمة التحالفات الموسعة؛
- لضمان أن مداخلات الحكومة سيكون لها وقع قوي على مجمل أمن المعلوماتية والصمود الوطنيين، سنسعى لتحديد وتحليل وتقديم البيانات التي تقيس حالة أمن المعلوماتية الجماعي لدينا ونجاحنا في بلوغ أهدافنا الاستراتيجية.

الأدوار والمسؤوليات

6-4 تتطلب حماية الفضاء الإلكتروني الوطني جهدا جماعيا. فكل واحد منا له دور هام يؤديه.

الأفراد

7-4 كمواطنين وموظفين ومستهلكين، نتخذ خطوات عملية لحماية ممتلكاتنا في العالم المادي. وعلينا أن نفعل ذلك أيضا في العالم الافتراضي. ذلك يعني القيام بواجبنا في اتخاذ كافة الإجراءات المعقولة، ليس فقط لحماية أجهزتنا الإلكترونية - كهواتفنا الذكية وغيرها من الأجهزة - بل أيضا البيانات والبرامج والأنظمة التي تمنحنا الحرية والمرونة والراحة في حياتنا الخاصة والمهنية.

الشركات والمؤسسات

8-4 تحتفظ الشركات ومؤسسات القطاعين العام والخاص وغيرها من المؤسسات ببيانات شخصية، وتوفر الخدمات وتشغل الأنظمة في المجال الرقمي. إن توفر تلك المعلومات عبر الإنترنت قد أحدث ثورة في طريقة عمل تلك المؤسسات. ولكن مع هذا التحول التكنولوجي تأتي المسؤولية على المؤسسات لحماية تلك الموارد التي بحوزتها، والاستمرار في تقديم خدماتها، وإدخال المستوى الملائم من الأمن على المنتجات التي تبيعها. ويتوقع المواطنون والمستهلكون، والمجتمع بصفة عامة، من الشركات والمؤسسات أن تأخذ كافة الإجراءات المعقولة لحماية بياناتهم الشخصية ولتحقيق القدرة على الصمود - القدرة على التحمل والتعافي - في الأنظمة والهياكل التي تعتمد عليها. كما يتوجب على الشركات والمؤسسات أن تعي أنها لو وقعت ضحية لاعتداء إلكتروني، فإنها ستكون مسؤولة عن نتائج ذلك.

الحكومة

9-4 الواجب الأساسي على الحكومة هو أن تدافع عن البلاد ضد هجمات الدول الأخرى، وأن تحمي المواطنين والاقتصاد من الأذى، وأن تضع الإطار العام الداخلي والدولي لحماية مصالحنا والدفاع عن الحقوق الأساسية وتقديم المجرمين لمواجهة العدالة.

10-4 ولكون الحكومة هي التي تحتفظ بالبيانات الهامة وتوفر الخدمات، فإنها تتخذ إجراءات صارمة لحماية ما لديها من معلومات. كما أن على الحكومة مسؤولية هامة بأن تنصح المواطنين والمؤسسات وترشدهم إلى ما يتوجب عليهم أن يفعلوه لحماية أنفسهم على الإنترنت. وينبغي عليها أيضا، حين تقتضي الضرورة، أن تحدد المعايير التي تتوقع من الشركات والمؤسسات الكبرى أن تستوفيها.

11-4 رغم أن قطاعات أساسية من اقتصادنا هي في أيدي مؤسسات خاصة، فإن الحكومة هي المسؤولة في نهاية المطاف عن ضمان قدرة هذه المؤسسات على الصمود إزاء أي هجوم، وعن استمرار الخدمات والمهام الرئيسية في أنحاء الحكومة برمتها، بالتعاون مع شركائها في مختلف أركان الإدارة الحكومية.

إحداث التغيير: دور السوق

12-4 إن استراتيجية عام 2011 والبرنامج الوطني لأمن المعلوماتية قد سعيا لتحقيق النتائج وزيادة القدرات في كل من القطاعين العام والخاص عن طريق التطلع إلى السوق لتشجيع الممارسات السليمة. وقد توقعنا أن تؤدي الضغوط التجارية والحوافز التي تقدمها الدولة من أجل ضمان الاستثمار الملائم من الشركات في أمن المعلوماتية إلى تحفيز تدفق الاستثمارات إلى قطاع المعلوماتية لدينا، وتشجيع توفر موارد مستمرة وملائمة من المهارات في هذا القطاع.

13-4 لقد تم إنجاز الكثير. فالوعي بالمخاطر وبالعمل المطلوب لتخفيف حدة المخاطر الإلكترونية قد ازداد في كافة قطاعات الاقتصاد وفي المجتمع بصورة أعم خلال السنوات الخمس الماضية. إلا أن ذلك المزيج من قوى السوق والتشجيع الحكومي لم يكن كافيا بحد ذاته لحماية مصالحنا طويلة الأمد في الفضاء الإلكتروني بالوتيرة المرغوبة. فهناك الكثير جدا من الشبكات، ومنها في قطاعات حيوية، لا تزال غير آمنة. والسوق لا يعطي الخطر الإلكتروني حق قدره، وبالتالي لا يديره بالشكل الصحيح. ولا يزال الكثير جدا من الشركات يتعرض لانتهاكات إلكترونية حتى على أبسط المستويات. وهناك عدد ضئيل جدا من المستثمرين ممن أبدوا استعدادهم للمجازفة بدعم رواد الأعمال في هذا القطاع. ويضاف إلى ذلك أن عددا ضئيلا من الخريجين وغيرهم من ذوي المهارات الملائمة يبرز من قطاع التعليم ونظام التدريب.

14-4 لا يزال هناك دور للسوق ليلعبه، وعلى المدى الطويل سيكون للسوق تأثير أكبر مما قد تحققه الحكومة على الإطلاق. إلا أن الخطر الداهم الذي تواجهه المملكة المتحدة واتساع نقاط الضعف في بيئتنا الرقمية يدعوان لتحرك أكبر من جانب الحكومة على المدى القصير.

إحداث التغيير: الدور الموسع للحكومة

15-4 ينبغي على الحكومة بالتالي أن تحدد الوتيرة للاستجابة للاحتياجات الوطنية للبلاد بالنسبة لأمن المعلوماتية. فالحكومة هي وحدها التي تستطيع تستفيد من المعلومات الاستخباراتية والموارد الأخرى المطلوبة لكي تدافع عن البلاد ضد أشد التهديدات تطورا. وهي وحدها التي تستطيع أن تدفع بالتعاون بين القطاعين العام والخاص وأن تضمن مشاركة المعلومات بينهما. وللحكومة دور قيادي في تحديد ما يجب أن يكون عليه أمن المعلوماتية الجيد وضمان تطبيقه، وذلك بالتشاور مع قطاع المعلوماتية.

16-4 ستُدخل الحكومة تحسينا كبيرا على أمن المعلوماتية الوطني لدينا على مدى السنوات الخمس القادمة. وسوف يركز هذا البرنامج التطويري الطموح على الجوانب العامة الأربعة التالية:

- **العوامل المساعدة والحوافز**. سوف تستثمر الحكومة لكي ترفع إلى الحد الأقصى إمكانات قطاع معلوماتية مبدع حقا في المملكة المتحدة. وسوف نفعل ذلك من خلال دعم الشركات الناشئة، وبالاستثمار في الابتكار. كما سنسعى لاستكشاف واستمالة المواهب في مرحلة مبكرة من النظام التعليمي، وتطوير سبل أكثر وضوحا تؤدي إلى اختيار العمل في مهنة تحتاج لتعريفها بشكل أفضل. كما ستستفيد الحكومة من كافة العوامل المساعدة المتاحة، بما في ذلك "قواعد حماية البيانات العامة" التي ستصدر قريبا، وذلك لرفع مستويات أمن المعلوماتية في كافة قطاعات الاقتصاد، بما فيها اللجوء إلى التنظيم، إن اقتضت الضرورة.
- **العمل الاستخباراتي الموسع وتركيز أجهزة تطبيق القانون على التهديدات**. إن أجهزة الاستخبارات ووزارة الدفاع والشرطة والوكالة الوطنية لمكافحة الجريمة ستوسع نطاق جهودها، بالتنسيق مع أجهزة دولية شريكة، لكي تكشف الأنشطة الإلكترونية العدائية للناشطين الخارجيين ومجرمي الإنترنت والإرهابيين، وتتوقع حدوثها وتعرقلها. وهذا من شأنه أن يحسن قدرة تلك المؤسسات على جمع المعلومات والاستفادة منها، لغرض الحصول على معلومات استباقية عن نوايا أعدائنا وقدراتهم.
- **تطوير التكنولوجيا واستخدامها** بالشراكة مع قطاع المعلوماتية، بما في ذلك تدابير "الدفاع الإلكتروني الفعال"، من أجل تعميق فهمنا للتهديد ولتقوية أمن الأنظمة والشبكات في القطاعين العام والخاص في المملكة المتحدة بمواجهة ذلك التهديد، ولعرقلة أي نشاط خبيث.
- **المركز الوطني لأمن المعلوماتية**. أنشأته الحكومة ليكون جهة مركزية واحدة للأمن الإلكتروني على المستوى الوطني. سوف يدير هذا المركز الحوادث الإلكترونية على مستوى البلاد، وسيوفر الرأي الخبير والخبرة فيما يتعلق بأمن المعلوماتية، ويقدم الدعم والمشورة اللذين يلبيان احتياجات الوزارات، والحكومات المفوضة، والجهات التنظيمية، والشركات. وسوف يعمل هذا المركز لتحليل التهديدات الإلكترونية وكشفها وفهمها، كما سيقدم خبرته في مجال أمن المعلوماتية لدعم جهود الحكومة الرامية لرعاية الابتكار، ولمساندة قطاع أمن المعلوماتية المزدهر، وتحفيز عملية تطوير مهارات أمن المعلوماتية. وينفرد المركز، كمؤسسة خدماتها متاحة لعامة المواطنين، بأنه يتبع القيادة المركزية الحكومية للاتصالات، وبالتالي يستطيع الاستفادة من الخبرة عالمية المستوى والقدرات الحساسة لتلك المؤسسة، وهو ما سيحسن من الدعم الذي سيقدمه المركز للاقتصاد والمجتمع بشكل أعم. وسوف تظل مسؤولية ضمان تطبيق نصائح أمن المعلوماتية بفعالية تقع على عاتق الإدارات

الحكومية.

"نظرا لسرقة ممتلكات فكرية على مستوى واسع من شركاتنا وجامعاتنا، إلى جانب العديد من حالات التصيد بالرسائل الإلكترونية والاحتيال بالبرامج الضارة التي تهدر المال والوقت، يُظهر المركز الوطني لأمن المعلوماتية أن المملكة المتحدة تركز جهودها على مكافحة التهديدات الموجودة على الإنترنت."

روبرت هانيغان، مدير القيادة المركزية الحكومية للاتصالات، مارس 2016

17-4 إن إنجاز هذه التغييرات في أمننا الإلكتروني وقدرتنا على الصمود أمام الهجمات سيتطلب موارد إضافية. وفي مراجعة الدفاع الاستراتيجي والأمن لعام 2015، خصصت الحكومة مبلغ 1.9 مليار جنيه إسترليني على مدى السنوات الخمس للاستراتيجية لتنفيذ تلك الالتزامات والأهداف.

المركز الوطني لأمن المعلوماتية

تأسس المركز الوطني لأمن المعلوماتية (NCSC) في الأول من أكتوبر 2016. يوفر هذا المركز فرصة نادرة لتأسيس شراكات فاعلة في مجال أمن المعلوماتية بين الحكومة وقطاع المعلوماتية والمواطنين لضمان أن تصبح المملكة المتحدة أكثر أماناً على الإنترنت. سيوفر المركز الاستجابة لحوادث الهجمات الإلكترونية، وسيمثل الرأي الخبير للمملكة في قضايا أمن المعلوماتية. وللمرة الأولى ستتمكن قطاعات رئيسية من أن تتواصل مباشرة مع العاملين في المركز من أجل الحصول على أفضل مشورة ومساعدة ممكنة حول حماية الشبكات والأنظمة من التهديدات الإلكترونية.

هذا المركز:

- مصدر موحد لتقديم المشورة للحكومة بمجال جمع المعلومات عن التهديدات الإلكترونية، ولضمان أمن المعلومات؛
- هو الواجهة العامة القوية لما تفعله الحكومة للتصدي للتهديدات الإلكترونية - وهو يعمل جنبا إلى جنب مع قطاع المعلوماتية والأكاديميين والشركاء الدوليين لحماية المملكة المتحدة من الهجمات الإلكترونية؛
- مركز خدماته متاحة لعامة المواطنين، ويستطيع أن يلجأ إلى القيادة المركزية الحكومية للاتصالات للحصول على معلومات استخباراتية، سرية بالضرورة، وخبرة فنية على مستوى عالمي.

وسوف تُتَّبع مقاربة متدرجة لبناء قدرات المركز على مدى عمر هذه الاستراتيجية. وسوف يجمع القدرات التي طورتها الهيئة الفنية الوطنية لضمان المعلومات في المملكة المتحدة (CESG) - وهي ذراع أمن المعلوماتية التابع للقيادة المركزية الحكومية للاتصالات، ومركز حماية البنية التحتية الوطنية (CPNI)، والفريق الوطني للاستجابة لطوارئ الكومبيوتر (CERT)، ومركز تقييم المعلوماتية (CAA)، الأمر الذي سيمكننا من البناء على أفضل ما هو لدينا أصلا، مع تبسيط الإجراءات السابقة بشكل كبير في نفس الوقت. وسيكون تركيز هذا المركز أساسا على ما يلي:

- تطوير قدرة إدارة الحوادث على مستوى عالمي للتعامل مع الأضرار الناجمة عن الحوادث الإلكترونية وتقليل ضررها - من الحوادث التي تصيب مؤسسة منفردة وحتى الهجمات واسعة النطاق على المستوى الوطني؛
- توفير معلومات عن كيفية تعامل المؤسسات في القطاعين العام والخاص مع مسائل أمن المعلوماتية، الأمر الذي يسهل تشارك المعلومات حول التهديدات الإلكترونية؛
- الاستمرار في تقديم المشورة الخبيرة عن قطاعات معينة للحكومة والقطاعات الحيوية، كالاتصالات اللاسلكية والطاقة والمال، وكذلك تقديم المشورة بشأن أمن المعلوماتية في كافة أرجاء المملكة المتحدة.

ويوفر المركز الوطني لأمن المعلوماتية وسيلة فعالة للحكومة لتنفيذ عناصر عديدة من هذه الاستراتيجية. ونحن ندرك أنه مع نمو المركز ستكون هناك حاجة لتعديل قدراته وأوجه تركيزه لتتماشى مع التحديات الجديدة والدروس المستفادة.

خطة التنفيذ

إن أهدافنا من أجل أمن المعلوماتية في البلاد على مدى السنوات الخمس القادمة طموحة بكل حق. وتحقيقها يتطلب منا أن نعمل بمسؤولية وعزيمة على الساحة الرقمية ككل. والعمل الذي سنؤديه لتحقيق رؤية الحكومة سوف يخدم الأهداف الرئيسية الثلاثة للاستراتيجية: **الدفاع** عن فضائنا الإلكتروني، و**ردع** أعدائنا، و**تطوير** قدراتنا، وكل ذلك بالاستناد إلى **عمل دولي** فعال.

5 الدفاع

1-0-5 تهدف عناصر الدفاع في هذه الاستراتيجية لضمان أن تكون شبكات وبيانات وأنظمة القطاع العام والمؤسسات التجارية والخاصة قادرة على الصمود أمام الاعتداءات الإلكترونية ومحمية منها. لن يكون بالإمكان أبدا وقف كل اعتداء إلكتروني، كما هو ليس ممكنا منع كل جريمة. ولكن حين يعمل المواطنون والمؤسسات التعليمية والأكاديميون والشركات والحكومات الأخرى مع بعضهم البعض، ستتمكن المملكة المتحدة من بناء خطوط دفاعية يمكنها أن تقلل بدرجة كبيرة من تعرض البلاد لحوادث إلكترونية، وأن تحمي أغلى ما نمتلك، وأن تتيح لنا جميعا أن نعمل بنجاح ونزدهر في الفضاء الإلكتروني. كما إن العمل من أجل تطوير التعاون بين الدول، وتطبيق الممارسات الجيدة في مجال أمن المعلوماتية، سيصب أيضا في مصلحة أمننا الجماعي.

2-0-5 ستتخذ الحكومة إجراءات لضمان أن تتوفر للأفراد والشركات ومؤسسات ومنظمات القطاعين العام والخاص المعلومات المناسبة للدفاع عن نفسها. ويوفر المركز الوطني لأمن المعلوماتية مصدرا موحدا لتقديم المشورة في الحكومة حول الاستخبارات بشأن التهديدات وحماية المعلومات، بحيث يمكننا تقديم إرشادات حسب الحاجة من أجل الدفاع الإلكتروني، وأن نرد بسرعة وفاعلية على الحوادث الكبرى في الفضاء الإلكتروني. وستعمل الحكومة مع قطاع المعلوماتية والشركاء الدوليين من أجل تحديد ماهية أمن المعلوماتية الجيد للقطاعين العام والخاص، ولأنظمتنا وخدماتنا الأكثر أهمية، وللاقتصاد ككل. وسوف نحرص على تصميم كافة الأنظمة الحكومية والحيوية بحيث تكون آمنة افتراضيا (secure by default). وستتعاون الأجهزة الأمنية بشكل وثيق مع قطاع المعلوماتية والمركز الوطني لأمن المعلوماتية من أجل توفير معلومات استخباراتية حيوية عن التهديدات الإجرامية التي يستطيع قطاع المعلوماتية من خلالها أن يدافع عن نفسه بشكل أفضل، وأن يطور المشورة ومعايير الحماية الأمنية.

1-5 الدفاع الإلكتروني الفاعل

1-1-5 الدفاع الإلكتروني الفاعل هو مبدأ تطبيق الإجراءات الأمنية لتقوية شبكة أو نظام لجعلهما أكثر صمودا في مواجهة الهجمات. في السياق التجاري، عادة ما يشير الدفاع الإلكتروني الفاعل إلى قيام محللي أمن المعلوماتية بتطوير فهمهم للتهديدات التي تتعرض لها شبكاتهم ومن ثم وضع وتطبيق إجراءات استباقية لمكافحة تلك التهديدات أو الدفاع ضدها. وفي سياق هذه الاستراتيجية، اختارت الحكومة أن تطبق نفس المبدأ على نطاق أوسع: فهي ستستغل خبراتها الفريدة وقدراتها ونفوذها لإحداث تغيير كبير في أمن المعلوماتية الوطني للرد على التهديدات الإلكترونية. و"الشبكة" التي نحاول أن ندافع عنها هي الفضاء الإلكتروني للمملكة المتحدة بأكمله. والأعمال المقترحة تمثل خطة عمل دفاعية تعتمد على خبرات المركز الوطني لأمن المعلوماتية بصفته "الهيئة الفنية الوطنية" للرد على التهديدات الإلكترونية الموجهة للمملكة المتحدة على مستوى الدولة.

الهدف

2-1-5 بتبنيها أسلوب الدفاع الإلكتروني الفاعل، فإن الحكومة تهدف إلى:

- جعل المملكة المتحدة هدفا صعبا جدا بالنسبة للأطراف التي ترعاها دول ومجرمي الإنترنت، وذلك عن طريق زيادة قدرة شبكات المملكة على الصمود في حال وقوع اعتداء؛
- هزيمة الغالبية العظمى من أنشطة البرامج الضارة واسعة النطاق ومنخفضة التعقيد ضد شبكات المملكة المتحدة، وذلك عن طريق حجب اتصالات البرامج الضارة بين القراصنة وضحاياهم؛
- تطوير وزيادة مجال ومستوى قدرات الحكومة على عرقلة التهديدات الإلكترونية الخطيرة التي ترعاها دول، والتهديدات الإجرامية الإلكترونية؛
- حماية خدمة الإنترنت وحركة الاتصالات اللاسلكية من الاختطاف من جانب أطراف خبيثة؛
- تقوية البنية التحتية الحيوية للمملكة المتحدة والخدمات المقدمة للمواطنين ضد التهديدات الإلكترونية؛
- تعطيل منهج عمل المهاجمين بكافة أشكالهم، لثنيهم عن عزمهم ولخفض الضرر الذي يمكن أن تسببه هجماتهم.

مقاربتنا

3-1-5 في سعيها لتحقيق تلك الأهداف، فإن الحكومة:

- ستعمل مع قطاع المعلوماتية، وخاصة مقدمي خدمات الاتصالات، من أجل جعل الهجوم على خدمات الإنترنت ومستخدميها في المملكة المتحدة أصعب بكثير، ومن أجل ضمان تقليل كبير في احتمال أن يكون للهجمات تأثير مستدام على المملكة. سوف يشمل ذلك التصدي للتصيّد بالرسائل الإلكترونية، وحجب النطاقات الإلكترونية وعناوين بروتوكولات الإنترنت (IP) الضارة، بالإضافة إلى خطوات أخرى من أجل عرقلة هجمات البرامج الضارة. كما سيشمل أيضا إجراءات لحماية الاتصالات اللاسلكية والبنية التحتية لنظام توجيه الإنترنت (routing).

- وستزيد من نطاق وتطوير قدرات القيادة المركزية الحكومية للاتصالات، ووزارة الدفاع، والوكالة الوطنية لمكافحة الجريمة من أجل تعطيل التهديدات الإلكترونية الأشد خطورة ضد المملكة المتحدة، بما في ذلك الحملات التي يشنها مجرمو إنترنت محنكون وأطراف أجنبية معادية.

- وستحمي أنظمة الحكومة وشبكاتها بشكل أفضل، وتساعد قطاع المعلوماتية في تقوية أمن سلسلة موردي البنية التحتية الوطنية الحيوية، وتجعل بيئة البرامج أكثر أمنا بالمملكة المتحدة، وستوفر حماية آلية للخدمات التي تقدمها الحكومة للمواطنين عبر الإنترنت.

4-1-5 حيثما أمكن، سيتم تنفيذ هذه المبادرات إما ضمن أو من خلال شراكات مع قطاع المعلوماتية. وبالنسبة للكثيرين، سوف يتولى قطاع المعلوماتية التصميم وقيادة التنفيذ، بينما المساهمة الحيوية من جانب الحكومة تتمثل بالدعم من الخبراء وتقديم والمشورة والقيادة الفكرية.

5-1-5 كما ستتخذ الحكومة تدابير محددة لتنفيذ تلك الإجراءات، والتي سوف تشمل ما يلي:

- العمل مع مقدمي خدمات الاتصالات لحجب اعتداءات البرامج الضارة. وسنفعل ذلك عن طريق تقييد الوصول إلى نطاقات (domains) معينة أو مواقع إلكترونية تعرف بأنها مصدر للبرامج الضارة (malware). وهذا ما يعرف بحجب أو فلترة "نظام اسم النطاق" (Domain Name System)؛

- منع أنشطة التصيّد بالرسائل الإلكترونية التي تعتمد على انتحال الهوية في النطاق (حيث تبدو الرسالة وكأنها مرسلة من طرف معين، مثل البنك أو إدارة حكومية، ولكنها في حقيقة الأمر خدعة)، وسيتم المنع باستخدام نظام التحقق من الرسائل الإلكترونية على شبكات الحكومة كإجراء ثابت، وتشجيع قطاع المعلوماتية أن يفعل الشيء ذاته؛

- ترويج أفضل الممارسات الأمنية عن طريق مؤسسات متعددة الأطراف لإدارة الإنترنت، مثل مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN) (التي تنسق نظام اسم النطاق)، وفريق مهام هندسة الإنترنت (IETF)، والسجل الأوروبي الإقليمي للإنترنت (RIPE)، وكذلك عن طريق التعاون مع المعنيين في منتدى الأمم المتحدة لإدارة الإنترنت (IGF)؛

- العمل مع قنوات تنفيذ القانون من أجل حماية مواطني المملكة المتحدة من الاستهداف بالهجمات الإلكترونية من خلال بنية تحتية خارجية غير محمية؛

- العمل من أجل تنفيذ ضوابط لحماية نظام توجيه خطوط الإنترنت للدوائر الحكومية، وذلك لضمان عدم إمكانية إعادة توجيهها بطريقة غير مشروعة من جانب أطراف خبيثة؛

- الاستثمار في برامج وزارة الدفاع، والوكالة الوطنية لمكافحة الجريمة، والقيادة المركزية الحكومية للاتصالات، بحيث تعزز تلك البرامج قدرات هذه المؤسسات للاستجابة للعمليات الإلكترونية الإجرامية الخطيرة التي ترعاها دول وتستهدف شبكات المملكة المتحدة، وعرقلتها.

ومع تطور التهديدات، سوف نطور تلك القدرات الفنية على التدخل لكي نضمن أن مواطني المملكة المتحدة وشركاءنا محميين افتراضيا من غالبية الهجمات الإلكترونية الكبيرة التي تُستخدم فيها برامج متوفرة تجاريا.

قياس النجاح

6-1-5 سوف تقيس الحكومة مدى نجاحها في إنشاء دفاع إلكتروني فعال عن طريق تقييم التقدم الذي تم إحرازه نحو تحقيق النتائج التالية:

- جعل المملكة المتحدة هدفا صعبا لمحاولات التصيّد بالرسائل الإلكترونية لأن لدينا دفاعات واسعة النطاق ضد استخدام النطاقات (domains). ولدينا حماية أكثر فاعلية ضد التصيّد، كما إنه من الصعب جدا استخدام أساليب أخرى للاتصالات مثل التصيد الصوتي (vishing) وانتحال الشخصية بالرسائل النصية (SMS spoofing) من أجل شن هجمات من نوع "الهندسة الاجتماعية"؛
- حجب الجزء الأكبر من اتصالات البرامج الضارة والخدع التقنية المصاحبة للهجوم الإلكتروني والاستغلال؛
- جعل انسياب الاتصالات اللاسلكية والإنترنت في المملكة المتحدة أقل تعرضا بكثير لإعادة التوجيه من جانب الأطراف الخبيثة،
- تحقيق زيادة ملحوظة في قدرات القيادة المركزية الحكومية للاتصالات، والقوات المسلحة، والوكالة الوطنية لمكافحة الجريمة للرد على التهديدات الإجرامية الخطيرة وتلك التي ترعاها دول.

2-5 بناء إنترنت أكثر أمنا

1-2-5 تغيير التكنولوجيا يوفر لنا الفرصة لأن نقلل بشكل كبير قدرة أعدائنا على شن هجمات إلكترونية على المملكة المتحدة، وذلك عن طريق ضمان أن تكون أجهزة وخدمات الإنترنت التي ستطرح مستقبلا "آمنة افتراضيا". وذلك يعني ضمان الجهة المُصنّعة تفعيل الضوابط الأمنية الداخلة في تصميم الاجهزة والبرامج التي نستخدمها بحيث تكون آمنة افتراضيا كي يحصل المستخدمون على أقصى درجة من الأمان المتاح لهم ما لم يختاروا طوعا عدم تفعيلها. والتحدي الماثل هو إحداث تغيير تحويلي بطريقة تدعم المستخدم النهائي وتقدم منتجات أو خدمات متوفرة تجاريا وآمنة بنفس الوقت - وكل ذلك ضمن سياق الحفاظ على الطبيعة الحرة والمنفتحة للإنترنت.

"الأمور المتصلة بالإنترنت تتضاعف بسرعة، وقد رأينا الكثير من الاعتداءات التجريبية والحقيقية في عام 2015، والتي أدت إلى كشف نقاط ضعف في السيارات والأجهزة الطبية والكثير غيرها. ينبغي على المُصنّعين إعطاء الأولوية للأمن من أجل تقليل خطر العواقب الشخصية والاقتصادية والاجتماعية الخطيرة."

تقرير شركة سيمانتك (Symantec) 2016 عن التهديدات لأمن الإنترنت

2-2-5 إن الحكومة بمكانة تتيح لها أن تلعب دورا قياديا في اكتشاف تلك التكنولوجيات الجديدة التي ستحمي أنظمتنا بشكل أفضل، وتساعد قطاع المعلوماتية في إدخال المزيد من المزايا الأمنية في سلسلة التوريد، وأن تحمي بيئة البرامج وتوفر أساليب حماية آلية للمواطنين الذين يدخلون على خدمات الحكومة على الإنترنت. وعلى الحكومة أن تختبر وتطبق تكنولوجيات جديدة تقدم حماية آلية للمنتجات والخدمات الحكومية المقدمة عبر. ولا بد من تقديم تكنولوجيات مشابهة للمواطنين والقطاع الخاص حيثما أمكن ذلك.

الهدف

3-2-5 غالبية المنتجات والخدمات المتوفرة عبر الإنترنت والتي ستدخل الخدمة ستصبح "آمنة افتراضيا" بحلول 2021. وسيتم تمكين المستهلكين لاختيار المنتجات والخدمات التي يكون الأمن مدمج في تصميمها بحيث تكون "آمنة افتراضيا". وبإمكان الأفراد تعطيل هذه الخاصية إن أرادوا ذلك، إلا أن المستهلكين الذين يرغبون بالتعامل من خلال الفضاء الإلكتروني بأكثر الطرق أمنا سيكونون محميين تلقائيا.

مقاربتنا

4-2-5 سوف نتبع الإجراءات التالية:

- ستكون الحكومة قدوة بأن تشغل خدمات آمنة على الإنترنت لا تُعوِّل على كون الإنترنت نفسها آمنة؛
- ستبحث الحكومة في خيارات التعاون مع قطاع المعلوماتية لتطوير طرق متطورة لجعل الأجهزة والبرامج "آمنة افتراضيا"؛

- سنتبنى تكنولوجيات أمن معلوماتية جديدة ومعقدة في الحكومة، مع تشجيع الحكومات المفوضة على أن تحذو حذونا، من أجل تقليل المخاطر التي قد تظهر في تبني تلك التكنولوجيات الجديدة. إن ذلك سيكون مثالا حيا وسيوضح الفوائد الأمنية للتكنولوجيات والمقاربات الجديدة. كما أنه سيضع مسألة الأمن في قلب جهود تطوير منتجات جديدة، ويزيل أية فرص للاستغلال الإجرامي، وبالتالي يحمي المستخدم النهائي.

5-2-5 ولكي ننجز ذلك، فإننا سوف:

- نستمر في تشجيع موردي الأجهزة والبرامج على أن يبيعوا منتجات تكون الإعدادات الأمنية فيها مُفعّلة بحيث تكون آمنة افتراضيا، الأمر الذي يعني أن المنتج لن يصبح غير آمن إلا إذا تعمد المستخدم أن يوقف عمل تلك الإعدادات. بعض البائعين يفعلون ذلك بالفعل، ولكن آخرين لم يتخذوا بعد هذه الخطوات الضرورية؛

- نواصل تطوير خدمة تقييم سمعة بروتوكولات الإنترنت (IP) لكي نحمي الخدمات الرقمية الحكومية (سوف يسمح ذلك لخدمات الإنترنت بالحصول على معلومات حول عناوين بروتوكولات الإنترنت المتصلة بها، ما يساعد الخدمة على أن تتخذ قرارات بشأن إدارة المخاطر تستند إلى المعلومات وبالوقت المناسب)؛

- نسعى لإدخال منتجات على شبكات الحكومة من شأنها أن توفر الضمان بأن البرامج تعمل بالشكل السليم، وأنها لا تتعرض لتدخلات خبيثة؛

- نحرص على التوسع لما وراء نطاق موقع GOV.UK وصولا إلى إجراءات خدمات رقمية أخرى تحذر المستخدمين الذين يستعملون مواقع تصفح قديمة؛

- نستثمر في تكنولوجيات مثل شراح الأمان (TPM) وفي المقاييس الناشئة في قطاع المعلوماتية مثل التحقق من هوية المستخدم سريعا على الإنترنت (FIDO) التي لا تعتمد على كلمات المرور من أجل التحقق من هوية المستخدم، ولكنها تستخدم الجهاز وأدوات أخرى في حوزة المستخدم من أجل هذا الغرض. وسوف تختبر الحكومة آليات مبتكرة للتحقق من الهوية لكي تُظهر ما يمكن لتلك الآليات أن تقدمه، سواء من ناحية الأمن وكذلك من ناحية إجمالي تجربة المستخدم على الإنترنت.

6-2-5 كما ستبحث الحكومة في كيفية تشجيع السوق عن طريق إعطاء تصنيف أمني للمنتجات الجديدة، بحيث تتوفر للمستهلكين معلومات واضحة عن المنتجات والخدمات التي تقدم لهم أقصى درجات الأمن. وستبحث الحكومة في كيفية ربط تصنيفات تلك المنتجات بالجهات التنظيمية، القائمة والجديدة، وعن سبل تحذير المستهلكين عندما يكونون مقبلين على اتخاذ خطوة ما على الإنترنت من شأنها أن تعرض أمنهم للخطر.

قياس النجاح

7-2-5 سوف تقيس الحكومة مدى نجاحها في بناء خدمة إنترنت آمنة عن طريق تقييم ما تم إحرازه من تقدم نحو تحقيق الغايات التالية:

- أن تكون غالبية المنتجات والخدمات المتوفرة في المملكة المتحدة عام 2021 تساهم في جعلها أكثر أمنا لأن الإعدادات الأمنية لهذه المنتجات محددة بحيث تكون "أمنة افتراضيا"، أو أن مستلزمات الأمن مدمجة أصلا في تصميمها؛

- يثق المواطنون البريطانيون بكافة الخدمات التي تقدمها الحكومة على المستوى الوطني والمحلي وعلى مستوى الحكومات المفوضة لأنها تُقدّم بأعلى درجة ممكنة من الأمن، ومستويات الاحتيال الذي يستهدفها تقع ضمن المعايير المقبولة للخطر.

3-5 حماية الحكومة

1-3-5 إن لدى حكومة المملكة المتحدة والحكومات المفوضة والقطاع العام عموما كميات ضخمة من البيانات الحساسة. وهذه الجهات تقدم خدمات أساسية للجمهور وتُشغِّل شبكات في غاية الأهمية للأمن القومي ولقدرة البلاد على الصمود أمام الخطر الإلكتروني. وأنظمة الحكومة هي الأساس الذي يرتكز عليه أداء المجتمع. وتحديث خدمات القطاع العام سوف يبقى حجر الأساس في الاستراتيجية الرقمية للمملكة المتحدة - فالطموح الرقمي للحكومة هو أن تصبح المملكة المتحدة البلد الرقمي الرائد في العالم. وللحفاظ على ثقة المواطنين بخدمات وأنظمة القطاع العام على الإنترنت، لا بد للبيانات التي في عهدة الحكومة أن تكون محمية، كما يجب على كافة فروع الحكومة تطبيق مستويات مناسبة من أمن المعلوماتية للتصدي لمحاولات متواصلة من جانب الأطراف المعادية للدخول على شبكات وبيانات الحكومة والقطاع العام.

الهدف

2-3-5 نرغب في تحقيق كل النتائج التالية:

- أن يستخدم المواطنون خدمات الإنترنت الحكومية بثقة: أي أن يكونوا مطمئنين بأن بياناتهم الحساسة في مأمن، وبالمقابل أن يتفهموا مسؤوليتهم بشأن تقديم بياناتهم الحساسة للحكومة على الإنترنت بطريقة آمنة.
- أن تضع الحكومة المعايير الأكثر ملاءمة للحفاظ على أمن المعلوماتية، وأن تلتزم بها لضمان أن كافة فروع الحكومة تتفهم واجباتها وتفي بها من أجل حماية شبكاتها وبياناتها وخدماتها.
- أن تكون المؤسسات الحكومية الحيوية، بما فيها الأعلى سرية، محمية من الهجمات الإلكترونية.

مقاربتنا

3-3-5 سوف تستمر الحكومة البريطانية في نقل المزيد من خدماتها إلى الإنترنت بحيث يمكن للمملكة المتحدة أن تصبح حقا "رقمية افتراضيا". وسوف يعمل كل من "الخدمة الرقمية الحكومية" (GDS) وإدارة "الخدمة التجارية الحكومية" (CCS) والمركز الوطني لأمن المعلوماتية لضمان أن تكون كافة الخدمات الرقمية الجديدة التي تؤسسها أو تشتريها الحكومة هي أيضا "آمنة افتراضيا".

4-3-5 الشبكات الحكومية شديدة التعقيد، وهي في كثير من الحالات لا تزال تستخدم أنظمة قديمة، بالإضافة إلى بعض البرامج المتوفرة تجاريا ولكنها لم تعد مدعومة بخدمة البائعين. لذلك سنعمل لضمان أنه لن تكون هناك أية مخاطر خارج السيطرة من الأنظمة القديمة ومن البرامج غير المدعومة.

5-3-5 سوف نحسن قدرة الحكومة والقطاع العام عموما على الصمود في وجه الهجمات الإلكترونية. ذلك يعني ضمان معرفة دقيقة وتستند إلى أحدث المعلومات عن كافة الأنظمة والبيانات، وعن الذين لديهم صلاحية الدخول إليها. إن احتمال وقوع حادث إلكتروني والآثار المترتبة عليه يمكن تقليلها لأقصى درجة عن طريق تطبيق أفضل الممارسات، وفق ما أشار إليه المركز الوطني لأمن المعلوماتية. وسوف تضمن الحكومة أيضا أنها ستكون قادرة على الرد بفعالية على أية حوادث إلكترونية من خلال برنامج للتدريب على الحوادث والاختبار الدوري لشبكات الحكومة. وسندعو الحكومات المفوضة والسلطات المحلية للمشاركة في هذه التدريبات، وفق ما يكون ملائما. ومن خلال إجراء المسح الآلي، سنضمن أن لدينا دراية أفضل بوضع أمن شبكة الإنترنت الحكومية.

6-3-5 أمن المعلوماتية ليس مرتبطا بالتكنولوجيا فقط. فتقريبا كافة الهجمات الإلكترونية الناجحة كان فيها عنصر بشري مساعد. لذلك سنستمر في الاستثمار بالأفراد لنضمن أن كل من يعمل في الحكومة لديه وعي كافٍ بالمخاطر الإلكترونية. وسنطور خبرات إلكترونية محددة في المجالات التي تكون درجة المخاطر فيها مرتفعة، وسنتأكد من أننا نطبق الإجراءات المناسبة لإدارة هذه المخاطر بشكل فعال.

7-3-5 سيطور المركز الوطني لأمن المعلوماتية إرشادات رائدة عالميا بشأن أمن المعلوماتية تواكب التهديدات وتَطور التقنيات الجديدة. وسنتخذ الخطوات اللازمة لضمان أن تتوفر لمؤسسات الحكومة بسهولة معلومات عن التهديدات لتستند إليها في فهمها للمخاطر الإلكترونية الخاصة بها وتتخذ الإجراءات الصحيحة.

8-3-5 سنواصل تحسين شبكاتنا الأكثر سرية لحماية اتصالات الحكومة الأكثر حساسية.

9-3-5 تمثل أنظمة الصحة والرعاية تحديات فريدة في مجال أمن المعلوماتية. إذ يعمل في هذا القطاع نحو 1.6 مليون شخص في أكثر من 40,000 مؤسسة، ولدى كل منها قدرات وموارد متباينة جدا حول أمن المعلومات. وقد وضعت مؤسسة حماية البيانات الوطنية لشؤون الصحة والرعاية معايير جديدة لحماية بيانات أنظمة الصحة والرعاية الاجتماعية في إنجلترا، إلى جانب نموذج يتطلب من المرضى أن يعلنوا إن كانوا يوافقون على التصريح ببياناتهم أم لا. وستعمل الحكومة مع مؤسسات الصحة والرعاية الاجتماعية لتطبيق تلك المعايير.

"بريطانيا رائدة عالميا في مجال أمن المعلوماتية. ولكن مع تزايد التهديدات، فإن مركز عمليات أمن المعلوماتية هذا سيكفل أن تستمر قواتنا المسلحة في العمل بأمان. وإن ميزانيتنا الدفاعية المتزايدة تعني أن بإمكاننا أن نكون متقدمين على أعدائنا في الفضاء الإلكتروني، فيما نحن ماضين بالاستثمار في القدرات التقليدية."

مايكل فالون، عضو البرلمان ووزير الدفاع، إبريل 2016.

10-3-5 أمن المعلوماتية بالغ الأهمية لدفاعنا. إذ تعتمد قواتنا المسلحة على أنظمة المعلومات والاتصالات، سواء داخل المملكة أم في عملياتها بمختلف أرجاء العالم. لذلك فإن البنية التحتية لوزارة الدفاع، وكذلك العاملين فيها، أهداف بارزة. كما تُستَهدف أنظمة الدفاع بشكل دوري من جانب مجرمي الإنترنت، وأجهزة الاستخبارات الأجنبية، وأطراف أخرى خبيثة، إذ يسعى جميعهم لاستغلال العاملين، وتعطيل سير العمل والعمليات، وإفساد المعلومات وسرقتها. وعليه، سوف نرفع درجة الوعي بالتهديدات الإلكترونية، وقدرات كشفها وآليات الرد عليها، وذلك بتطوير "مركز عمليات أمن المعلوماتية" الذي يستخدم قدرات دفاعية إلكترونية متطورة لحماية الفضاء الإلكتروني لوزارة الدفاع وللتعامل مع التهديدات. وسيعمل هذا المركز بشكل وثيق مع المركز الوطني لأمن المعلوماتية لمواجهة التحديات بالنسبة للأمن الإلكتروني لوزارة الدفاع، وللمساهمة في حماية أمن المعلوماتية الوطني بصورة أعم.

قياس النجاح

11-3-5 سوف تقيس الحكومة مدى نجاحها في حماية شبكاتها وأنظمتها وبياناتها عن طريق تقييم التقدم الحاصل نحو تحقيق كل من الغايات التالية:

- أن يكون لدى الحكومة فهم متعمق لمستوى المخاطر على أمن المعلوماتية في كافة إدارات الحكومة والقطاع العام بصورة أشمل؛
- أن تعمل كل إدارة من إدارات الحكومة والمؤسسات الأخرى على حماية نفسها بما يوازي مستوى المخاطر لديها وفقا لمعيار الحد الأدنى المتفق عليه في الحكومة؛
- أن تكون إدارات الحكومة والقطاع العام بصورة أشمل قادرة على الصمود في وجه الاعتداءات، وأن تستطيع الرد بفاعلية على الحوادث الإلكترونية بينما تواصل مهامها وتتعافى بسرعة؛
- أن تكون التكنولوجيات والخدمات الرقمية الجديدة التي تستخدمها الحكومة محمية إلكترونيا بشكل افتراضي؛
- أن نكون مدركين لكافة نقاط الضعف المعروفة عبر الإنترنت في أنظمة الحكومة وخدماتها، وأن نعمل بدأب لتخفيف وقعها؛
- أن يلتزم كافة الموردين للحكومة بمعايير أمن المعلوماتية السليمة.

4-5 حماية بنيتنا التحتية الحيوية وغيرها من القطاعات ذات الأولوية

السياق

1-4-5 إن أمن المعلوماتية لبعض المؤسسات الأمنية في المملكة المتحدة له أهمية خاصة، ذلك لأن أي هجوم إلكتروني ناجح عليها سيكون له أشد العواقب على الأمن القومي للبلاد. ويمكن لتلك العواقب أن تُؤثر على حياة المواطنين البريطانيين، أو على استقرار ومتانة اقتصاد البلاد، أو على مكانة المملكة المتحدة وسمعتها دوليا. وهذه المجموعة من المؤسسات والشركات الهامة في القطاعين العام والخاص تشمل البنية التحتية الحيوية التي توفر الخدمات الأساسية للبلاد ككل. لذا، فإن ضمان بقاء تلك البنية التحتية محمية وصامدة في وجه الاعتداءات الإلكترونية سيكون من أولويات الحكومة. وهذه المجموعة الهامة تضم أيضا شركات ومؤسسات أخرى، أوسع من البنية التحتية الحيوية، تتطلب مستوى أعلى من الدعم، ومن ضمنها:

- أكثر الشركات نجاحا في المملكة المتحدة والتي تعتبر جواهر التاج الاقتصادي، وكذلك الشركات التي بيدها قوَّتنا الاقتصادية مستقبلا من حيث قيمة أبحاثها وممتلكاتها الفكرية؛
- المؤسسات التي تختزن البيانات - ولا يقتصر ذلك على المؤسسات التي بحوزتها كميات ضخمة من البيانات الشخصية، بل تشمل أيضا تلك التي تحتفظ ببيانات عن مواطنين معرضين للخطر هنا وفي الخارج، كالمنظمات الخيرية؛
- الأهداف الأكثر عرضة للتهديد - كالمؤسسات الإعلامية، والتي قد يسبب الاعتداء عليها ضررا بسمعة المملكة المتحدة، أو يقوض ثقة الناس بالحكومة، أو يُعرّض حرية التعبير للخطر؛
- الأركان الرئيسية التي تعتمد عليها مصداقية اقتصادنا الرقمي - أي مقدمي الخدمات الرقمية الذين يمَكّنون تجارتنا الإلكترونية واقتصادنا الرقمي، والذين يعتمدون على ثقة المستهلك بخدماتهم؛
- المؤسسات التي تستطيع، من خلال قِوى السوق

وسلطتها، أن تمارس تأثيرها على الاقتصاد بأكمله لتحسين أمنها الإلكتروني، ومن بينها شركات

2-4-5 هناك الكثير مما يتوجب فعله لحماية تلك الأركان الحيوية من اقتصادنا، ولدعم المؤسسات التي لها تأثير قوي على الآخرين. فلا تزال بنيتنا التحتية الحيوية - في كلا القطاعين العام والخاص - هدفا للهجمات. وفي تلك البنية والكثير غيرها من القطاعات ذات الأولوية لا يزال خطر الهجوم الإلكتروني غير مفهوم كما ينبغي، أو لا تتم إدارته بشكل صحيح، حتى في الوقت الذي تتنوع فيه المخاطر وتزداد.

الهدف

3-4-5 ستعمل الحكومة البريطانية، بالتعاون مع الحكومات المفوضة والسلطات المسؤولة الأخرى، حيثما يكون ذلك ملائما، على ضمان الحماية الوافية للمؤسسات والشركات الأكثر أهمية في المملكة المتحدة، وأن تكون قادرة على الصمود إزاء الهجمات الإلكترونية. ولكن لا الحكومة ولا غيرها من أجهزة القطاع العام سوف تضطلع بمسؤولية إدارة تلك المخاطر للقطاع الخاص، حيث يبقى ذلك من مهام مجالس إدارات الشركات ومُلّاكها ومن يُشغّلها. إلا أن الحكومة ستوفر الدعم والضمان بما يتماشى مع كل من حجم التهديد الذي تواجهه تلك المؤسسات والشركات وعواقب تعرضها للهجوم فعليا.

"إن أمن المعلوماتية أساسي لفتح الآفاق أمام الابتكار والتوسع. وبتبني المؤسسات لمقاربة تناسبها وتركز على مخاطر أمن المعلوماتية فيها، تستطيع أن تُحوّل اهتمامها إلى الفرص والاكتشافات. إن بناء الثقة بشركة تعمل بنجاح ضمن "إنترنت الاشياء"، وتدعم الأفراد بالكامل وتحميهم وتحمي أجهزتهم النقالة (من الهاتف العادي إلى جهاز العناية الطبية، ومن الأجهزة الذكية إلى السيارات الذكية)، يعتبر عاملا تنافسيا فارقا ويجب أن يكون من الأولويات".

مسح أجرته شركة إيرنست آند يونغ عام 2015 عن أمن المعلوماتية العالمي

مقاربتنا

4-4-5 إن مجالس إدارة المؤسسات والشركات مسؤولة عن ضمان أمن شبكاتها. فعليهم أن يحددوا الأنظمة

التأمين وشركات الاستثمار والجهات التنظيمية والشركات الاستشارية المتخصصة.

الحساسة وأن يُقيموا بشكل دوري نقاط الضعف فيها على ضوء التهديدات والبيئة التكنولوجية الآخذة في التطور. ولا بد لهم أن يستثمروا في التكنولوجيا وفي موظفيهم لتقليل نقاط الضعف في الأنظمة الحالية والمستقبلية، وكذلك في سلسلة التوريد، من أجل الحفاظ على مستوى من أمن المعلوماتية يتناسب مع المخاطر. كما ينبغي أن تتوفر لديهم في مؤسساتهم قدرات مُجرّبة للاستجابة في حال وقوع هجوم. أما بشأن البنية التحتية الوطنية الحيوية، فعليهم أن يفعلوا ذلك مع المؤسسات الحكومية والجهات التنظيمية، بحيث نكون نحن على ثقة من أن الخطر الإلكتروني يُدار بالشكل الصحيح، وإن لم يكن كذلك فإننا سنتدخل من أجل مصلحة الأمن القومي.

5-4-5 لذلك، ستعمل الحكومة على فهم أمن المعلوماتية في كافة أنحاء بنيتنا التحتية الحيوية، وستكون لديها تدابير للتدخل، حيثما لزم الأمر، لإدخال التحسينات التي تخدم المصلحة الوطنية.

6-4-5 ستقوم الحكومة بما يلي:

- مشاركة المعلومات عن التهديدات، خصوصا المعلومات التي يمكن للحكومة فقط الحصول عليها، مع قطاع المعلوماتية كي يعرفوا ما عليهم أن يحموا أنفسهم منه؛
- تقديم المشورة والإرشادات عن كيفية إدارة المخاطر الإلكترونية، وتحديد ماهية أمن المعلوماتية الجيد، وذلك بالعمل المشترك مع قطاع المعلوماتية والمؤسسات الأكاديمية.
- تشجيع إدخال أحدث أنواع التكنولوجيا الأمنية اللازمة لحماية البنية التحتية الحيوية، مثل مرافق التدريب ومختبرات التجارب، والمعايير الأمنية، والخدمات الاستشارية؛
- إجراء تمارين بالاشتراك مع شركات البنية التحتية الحيوية لمساعدتها على إدارة مخاطرها الإلكترونية ونقاط ضعفها.

7-4-5 سيوفر المركز الوطني لأمن المعلوماتية هذه الخدمات للشركات والمؤسسات الأكثر أهمية في المملكة المتحدة، بما في ذلك البنية التحتية الحيوية. وسيفعل ذلك بالشراكة مع الإدارات والجهات التنظيمية، والتي سوف تتحقق فيما إذا كانت المخاطر الإلكترونية في قطاعاتها تدار بالمستوى الذي تتطلبه المصلحة الوطنية أم لا.

8-4-5 كما ستضمن الحكومة وجود الإطار التنظيمي المناسب للأمن الإلكتروني. وذلك الإطار سوف:

- يضمن أن قطاع المعلوماتية سوف يعمل لحماية نفسه من التهديدات؛
- يكون تركيزه مُنصباً على النتائج، وأن يكون مرنا بالشكل الكافي بحيث لا يتخلف عن التهديدات، أو أن يؤدي فقط إلى الامتثال للقواعد وليس إلى الإدارة الحكيمة للمخاطر؛
- يكون مرنا بما يكفي كي يعزز النمو والابتكار لا أن يكون في طليعته؛
- يكون متناسقا مع الأنظمة المتبعة في دول أخرى بحيث لا تعاني الشركات البريطانية نتيجة مقاربة غير متماسكة وتشكل عبئا عليها؛
- يقدم مزايا تنافسية للمملكة المتحدة، بدعم فعال من الحكومة.

9-4-5 تم بالفعل تنظيم الكثير من قطاعاتنا الصناعية من ناحية أمن المعلوماتية. ورغم ذلك، لا بد لنا أن نضمن اتخاذ الإجراءات الصحيحة في الاقتصاد ككل، بما في ذلك البنية التحتية الحيوية، من أجل إدارة مخاطر أمن المعلوماتية.

قياس النجاح

10-4-5 ستقيس الحكومة مدى نجاحها في حماية بنيتنا التحتية الحيوية وغيرها من القطاعات ذات الأولوية عن طريق تقييم ما حققته من تقدم تجاه النتائج التالية:

- أن نكون مدركين لمستوى أمن المعلوماتية في كافة أرجاء البنية التحتية الحيوية، وأن تتوفر لدينا إجراءات للتدخل، عند الضرورة، لإدخال تحسينات لخدمة المصلحة الوطنية؛
- وأن تتفهم مؤسساتنا وشركاتنا الأكثر أهمية مستوى المخاطر، وأن تطبق ما يتناسب معها من ممارسات أمن المعلوماتية.

5-5 تغيير سلوكيات الأفراد والشركات

1-5-5 يعتمد الاقتصاد البريطاني الرقمي الناجح على ثقة الشركات والأفراد بخدمات الإنترنت. وقد عملت الحكومة البريطانية مع قطاع المعلوماتية والمكونات الأخرى للقطاع العام لزيادة الوعي بالتهديدات وفهمها. كما وفرت الحكومة للأفراد والشركات الأدوات التي يحتاجونها لحماية أنفسهم. وفي حين أن هناك مؤسسات كثيرة أداؤها ممتاز - وبعضها على مستوى عالمي - في حماية نفسها وفي توفير الخدمات للآخرين عبر الإنترنت، فإن غالبية الشركات والأفراد ما زالوا لا يديرون المخاطر الإلكترونية كما ينبغي.

"في العام الماضي، بلغ متوسط تكلفة الاختراقات التي تعرضت لها الشركات الكبرى 36,500 مليون جنيه استرليني. أما بالنسبة للشركات الصغيرة فقد بلغ متوسط تكلفة الاختراقات 3,100 جنيه. وكانت 65% من الشركات الكبرى قد أبلغت عن تعرضها لاختراق أمن المعلومات في العام الماضي، بينما أفادت نسبة 25% من تلك الشركات أنها تعرضت لاختراقات مرة واحدة في الشهر على الأقل. وحوالي سبع من كل عشر هجمات تضمنت استخدام الفيروسات وبرامج التجسس أو برامج ضارة، والتي كان يمكن منعها لو أن الشركات استعانت بخطة الحكومة لأساسيات الإنترنت".

الاستقصاء الحكومي لعام 2016 حول فحص الصحة الإلكترونية اختراقات أمن المعلوماتية

الهدف

2-5-5 هدفنا هو ضمان أن الأفراد والمؤسسات، بصرف النظر عن حجمها أو القطاع الي تعمل به، يتخذون الخطوات المناسبة لحماية أنفسهم وعملائهم من الضرر الذي تسببه الهجمات الإلكترونية.

مقاربتنا

3-5-5 ستقدم الحكومة المشورة التي يحتاجها الاقتصاد لحماية نفسه. ونحن سنحسن طريقة تقديم تلك المشورة لتحقيق الفائدة القصوى منها. أما بالنسبة للأفراد، فإن الحكومة ستسخّر "الأصوات الموثوقة" من أجل توسيع انتشار رسالتنا ومصداقيتها وملاءمتها. وسنقدم مشورة يسهل اتباعها وتكون ملائمة للأفراد حين يدخلون على الخدمات الإلكترونية ويعرضون أنفسهم للخطر. وسوف نعمل مع الحكومات المفوضة والهيئات الأخرى على النحو المناسب.

4-5-5 بالنسبة للشركات، سنعمل من خلال مؤسسات مثل شركات التأمين والجهات التنظيمية وشركات الاستثمار التي يمكنها أن تمارس ضغطا على الشركات لضمان أنها تدير المخاطر. وبقيامنا بذلك، سوف نلقي الضوء على الفوائد التجارية الواضحة وتكلفة المخاطر الإلكترونية حسب تقييم القوى المؤثرة في السوق. وسوف نحاول أن نفهم بشكل أفضل لماذا لا تزال شركات كثيرة تعجز عن حماية نفسها بشكل كاف، ومن ثم سنعمل بالشراكة مع مؤسسات مثل الجهات التي تضع المعايير المهنية لكي ننتقل لأبعد من زيادة الوعي وصولا إلى إقناع الشركات باتخاذ التدابير اللازمة. وسوف نضمن أيضا أن يكون لدينا الإطار التنظيمي الصحيح لإدارة المخاطر الإلكترونية التي يفشل السوق بمعالجتها. وفي سياق ذلك، سنسعى إلى استخدام عوامل مساعدة مثل "القاعدة العامة لحماية البيانات" (GDPR) لرفع معايير أمن المعلوماتية وحماية المواطنين.

5-5-5 سوف تتوفر للأفراد والمؤسسات في المملكة المتحدة المعلومات والمعرفة والأدوات التي يحتاجونها لحماية أنفسهم. ولضمان أننا سنُحدث تغييرا كبيرا في سلوك المواطنين، ستكون لدينا مجموعة من الرسائل المترابطة والمستمرة بشأن إرشادات أمن المعلوماتية تُرسل من طرف الحكومة وشركائنا. وسيوفر المركز الوطني لأمن المعلوماتية المشورة الفنية لمساندة ذلك الإرشاد، والتي ستعكس أولويات وممارسات الشركات والأفراد، وستكون واضحة ومتاحة للجميع ومتسقة، كما ستكون في نفس الوقت مواكبة للتهديدات. أما الأجهزة الأمنية، فستعمل بشكل وثيق مع قطاع المعلوماتية والمركز الوطني لأمن المعلوماتية لتبادل آخر المعلومات الاستخباراتية بخصوص التهديدات الإجرامية، ولدعم قطاع المعلوماتية في حماية نفسه من التهديدات، ولتخفيف وقع الاعتداءات على الضحايا في المملكة المتحدة.

قياس النجاح

6-5-5 ستقيس الحكومة مدى نجاحها في حماية بنيتنا التحتية الحيوية وغيرها من القطاعات ذات الأولوية عن طريق تقييم التقدم الحاصل نحو تحقيق النتائج التالية:

- أن يصبح مستوى أمن المعلوماتية في اقتصاد المملكة المتحدة يماثل، أو يفوق، ما هو عليه في الاقتصادات المنافسة المتقدمة؛
- أن ينخفض عدد وشدة وتأثير الاعتداءات الإلكترونية الناجحة ضد الشركات في المملكة المتحدة بسبب تحسن معايير الإجراءات الوقائية الإلكترونية؛
- أن يكون هناك تحسن في ثقافة أمن المعلوماتية في أنحاء المملكة المتحدة بحيث تدرك المؤسسات والأفراد مستويات تعرضهم للمخاطر الإلكترونية، ويعرفون خطوات الإجراءات الوقائية الإلكترونية التي يجب أن يتخذوها لإدارة تلك المخاطر.

التوعية الإلكترونية

إن حملة التوعية الإلكترونية، المعروفة سابقا باسم Cyber Streetwise، تقدم المشورة التي يحتاجوها المواطنون لحماية أنفسهم من مجرمي الإنترنت. وستعمل الرسائل الموجهة التي تُنشر عبر وسائل التواصل الاجتماعي والإعلانات، وبالتعاون مع الشركات، على الترويج للنصيحتين التاليتين:

- استخدام ثلاث كلمات منتقاة عشوائيا للخروج بكلمة مرور قوية؛
- والحرص دائما على تنزيل آخر تحديثات البرامج.

يتفق الخبراء على أن اتباع هذه السلوكيات سيوفر للشركات الصغيرة والأفراد الحماية ضد الجرائم الإلكترونية. وتلقى حملة التوعية الإلكترونية الدعم حاليا من 128 شريكا من مختلف القطاعات، بما فيها الشرطة وشركات مبيعات التجزئة والترفيه والسفر وقطاعات الخدمات المهنية. وفي سنة 2016/2015 أفاد حوالي 10 ملايين شخص بالغ ومليون شركة صغيرة إلى أنهم باتوا أكثر استعدادا لاتباع سلوكيات أمن المعلوماتية الأساسية أو الحفاظ عليها كنتيجة لحملة التوعية الإلكترونية.

لمزيد من المعلومات يرجى زيارة الموقع التالي www.cyberaware.gov.uk

أساسيات الفضاء الإلكتروني

وُضعت خطة أساسيات الفضاء الإلكتروني لكي تشرح للمؤسسات كيف تحمي نفسها من "التهديدات التجارية" منخفضة المستوى. إذ تعرض الخطة خمسة ضوابط فنية ينبغي على المؤسسات أن تلتزم بها (التحكم بالدخول؛ وجدران الحماية وبوابات الإنترنت؛ والحماية من البرامج الضارة؛ إدارة تصحيح البرامج (patching)؛ والتكوين الآمن). إن الغالبية العظمى من الاعتداءات الإلكترونية تستخدم أساليب بسيطة نسبيا تستغل نقاط الضعف الأساسية في البرامج وأجهزة الكومبيوتر. وهناك أدوات وتقنيات متوفرة علناً عبر الإنترنت من شأنها أن تُمكّن حتى الأطراف التي تفتقر إلى المهارات من استغلال نقاط الضعف تلك. وإن تطبيق خطة الأساسيات الإلكترونية كفيل بالوقاية من الغالبية العظمى من التهديدات الإلكترونية الشائعة.

5-6 إدارة الحوادث وفهم التهديدات

1-6-5 من المرجح أن تزداد أعداد وشدة الحوادث الإلكترونية التي تصيب المؤسسات في كل من القطاعين العام والخاص. وبالتالي، علينا أن نعرف كيف سيتعامل القطاع الخاص والمواطنون مع الحكومة لدى وقوع حادث إلكتروني. وسنعمل لضمان أن يكون مستوى الدعم الذي تقدمه الحكومة البريطانية لكل من القطاعين محددا ومفهوما بشكل واضح - مع الأخذ بعين الاعتبار مدى النضج الإلكتروني. وإن جمع الحكومة للمعلومات عن التهديد وتوزيعها يجب أن يتم بالأسلوب والسرعة الملائمين لكافة أنواع المؤسسات. في الوقت الحالي، يستطيع القطاع الخاص والحكومة والمواطنون الاطلاع على مصادر عديدة للمعلومات والإرشادات والمساعدة بخصوص أمن المعلوماتية. لا بد من تبسيط تلك العملية.

2-6-5 علينا أن نضمن أن ما تقدمه الحكومة، إن كان ذلك استجابة للحوادث أو لتقديم الإرشاد، ليس بمعزل عن القطاع الخاص، بل بالمشاركة معه. ولا بد لعمليات إدارة الحوادث لدينا أن تعكس مقاربة شاملة للحوادث، بحيث نتعلم من شركائنا ونتشارك معهم أساليب تخفيف الآثار. كذلك سنستمر باستخدام علاقاتنا مع الفرق الوطنية للاستجابة لطوارئ الكومبيوتر ومع حلفائنا كجزء من مهامنا في إدارة الحوادث.

3-6-5 تبقى إدارة الحوادث مجزأة على امتداد الإدارات الحكومية في الوقت الحالي، إلا أن هذه الاستراتيجية ستنشئ مقاربة موحدة. وسوف يوفر المركز الوطني لأمن المعلوماتية جهود استجابة فعالة وسريعة بقيادة الحكومة لدى وقوع حوادث إلكترونية. وفي حال وقوع حادث إلكتروني خطير، سوف نعمل لضمان أن القوات المسلحة قادرة على تقديم المساعدة، سواء بالشكل التقليدي للتعامل مع التأثير المادي للحادث، أو على شكل دعم من جانب خبراء الإنترنت النظاميين أو الاحتياط. وفي حين أننا سنقدم كل المساندة التي تسمح بها مواردنا، تستمر الحكومة في تأكيد أهمية أن يعمل قطاع المعلوماتية والمجتمع والأفراد على حماية أمنهم الإلكتروني الأساسي.

الهدف

4-6-5 أهدافنا هي التالية:

- أن يكون لدى الحكومة مقاربة واحدة مترابطة لإدارة الحوادث، تقوم على فهم أفضل للتهديدات ووعي لها، وللأعمال المعادية المتخذة ضدنا. وسيكون المركز الوطني لأمن المعلوماتية أحد العوامل الرئيسية المساعدة في ذلك، كما هي الحال أيضا بالنسبة للشراكة مع القطاع الخاص وأجهزة تنفيذ القانون والإدارات والهيئات والأجهزة الحكومية الأخرى.
- أن يحدد المركز الوطني لأمن المعلوماتية خطوات واضحة من أجل الإبلاغ عن الحوادث تكون مصممة بناء على مواصفات الضحية.
- أن نتمكن من منع وقوع الحوادث الإلكترونية الأكثر شيوعا، وأن توجد لدينا آليات فعالة لتقاسم المعلومات التي تستند إليها خطط "ما قبل وقوع الحادث".

مقاربتنا

5-6-5 يقع على عاتق إدارة المؤسسة والشركة، في كل من القطاعين العام والخاص، ضمان أن شبكاتها آمنة، وأن تتدرب على خطط الاستجابة للحوادث. وفي حال وقوع حادث كبير، فإن إدارة الحكومة للحادث سوف تعكس العوامل الثلاثة المميزة للحادث الإلكتروني: المُسببات التي أدت لوقوع الحادث، والحادث نفسه، والاستجابة بعد الحادث.

6-6-5 ولتقديم إدارة حوادث فعالة لكل من الحكومة والقطاع الخاص، سنعمل عن كثب لمراجعة وتحديد نطاق الرد الحكومي لضمان أنه يعزز التعاون. وسوف نعتمد على خطتنا الوطنية للتدريب الإلكتروني، مستعينين بفهمنا ووعينا الأفضل للتهديدات، لكي نُحسّن ما نقدمه من دعم لشركائنا في القطاعين العام والخاص.

7-6-5 سوف ننشئ كيانا حكوميا موثوقا به ويمكن الاعتماد عليه لتقديم المشورة والمساعدة والضمان بشأن الحوادث. وذلك سوف يرفع من درجة الوعي بأمن المعلوماتية في أنحاء المجتمع الرقمي في المملكة المتحدة، وسيمكننا من التعرف على التوجهات بشكل أفضل، وأن نتخذ إجراءات استباقية ونمنع وقوع الحوادث في نهاية المطاف.

8-6-5 ومع توجهنا نحو التقاسم الآلي للمعلومات (أي أن تقوم أنظمة أمن المعلوماتية بتنبيه بعضها البعض تلقائيا بشأن الحوادث والاعتداءات)، سنقدم خدمة أكثر فعالية. وهذا ما سيسمح للمؤسسات أن تتحرك بسرعة بناء على المعلومات ذات الصلة بالتهديد.

قياس النجاح

9-6-5 ستقيس الحكومة مدى نجاحها بإدارة الحوادث من خلال تقييم التقدم الذي تم إحرازه نحو تحقيق الغايات التالية:

- ارتفاع في نسبة إبلاغ السلطات عن الحوادث، الأمر الذي يؤدي إلى فهم أفضل لحجم ومستوى التهديد؛
- إدارة الحوادث بفعالية وكفاءة أفضل وبشكل شامل نتيجة لإنشاء المركز الوطني لأمن المعلوماتية كآلية مركزية للإبلاغ عن الحوادث والاستجابة لها؛
- معالجة الأسباب الجذرية للاعتداءات على المستوى الوطني، ما يقلل من حدوث الاستغلال المتكرر للعديد من الضحايا والقطاعات.

6 الردع

1-0-6 تنص استراتيجية الأمن الوطني على أن الدفاع والحماية يبدآن بالردع. ويصح ذلك في الفضاء الإلكتروني كما في أي مجال آخر. ولتحقيق رؤيتنا كبلد آمن وصامد في وجه التهديدات الإلكترونية، ومزدهر وواثق في العالم الرقمي، علينا أن نثبط عزيمة أولئك الذين يسعون لإلحاق الضرر بنا وبمصالحنا وأن نردعهم. ولتحقيق ذلك، علينا جميعا أن نستمر في رفع مستويات أمن المعلوماتية لجعل الاعتداء علينا في الفضاء الإلكتروني - سواء للسرقة منا أو الإضرار بنا - لا يكون رخيص التكلفة ولا سهلا. ينبغي أن يعرف أعداؤنا أنه ليس بإمكانهم تنفيذ هجماتهم دون مساءلة: وأن بإمكاننا كشفهم وسوف نفعل ذلك، وأننا نستطيع اتخاذ إجراء ضدهم مستخدمين أكثر الردود ملاءمة من ضمن كافة الأدوات المتاحة لنا. وسوف نستمر في بناء التحالفات العالمية، وفي الدعوة لتطبيق القانون الدولي في الفضاء الإلكتروني. كما سنعمل بجد على إحباط نشاط كل من يهددوننا في الفضاء الإلكتروني، وعلى تعطيل البنية التحتية التي يعتمدون عليها. وتحقيق هذا الطموح يتطلب قدرات سيادية عالمية المستوى.

1-6 دور الإنترنت في الردع

1-1-6 الفضاء الإلكتروني هو مجرد أحد المجالات التي علينا أن ندافع عن مصالحنا وسيادتنا فيه. ومثلما أن أنشطتنا في المجال المادي لها صلة بأمن المعلوماتية لدينا وبالردع، فكذلك لا بد لأعمالنا ومواقفنا في الفضاء الإلكتروني من أن تسهم في أمننا القومي الأعم.

2-1-6 إن مبادئ الردع قابلة للتطبيق في الفضاء الإلكتروني كما هي عليه في المجال المادي. ولا تدع المملكة المتحدة مجالا للشك بأننا سوف نستعين بكافة قدراتنا لردع الأعداء ولحرمانهم من فرص الاعتداء علينا. إلا أننا ندرك أن أمن المعلوماتية والقدرة على الصمود هما بذاتهما وسيلة لردع الاعتداءات التي تعتمد على استغلال نقاط الضعف.

3-1-6 سنتبع مقاربة وطنية شاملة بشأن أمن المعلوماتية والردع ليجعل المملكة المتحدة هدفا أكثر صعوبة، مع تقليل الفوائد للأعداء ورفع التكلفة التي سيتكبدونها - سواء أكانوا أعداءً سياسيين أم ديبلوماسيين أم اقتصاديين أم استراتيجيين. وينبغي علينا ضمان أن أعداءنا المحتملين يدركون قدرتنا على الرد وتصميمنا عليه، لكي يؤثر ذلك على قرارهم. وستكون لدينا الأدوات والقدرات التي نحتاجها: لنحرم أعداءنا من الفرص السهلة للإضرار بشبكاتنا وأنظمتنا، ولكي نفهم نواياهم وقدراتهم، ولنحبط تهديدات البرامج التجارية الضارة على نطاق واسع، وللاستجابة وحماية البلد في الفضاء الإلكتروني.

2-6 تقليل الجرائم الإلكترونية

1-2-6 يتوجب علينا أن نجعل الأنشطة الإلكترونية الإجرامية أكبر تكلفة وخطرا على مرتكبيها وأقل مردودا لهم. وفي حين أن علينا أن نُقوّي المملكة المتحدة في وجه الاعتداءات الإلكترونية وأن نقلل من نقاط الضعف، فلا بد لنا أيضا من ألا نتوانى في التركيز على تعقب المجرمين الذين ما زالوا يستهدفون المملكة المتحدة.

2-2-6 ستركز الأجهزة الأمنية جهودها على تعقب المجرمين الذين لا ينفكون عن مهاجمة مواطني المملكة المتحدة وشركاتها. وسنعمل مع شركاء محليين ودوليين لاستهداف المجرمين أيا كان موقعهم، ولنفكك بنيتهم التحتية والشبكات التي تسهل نشاطهم. كما ستستمر أجهزة الأمن في المساعدة على نشر التوعية ومعايير أمن المعلوماتية بالتعاون مع المركز الوطني لحماية المعلوماتية.

3-2-6 إن هذه الاستراتيجية تُكمل "استراتيجية الجرائم الخطيرة والمنظمة لعام 2013" التي قدمت تصوراً للرد الاستراتيجي للحكومة البريطانية على الجريمة الإلكترونية، إلى جانب الأشكال الأخرى من الجريمة الخطيرة والمنظمة. وقد تم إنشاء "الوحدة الوطنية لمكافحة الجريمة الإلكترونية" (NCCU) ضمن "الوكالة الوطنية لمكافحة الجريمة" كي تتولى قيادة وتنسيق الاستجابة الوطنية للجريمة الإلكترونية. ويعتبر مركز مكافحة الاحتيال مركزا وطنيا للتبليغ عن الاحتيال والجرائم الإلكترونية. وتوفر شبكة من وحدات الجريمة الإلكترونية، وهي جزء من "الوحدات الإقليمية لمكافحة الجريمة المنظمة" (ROCU) قدرات إلكترونية متخصصة على المستوى الإقليمي لدعم الوحدة الوطنية لمكافحة الجريمة الإلكترونية والقوى المحلية.

الهدف

4-2-6 سوف نخفض من تأثير الجريمة الإلكترونية على المملكة المتحدة ومصالحها عن طريق ردع مجرمي الإنترنت عن استهداف المملكة، والعمل دون هوادة على ملاحقة الذين يواظبون على مهاجمتنا.

مقاربتنا

5-2-6 لتخفيف أثر الجرائم الإلكترونية، فإننا سوف:

- نعزز قدرات ومهارات الجهات الأمنية في المملكة المتحدة على المستويات الوطنية والإقليمية والمحلية من أجل كشف مجرمي الإنترنت وملاحقتهم ومحاكمتهم وردعهم داخل المملكة المتحدة وخارجها؛
- نعمل للوصول إلى فهم أفضل لنموذج عمل الجريمة الإلكترونية لكي نعرف أين نوّجه تدخلاتنا من أجل تعطيل أثر الأنشطة الإجرامية بالطريقة الأكثر فاعلية. وسوف نستخدم تلك المعرفة لتحقيق ما يلي:
  - جعل المملكة المتحدة بيئة عالية التكلفة وشديدة الخطورة لعمل المجرمين، وذلك عن طريق استهداف بؤر الجريمة ومن خلال العمل مع قطاع المعلوماتية لتقليل قدرة المجرمين على استغلال البنية التحتية في المملكة المتحدة؛
  - والتصدي للجريمة الإلكترونية في مراحلها الأولى، بالضغط على أسلوب عمل المجرمين من خلال تفكيك بنيتهم التحتية وشبكاتهم المالية، وتقديمهم للمحاكمة كلما أمكن ذلك.
- تنمية الشراكات الدولية لوضع حد للحصانة المُدركة لمجرمي الفضاء الإلكتروني الذين يعملون ضد المملكة المتحدة، وذلك لتقديم المجرمين للمحاكمة في الأنظمة القضائية للدول الأخرى؛
- ردع الأفراد عن الانجذاب إلى الجريمة الإلكترونية، أو الانخراط بها، من خلال تنمية إجراءاتنا للتدخل المبكر؛
- تعزيز التعاون مع قطاع المعلوماتية لتزويدهم بالمعلومات الاستخباراتية عن التهديدات وليزودونا هم بالمعلومات التي بحوزتهم عن المراحل الاولى للتهديد لمساعدتنا في جهودنا لعرقلته؛
- تطوير خدمة جديدة تعمل على مدار الساعة طيلة أيام الأسبوع من أجل الإبلاغ عن الحوادث وتقدير السرعة المطلوبة للاستجابة في مركز مكافحة الاحتيال المرتبط بالمركز الوطني لحماية المعلوماتية والوحدة الوطنية لمكافحة الجريمة الإلكترونية التابعة للوكالة الوطنية لمكافحة الجريمة، وكذلك في باقي أجهزة الأمن بصورة أعم، وذلك لتحسين الدعم المقدم لضحايا الجرائم الإلكترونية، وتوفير استجابة أسرع للجرائم التي يتم الإبلاغ عنها، ومشورة أمنية وقائية محسنة. وسيتم إنشاء نظام إبلاغ جديد لتقاسم المعلومات بأسرع وقت ممكن بين كافة الأجهزة الأمنية عن الجرائم والتهديدات الإلكترونية؛
- العمل مع المركز الوطني لحماية المعلوماتية والقطاع الخاص لتقليل نقاط الضعف في البنية التحتية للمملكة المتحدة التي يمكن أن يستغلها مجرمو الفضاء الإلكتروني على نطاق واسع؛
- العمل مع القطاع المالي لجعل المملكة المتحدة بيئة معادية بشكل أكبر بالنسبة لمن يسعون لبيع البيانات المسروقة، بما في ذلك من خلال تعطيل شبكاتهم.

قياس النجاح

6-2-6 ستقيس الحكومة مدى نجاحها في خفض الجريمة الإلكترونية من خلال تقييم التقدم الذي أحرزته تجاه تحقيق الغايات التالية:

- أن تكون لدينا قدرة أكبر على تعطيل اعتداءات مجرمي الإنترنت ضد المملكة المتحدة، إلى جانب ارتفاع أعداد حالات القبض على المجرمين وصدور الأحكام القضائية بحقهم، وتفكيك أعداد أكبر من الشبكات الإجرامية كنتيجة لتدخل الأجهزة الأمنية؛
- أن تكون لدينا قدرات أمنية مُحسّنة، بما في ذلك استطاعة ومهارات أكبر لأخصائيين مكرسين لهذا الغرض ورجال الأمن العاديين، وتعزيز القدرات الأمنية لدى شركائنا في الخارج؛
- أن تتحسن فعالية تدابير التدخل المبكر وأن يتسع نطاقه، ومن شأن ذلك أن يثبط همة المعتدين ويؤدي إلى إصلاحهم؛
- أن يكون هناك عدد أقل من الهجمات الإلكترونية منخفضة المستوى كنتيجة لجعل الوصول للخدمات الإجرامية الإلكترونية أكثر صعوبة وجعلها أقل فعالية.

كيف تتصرف إذا وقعت ضحية لجريمة إلكترونية

إذا كنت من عامة المواطنين وتعتقد أنك وقعت ضحية لجريمة إلكترونية أو لاحتيال عن طريق الإنترنت، عليك الاتصال بمركز مكافحة الاحتيال.

بإمكانك أن تبلغ عن الحادث في أي وقت، ليلا أو نهارا، باستخدام أداة الإبلاغ عن الاحتيال على الموقع الإلكتروني للمركز، أو أن تتصل بالرقم 0300 123 2040. لمزيد من المعلومات يرجى زيارة الموقع التالي:
www.actionfraud.police.uk

شرطة مدينة لندن هي التي تدير خدمة مكافحة الاحتيال.

3-6 التصدي للأطراف الخارجية المعادية

1-3-6 نحتاج لتوظيف كامل نطاق قدرات الحكومة للتصدي للتهديد الآتي من الأطراف الخارجية المعادية التي تهدد أمننا السياسي والاقتصادي والعسكري بشكل متزايد. والعمل مع شركائنا الدوليين سيكون عاملا أساسيا لنجاحنا، وسوف نركّز أكثر فأكثر على إشراكهم والعمل معهم للتصدي للتهديد. والكثير من هذا العمل سوف يكون في السر. وإن استثماراتنا في القدرات السيادية وفي شراكاتنا مع قطاع المعلوماتية والقطاع الخاص سوف تستمر في دعم قدرتنا على كشف ومراقبة وتحديد ماهية هذه الأنشطة المتغيرة باستمرار والمعادية لنا.

الهدف

2-3-6 ستكون لدينا استراتيجيات وسياسات وأولويات لكل عدو، وذلك لضمان اتباع مقاربة استباقية مبرمجة بشكل جيد وفعالة للتصدي للتهديد، ولتخفيض عدد وشدة الحوادث الإلكترونية في المستقبل.

مقاربتنا

3-3-6 لتخفيض التهديد الإلكتروني من الأطراف الخارجية المعادية، سوف نقوم بما يلي:

- تعزيز تطبيق القانون الدولي في الفضاء الإلكتروني، بالإضافة إلى الدعوة لتطبيق اتفاق الأعراف الطوعية غير الملزمة لتصرف الدولة المسؤول، وتطوير وتطبيق تدابير لبناء الثقة؛
- العمل مع الشركاء الدوليين، وخاصة من خلال جوانب الدفاع الجماعي، والأمن التعاوني، والردع المُحسَّن التي توفرها عضويتنا في الناتو؛
- تحديد كل من الخصائص العامة والفريدة لنشاط أعدائنا الإلكترونيين؛
- خلق واكتشاف كل الخيارات المتاحة من أجل ردع هذا التهديد والتصدي له، بالاعتماد على كامل قدرات الحكومة. وسنأخذ في الحسبان العوامل الأخرى ذات الصلة، بما في ذلك الاستراتيجيات الخاصة بكل بلد، والأولويات الإلكترونية الدولية، والجريمة الإلكترونية، وأهداف الازدهار؛
- استخدام الشبكات والعلاقات القائمة مع حلفائنا الدوليين الأساسيين لتقاسم المعلومات حول التهديدات الحالية وتلك التي في طور التكوين، بما يغني معلوماتنا وخبراتنا؛
- إشهار هويات إلكترونية محددة عندما نرى أن ذلك يخدم المصلحة الوطنية.

قياس النجاح

4-3-6 ستقيس الحكومة مدى نجاحها في التصدي للأعمال العدائية من جانب الأطراف الخارجية من خلال تقييم التقدم الذي تم إحرازه نحو تحقيق الغايات التالية:

- أن شبكات تقاسم المعلومات القوية التي أسسناها مع شركائنا الدوليين، والاتفاقيات الأعم متعددة الأطراف لدعم السلوكيات المسؤولة والقانونية للدول، تساهم بشكل كبير في تعزيز قدرتنا على فهم التهديد والاستجابة له بما يؤدي إلى حماية أفضل للمملكة المتحدة؛
- أن تصبح المملكة المتحدة هدفا عسيرا للأطراف المعادية الخارجية لدرجة تمنعها من العمل ضدنا، بفضل إجراءاتنا للردع والدفاع، إلى جانب استراتيجياتنا الخاصة بكل بلد.

4-6 منع الإرهاب

1-4-6 تبقى القدرة الفنية للإرهابيين محدودة حاليا، إلا أنهم مستمرون في التطلع إلى القيام بعمليات ضارة بشبكات الكومبيوتر ضد المملكة المتحدة، حيث الدعاية لهم وتعطيل عمل الشبكات من الأهداف الرئيسية لنشاطهم الإلكتروني. والحكومة سوف تكشف هؤلاء الإرهابيين وتمنعهم من استخدام الفضاء الإلكتروني لهذا الغرض. وذلك سوف نقلل إلى الحد الأدنى تأثيرهم ونمنع تطور قدرات الإرهابيين الإلكترونية التي يمكن أن تهدد شبكات المملكة المتحدة وأمنها القومي.

الهدف

2-4-6 تخفيف التهديد الإرهابي باستخدام الفضاء الإلكتروني، وذلك بكشف أطراف الإرهاب الإلكتروني وتعطيل عمل الارهابيين الذين لديهم القدرة، ويسعون لتطويرها، لتهديد الأمن القومي للمملكة المتحدة.

مقاربتنا

3-4-6 لضمان بقاء التهديد الذي يشكله الإرهاب عبر الفضاء الإلكتروني منخفضا، فإننا سوف نعمل لأجل:

- كشف تهديدات الإرهاب الإلكتروني ومعرفة الأطراف التي تسعى للقيام بعمليات ضارة بالشبكات ضد المملكة المتحدة وحلفائها؛
- التحقيق بشأن الناشطين بالإرهاب الإلكتروني وعرقلة عملهم لكي نمنعهم من استخدام القدرات الإلكترونية ضد المملكة المتحدة وحلفائها؛
- العمل بشكل وثيق مع شركائنا الدوليين لنتمكن من مواجهة تهديد الارهاب الإلكتروني بشكل أفضل.

قياس النجاح

4-4-6 ستقيس الحكومة مدى نجاحها في منع الإرهاب من خلال تقييم التقدم الحاصل نحو تحقيق الغايات التالية:

- التوصل إلى فهم كامل للخطر الذي يمثله الإرهاب الإلكتروني، من خلال كشف تهديدات الإرهاب الإلكتروني للمملكة المتحدة والتحقيق فيها؛
- مراقبة القدرات الإلكترونية الإرهابية عن كثب وتعطيلها بأقرب فرصة ممكنة، بهدف منع تنامي تلك القدرات الإرهابية على المدى الطويل.

5-6 تعزيز القدرات السيادية - الهجوم الإلكتروني

1-5-6 القدرات الإلكترونية الهجومية تنطوي على الاختراق المتعمد لأنظمة الخصم أو شبكاته بقصد إلحاق الضرر بها وتعطيلها وتدميرها. ويشكل الهجوم الإلكتروني جزءا من نطاق لقدرات التي سنطورها لردع الخصوم ولحرمانهم من الفرص للاعتداء علينا، سواء في الفضاء الإلكتروني أم في المجال المادي. ومن خلال "البرنامج الوطني للهجوم الإلكتروني" (NOCP)، لدينا قدرة مكرسة للعمل في الفضاء الإلكتروني، وسوف نُسخّر الموارد لتطوير تلك القدرة وتحسينها.

الهدف

2-5-6 سنسعى لضمان أن تتوفر تحت تصرفنا قدرات إلكترونية هجومية ملائمة يمكننا نشرها في الزمان والمكان الذي نختاره، لأغراض الردع والأمور العملياتية الأخرى، بما ينسجم مع القوانين الوطنية والدولية.

مقاربتنا

3-5-6 لكي ننجز ذلك، فإننا سنقوم بما يلي:

- الاستثمار في البرنامج الوطني للهجوم الإلكتروني - وهو الشراكة بين وزارة الدفاع والقيادة المركزية الحكومية للاتصالات، التي تُسخِّر مهارات ومواهب كلتا الجهتين من أجل توفير الأدوات والأساليب والمستلزمات المهنية المطلوبة؛
- تطوير قدرتنا على استخدام أدوات الهجوم الإلكتروني؛
- تطوير قدرة قواتنا المسلحة على نشر الإمكانات الإلكترونية الهجومية كجزء من عملياتها، فنعزز بذلك التأثير الإجمالي الذي يمكن أن نُحدثه من خلال العمل العسكري.

قياس النجاح

4-5-6 ستقيس الحكومة مدى نجاحها في خلق قدرات إلكترونية هجومية من خلال تقييم النجاح الذي تم إحرازه نحو تحقيق الغايات التالية:

- أن تصبح المملكة المتحدة رائدة على مستوى العالم في القدرات الإلكترونية الهجومية؛
- أن يتوفر في المملكة المتحدة مورد مستمر من المهارات والخبرات من أجل تطوير ونشر قدراتنا الإلكترونية الهجومية السيادية.

6-6 تعزيز القدرات السيادية - التشفير

1-6-6 إن القدرة على التشفير ضرورية لحماية أهم ما نمتلك من معلومات حساسة، ولاختيار الطريقة التي ننشر بها قواتنا المسلحة وباقي قدرات أمننا القومي. وللحفاظ على تلك القدرة، سنحتاج لمهارات وتقنيات القطاع الخاص التي تضمنها القيادة المركزية الحكومية للاتصالات. وسيتطلب ذلك على الأرجح أن يتم العمل داخل المملكة المتحدة على أيدي مواطنين بريطانيين لديهم التصريح الأمني المطلوب، وممن يعملون لدى شركات مستعدة لأن تكون صريحة تماما حين تبحث مع القيادة المركزية الحكومية للاتصالات في حيثيات التصاميم وأدوات التنفيذ. وتعمل وزارة الدفاع والقيادة المركزية الحكومية للاتصالات للتوصل إلى فهم صحيح للتأثيرات طويلة الأمد لتكلفة الحفاظ على مثل تلك القدرات التشفيرية السيادية، بناء على الظروف السائدة في السوق وبالتعاون مع الشركات القادرة حاليا على توفير مثل تلك الحلول.

الهدف

2-6-6 لدينا الثقة بأن المملكة المتحدة ستكون لها السيطرة السياسية دائما على قدرات التشفير تلك الحيوية بالنسبة لأمننا القومي، وبالتالي ستكون لدها الوسائل لحماية أسرارها.

مقاربتنا

3-6-6 سنختار الوسائل التي تتيح لنا أن نتقاسم المعلومات بفعالية مع حلفائنا، ونضمن أن تتوفر لنا المعلومات الموثوقة وأجهزة المعلومات، حينما وأينما يتطلب الأمر. إن القيادة المركزية الحكومية للمعلومات ووزارة الدفاع، من خلال العمل الوثيق مع الإدارات والوكالات الحكومية الأخرى، سوف يحددان معا المتطلبات السيادية وما هي الطريقة المثلى للإيفاء بتلك المتطلبات عندما يكون الموردون محليين بالضرورة. وسوف يتم تنفيذ ذلك من خلال إطار مشترك جديد لتحديد المتطلبات من أجل المزايا العملياتية وحرية الحركة.

قياس النجاح

4-6-6 ستقيس الحكومة مدى نجاحها في الحفاظ على قدرات التشفير من خلال تقييمها للتقدم الذي تم إحرازه نحو تحقيق الغاية التالية:

- أن تكون قدراتنا التشفيرية السيادية فعالة في حفظ أسرارنا وبياناتنا الحساسة في مأمن من انكشافها لغير المصرح لهم بذلك.

التشفير

التشفير (encryption) هو عملية تحويل البيانات أو المعلومات إلى رموز لمنع انكشافها لغير المصرح لهم.

والحكومة تفضّل التشفير. فهو حجر الأساس لاقتصاد قوي قائم على الإنترنت: حيث أنه يحافظ على أمن البيانات الشخصية والملكية الفكرية للناس، ويوفر تجارة إلكترونية آمنة.

ولكن مع استمرار تطور التكنولوجيا، علينا ضمان عدم وجود "أماكن آمنة" مضمونة للإرهابيين والمجرمين تمكنهم من العمل خارج سلطة القانون.

تريد الحكومة أن تتعاون مع قطاع المعلوماتية بينما التكنولوجيا آخذة في التطور لضمان أن الشرطة ووكالات المخابرات يمكنها الاطلاع على مضمون اتصالات الإرهابيين والمجرمين، وذلك ضمن إطار قانوني متين وإشراف واضح. والقانون الحالي يسمح باعتراض اتصالات المجرمين والإرهابيين عندما تتوفر مذكرة قضائية بذلك. وعلى الشركات واجب العمل بمقتضى تلك المذكرة، وأن تُطلع الهيئة الحكومية المعنية على الاتصالات المطلوبة. وعندما يتم تقديم المذكرة للشركة المعنية، يُطلب منها أن تزيل أي تشفير قد وضعته بنفسها، أو الذي وضع نيابة عنها، بحيث تصبح المادة المقدمة مقروءة. وينص القانون أن على الشركات أن تتخذ إجراءات مناسبة لتنفيذ المذكرة. وأي تقييم لمنطقية المذكرة سوف يشمل تقييم الخطوات التي على الشركة أن تتخذها لإزالة التشفير.

7 التطوير

1-0-7 يستعرض مسار **التطوير** في هذه الاستراتيجية كيفية حصولنا على الأدوات والقدرات التي تحتاجها المملكة المتحدة لحماية نفسها من التهديد الإلكتروني، وكيفية تعزيز تلك القدرات.

2-0-7 تحتاج المملكة المتحدة إلى المزيد من المحترفين ذوي المواهب والكفاءات من المتخصصين في أمن المعلوماتية. وستعمل الحكومة حاليا لردم الهوة الآخذة في الاتساع بين العرض والطلب بالنسبة للمختصين الأساسيين في أمن المعلوماتية، ولكي تضخ طاقة متجددة في مجالات التعليم والتدريب. هذا هدف طويل الأمد غايته إحداث نقلة نوعية، وستكون هذه الاستراتيجية انطلاقة لهذا العمل الهام الذي سيستمر بالضرورة إلى ما بعد 2021. إن العمالة الماهرة هي بمثابة شريان الحياة بالنسبة لبيئة أمن معلوماتية تجارية متكاملة حيوية ورائدة عالميا. وهذه البيئة سوف تضمن لشركات الإنترنت الناشئة أن تزدهر وأن تتلقى الاستثمار والدعم اللذين تحتاجهما. ومثل ذلك الابتكار والطاقة لا يمكن أن يأتيا إلا عن طريق القطاع الخاص، ولكن الحكومة ستعمل لتطويره، وستسعى بجد للترويج لقطاع أمن المعلوماتية عموما في الأسواق العالمية. كما يحتاج الأمر إلى قطاع أبحاث علمية ناشط ومزدهر لدعم تطوير كوادر بشرية ذات مهارات عالية، وكذلك لضمان ترجمة الأفكار الجديدة إلى أحدث المنتجات.

1-7 تعزيز مهارات أمن المعلوماتية

1-1-7 المملكة المتحدة بحاجة لمعالجة المسائل المنهجية المتعلقة بصلب مشكلة نقص المهارات في قطاع الإنترنت: عدم توفر شباب يافعين ممن يرغبون بالدخول في تلك المهنة؛ والنقص في أعداد المتخصصين بأمن المعلوماتية حاليا؛ وعدم تطرق دورات الكمبيوتر بشكل واف لمفاهيم أمن المعلوماتية وأمن المعلومات؛ ونقص المعلمين المؤهلين جيدا؛ وغياب سبل الاحتراف والتدريب الراسخة التي تؤدي إلى اتخاذ أمن المعلوماتية كمهنة.

2-1-7 ذلك يدعو لتدخل سريع من جانب الحكومة للمساعدة في التصدي للنقص الحالي، ولتطوير استراتيجية متينة طويلة الأمد يكون بإمكانها البناء على تلك التدخلات من أجل ردم الفجوة في الكفاءات. إلا أنه ينبغي إدراك أنه لكي يعطي ذلك الجهد نتائج ملموسة، لابد له أن يكون عملا مشتركا يساهم فيه قطاع واسع من المشاركين والاطراف المؤثرة من الحكومات المفوضة والقطاع العام والجهات التعليمية والمؤسسات الأكاديمية وقطاع المعلوماتية.

الهدف

3-1-7 تتطلع الحكومة لضمان مصدر مستدام لأفضل ما يمكن إيجاده من مهارات محلية في مجال أمن المعلوماتية، وتعمل بنفس الوقت لتمويل تدخلات محددة على المدى القصير للمساعدة في سد النقص في مهارات معينة. كما سنعمل لتحديد وتطوير مهارات أمن المعلوماتية المطلوبة بين كافة المواطنين والقوى العاملة من أجل العمل على الإنترنت بأمن وأمان.

4-1-7 يتطلب ذلك عملا على مدى السنوات العشرين القادمة، وليس فقط السنوات الخمس القادمة. وسوف نحدد مجموعة الإجراءات المنسقة طويلة الأمد التي تحتاجها الحكومة وقطاع المعلوماتية والمؤسسات التعليمية والأكاديمية من أجل إيجاد مصدر مستدام من ذوي الكفاءات في مجال أمن المعلوماتية الذين يُلبّون المعايير والشهادات المطلوبة لممارسة عملهم بثقة وبشكل آمن.

5-1-7 سنسد الفجوة نقص المهارات بمجال الدفاع. فسوف نجتذب إلى الحكومة أخصائيي أمن المعلوماتية ممن ليسوا فقط مدربين بشكل جيد، بل إنهم أيضا مستعدون للمحافظة على أمننا القومي. ذلك يشمل فهم تأثير الفضاء الإلكتروني على العمليات العسكرية.

مقاربتنا

6-1-7 سوف نطور ونطبق استراتيجية مهارات قائمة بذاتها تبني على العمل الجاري حاليا لإدخال أمن المعلوماتية في النظام التعليمي. وسيستمر ذلك في تحسين حالة تدريس علوم الكمبيوتر بوجه عام، كما سيُدخل أمن المعلوماتية في المناهج. فكل من يدرس علوم الكمبيوتر أو التكنولوجيا أو المهارات الرقمية سيتعلم أساسيات أمن المعلوماتية، وسيكون بإمكانه أن يأتي بما تعلمه من مهارات إلى سوق العمل. وفي سياق هذا الجهد، سوف نعالج مسألة الاختلال في عدد الذكور والإناث في المهن المرتكزة على الإنترنت، وسنحاول الوصول إلى أناس من خلفيات متنوعة لكي نضمن أننا نأخذ من أكبر مجموعة متوفرة من المواهب. وسنعمل بشكل وثيق مع الحكومات

المفوضة للتشجيع على اتباع أسلوب متسق في كافة أرجاء المملكة المتحدة.

7-1-7 سنعرض بشكل أكثر وضوحا الأدوار الخاصة بكل من الحكومة وقطاع المعلوماتية، بما في ذلك كيف يمكن لتلك الأدوار أن تتطور مع الوقت. وللحكومة والحكومات المفوضة دور أساسي في توفير البيئة الملائمة لتطوير مهارات أمن المعلوماتية وتحديث النظام التعليمي بحيث يعكس الاحتياجات المتغيرة للحكومة ولهذا القطاع. ولكن ستقع على عاتق أرباب العمل مسؤولية كبيرة أيضا لطرح احتياجاتهم بشكل واضح ومُفصَّل، وكذلك لتدريب وتطوير العاملين لديهم ومن يدخلون المهنة من جيل الشباب. أما قطاع المعلوماتية فله دور هام في توفير السبل المهنية والتدريبية المتنوعة والجذابة بالشراكة مع المؤسسات الأكاديمية والمؤسسات المهنية والنقابات الحرفية.

8-1-7 إدراكا منا للتحدي الجماعي الذي نواجهه في سد النقص بالمهارات، سوف ننشئ مجموعة استشارية للمهارات تضم الحكومة وأرباب العمل وهيئات مهنية وجهات توفير المهارات ومؤسسات تعليمية وأكاديمية، الأمر الذي سيقوي الترابط بين تلك القطاعات الأساسية. ستعمل هذه المجموعة على دعم تطوير استراتيجية طويلة الأمد تأخذ في حسبانها التطورات الحاصلة في المجال الأعم للمهارات الرقمية، بما يضمن أن اعتبارات أمن المعلوماتية مدمجة ومتسقة في كافة المجالات. وستعمل المجموعة مع جهات مشابهة في أنحاء المملكة المتحدة.

9-1-7 وإلى جانب ذلك، ستستثمر الحكومة في مجموعة من المبادرات لإدخال تحسينات فورية، وللاستناد إليها في تطوير استراتيجية طويلة الأمد بشأن المهارات. وستشمل تلك المبادرات:

- وضع برنامج مدرسي لإحداث تغيير كبير في التعليم المتخصص بأمور أمن المعلوماتية والتدريب لليافعين الموهوبين من الفئة العمرية 14-18 سنة (ذلك يشمل أنشطة داخل الصفوف، وحلقات بعد الدوام المدرسي مع موجهين خبراء، ومشاريع محفزة لقدراتهم، ودروس أثناء عطلة الصيف)؛
- إنشاء برامج تدريبية على مستوى التعليم العالي والتعليم الجامعي ضمن قطاعات الطاقة والمالية والمواصلات لمعالجة نقص المهارات في مجالات أساسية؛
- تأسيس صندوق من أجل الاحتفاظ بالعاملين الذين يُظهرون إمكانات كبيرة للعمل في مهنة أمن المعلوماتية؛
- تحديد ودعم التعليم في المجال الإلكتروني لمرحلتي الجامعة والدراسات العليا، والتعرف على الثغرات في المهارات المتخصصة وسدها - مع الإقرار بالدور الأساسي الذي تلعبه الجامعات في تطوير المهارات؛
- دعم اعتماد التطوير المهني للمدرسين في مجال أمن المعلوماتية. وهذا من شأنه أن يساعد المدرسين وغيرهم في الوظائف التعليمية المساندة في فهم تدريس أمن المعلوماتية، كما يوفر السبيل لاعتمادهم من جهات خارجية.
- تطوير مهنة أمن المعلوماتية، ويشمل ذلك الحصول على اعتماد ملكي لمزاولة المهنة بحلول 2020، الأمر الذي يعزز تميّز أمن المعلوماتية في قطاع المعلوماتية، ويوفر جهة مركزية بإمكانها أن تقدم المشورة وأن ترسم السياسة الوطنية في هذا المجال؛
- إنشاء أكاديمية للدفاع الإلكتروني كمركز للجودة في التدريب الإلكتروني وإجراء التمارين لوزارة الدفاع وكافة إدارات الحكومة عموما، وتُعنى الأكاديمية بالمهارات المتخصصة والتعليم الأعم؛
- تطوير الفرص من أجل التعاون في التدريب والتعليم بين الحكومة والقوات المسلحة وقطاع المعلوماتية والمؤسسات الأكاديمية، إلى جانب منشآت للحفاظ على المهارات والتدريب عليها؛
- العمل مع قطاع المعلوماتية لتوسيع نطاق برنامج "الفضاء الإلكتروني أولا" (CyberFirst) لتحديد ورعاية المواهب الشابة المتنوعة للدفاع عن أمننا القومي؛
- إدخال أمن المعلوماتية والمهارات الرقمية كجزء لا يتجزأ من الدورات ذات الصلة ضمن النظام التعليمي، من المدارس الابتدائية إلى مرحلة الدراسات العليا، وبالتالي تحديد المعايير وتحسين النوعية وتوفير أساس صلب للمضي قُدُما في تطوير هذا المجال.

بما أن التعليم هو من المجالات التي تتكفل بها الحكومات المفوضة، فإن بعض تلك المبادرات سوف يُطبّق فقط في انجلترا. إلا أننا سنعمل مع الحكومات

المفوضة لتشجيعها على اتباع مقاربة متسقة في أنحاء

قياس النجاح

10-1-7 ستقيس الحكومة مدى نجاحها في تعزيز مهارات أمن المعلوماتية من خلال تقييم ما أحرزته من تقدم نحو تحقيق الغايات التالية:

- وجود سبل فعالة وواضحة لدخول مهنة أمن المعلوماتية بحيث تكون جذابة لشرائح متنوعة من الناس.
- تدريس أمن المعلوماتية بطريقة فعالة بحلول 2021 كجزء متكامل من الدورات ذات الصلة، من المرحلة الابتدائية إلى مرحلة الدراسات العليا؛
- اعتبار أمن المعلوماتية مهنة راسخة لها مسارات واضحة في الحياة العملية، وحاصلة على الاعتماد الملكي؛
- المعرفة الوافية بأمن المعلوماتية تصبح جزءا أساسيا من التطوير المهني المستمر لمحترفي العمل الأمني غير الإلكتروني في كافة مجالات الاقتصاد؛
- يتوفر للحكومة والقوات المسلحة أخصائيون بمجال الفضاء الإلكتروني قادرون على الحفاظ على أمن المملكة المتحدة وصمودها.

2-7 تنشيط النمو في قطاع أمن المعلوماتية

1-2-7 من الضروري لاقتصادنا الحديث والرقمي أن يكون لدينا قطاع أمن معلوماتية مزدهر ومبدع. وتوفر الشركات البريطانية العاملة في مجال أمن المعلوماتية تكنولوجيا وتدريبات ومشورة عالمية المستوى لقطاع المعلوماتية والحكومات. ولكن في حين أن المملكة المتحدة رائدة في هذا المجال، إلا أنها تواجه منافسة شرسة في الحفاظ على تفوقها. كما إن هناك عقبات ينبغي على الحكومة أن تجد حلا لها. فالشركات والعلماء البريطانيون يطورون التكنولوجيا المتقدمة، غير أن بعضهم يحتاج إلى الدعم لتطوير المهارات التجارية والتدريبية اللازمة للنجاح. وهناك فجوات في التمويل تقف عائقا أمام نمو الشركات الصغيرة والمتوسطة وتوسعها إلى أسواق ومناطق جديدة. والمنتجات والخدمات الأكثر إبداعا، التي تتيح لنا إمكانية البقاء متفوقين على التهديدات، تواجه صعوبة في إيجاد المستعدين لأن يتبنوها في المراحل المبكرة. إن التغلب على تلك المصاعب يتطلب من النظام التعليمي في المملكة المتحدة.

الحكومة وقطاع المعلوماتية والمؤسسات الاكاديمية أن يعملوا معا بفعالية.

الهدف

2-2-7 سوف تدعم الحكومة إنشاء قطاع أمن معلوماتية متنام ومُبتكِر وناجح في المملكة المتحدة لكي توفر بيئة يتحقق فيها ما يلي:

- شركات الأمن تزدهر أعمالها وتتلقى الاستثمارات التي تحتاجها للنمو؛
- التعاون الوثيق بين أفضل الأدمغة من الحكومة والجامعات والقطاع الخاص لتحفيز الابتكار؛
- عملاء الحكومة وقطاع المعلوماتية مطمئنون بالشكل الكافي ومستعدون للإقبال على الخدمات المتطورة.

مقاربتنا

3-2-7 لتوفير هذه البيئة، فإننا سوف:

- نعمل لتحويل الابتكار بالمؤسسات الأكاديمية إلى منتجات تجارية، ونوفر التدريب والإرشاد للأكاديميين؛
- ننشئ مركزين للابتكار للدفع تجاه تطوير أحدث المنتجات الإلكترونية وتأسيس شركات أمن معلوماتية حيوية جديدة، وسيكون المركزان في صلب برنامج للمبادرات غايته تقديم الدعم الذي تحتاجه الشركات الناشئة لكسب أوائل عملائها واجتذاب المزيد من الاستثمار؛
- نخصص جزءا من صندوق الدفاع والابتكار الإلكتروني البالغ 165 مليون جنيه إسترليني لدعم المشتريات المبتكرة في مجالي الدفاع والأمن؛
- نوفر للشركات مرافق لإجراء التجارب كي تطور منتجاتها، ويصاحب ذلك شكل من التقييم السريع للجيل القادم من منتجات وخدمات أمن المعلوماتية حين ظهورها، ما يُمكِّن العملاء من الاطمئنان لاستخدامها؛
- نعتمد على الخبرات الجماعية لشراكة النمو الإلكتروني بين الحكومة وقطاع المعلوماتية لكي نساعد في صياغة وتركيز التدخلات من أجل مزيد من النمو والابتكار؛

- نساعد الشركات من كافة الأحجام على التوسع ودخول الأسواق الدولية؛

4-2-7 سوف نستخدم أيضا ثِقل المشتريات الحكومية لتحفيز الابتكار. تواجه الحكومة حاليا بعضا من أصعب التحديات بمجال أمن المعلوماتية، وبعضا من أكبر التهديدات. وبإمكاننا، بل يتوجب علينا، أن نبحث عن الحلول الأكثر فعالية لتلك المشاكل. ذلك يعني أن نُسهِّل على الشركات الصغيرة أن تتعامل تجاريا مع الحكومة. كما يعني أيضا أن على الحكومة أن تكون أقل تخوفا من المجازفة في اختبار واستخدام المنتجات الجديدة. وهذا الحل مربح للطرفين: حيث تحصل الحكومة على أفضل الخدمات، بينما تحصل التكنولوجيا المُبدِعة على من يتبناها باكرا، ما يُسهِل جذب الاستثمارات وتوسيع قاعدة العملاء. وسوف سنشجع كافة الإدارات الحكومية، بما فيها الحكومات المفوضة، على تبني مقاربة مماثلة.

"نريد توفير بيئة إلكترونية تحصل فيها الشركات الإلكترونية الناشئة على الاستثمار والدعم الذي تحتاجه لكي تكسب صفقات تجارية حول العالم، وتوفير مصدر مستمر للابتكار يوزع الأفكار الجديدة بين القطاع الخاص والحكومة والمؤسسات الأكاديمية."

مات هانكون، عضو البرلمان ووزير الشؤون الرقمية والثقافة

قياس النجاح

5-2-7 ستقيس الحكومة مدى نجاحها في تنشيط النمو في قطاع أمن المعلوماتية من خلال تقييم ما تم إحرازه من تقدم نحو تحقيق الغايات التالية:

- نمو عالمي أعلى من المتوسط في حجم قطاع المعلوماتية للمملكة المتحدة سنة بعد سنة؛
- زيادة كبيرة بالاستثمار في الشركات التي هي في مراحلها الأولى؛
- اعتماد تكنولوجيات أمن معلوماتية أكثر ابتكارا وفعالية في الحكومة.

3-7 تشجيع علوم وتكنولوجيا أمن المعلوماتية

1-3-7 إن قطاع التكنولوجيا الإلكترونية المزدهر في المملكة المتحدة وأبحاثه المتطورة هو الركيزة الأساسية

- نعمل على نشر المعايير الدولية المتفق عليها التي تدعم الدخول إلى سوق المملكة المتحدة.

لقدراتنا في مجال أمن المعلوماتية الرائدة عالميا. وللحفاظ على سمعة المملكة المتحدة وتعزيزها كرائدة عالميا في أبحاثها المتطورة، فإننا نحتاج أن تستمر مؤسساتنا البحثية الأكاديمية باجتذاب أفضل وأذكى الأدمغة في مجال أمن المعلوماتية. وسيتطلب ذلك منا أن ندعم مراكز الإبداع التي تستقطب أقدر العلماء والباحثين وأكثرهم نشاطا، وأن نعمق الشراكة الفاعلة بين المؤسسات الأكاديمية والحكومة وقطاع المعلوماتية. وسوف يتضمن ذلك أن تلعب الحكومة دور التوفيق بين الشركاء الملائمين، حيث سنقدم الحوافز لمثل ذلك النمط من العمل المشترك. والنجاح في ذلك سيؤدي بنا لتأسيس بيئة إلكترونية قائمة بذاتها تتيح للأفكار - والأشخاص - التنقل بين القطاعات الثلاثة بطريقة مفيدة لكافة الأطراف.

الهدف

2-3-7 أن تكون المملكة المتحدة قد عززت مكانتها كرائدة عالميا في العلوم والتكنولوجيا الإلكترونية بحلول 2021. والشراكات المرنة بين الجامعات وقطاع المعلوماتية سوف تترجم الأبحاث إلى منتجات وخدمات ناجحة تجاريا. وستحافظ المملكة المتحدة على سمعتها في مجال التميّز بالابتكار، بما في ذلك بالمجالات التي تتميز فيها المملكة بقوة استثنائية على المستوى الوطني، مثل قطاع المال.

مقاربتنا

3-3-7 لتحقيق ذلك الهدف، ستشجع الحكومة العمل المشترك والابتكار وأنماط التمويل المرن للأبحاث، وتحويل الأبحاث إلى منتجات تجارية. وستعمل الحكومة على ضمان أن الجوانب الإنسانية والسلوكية للعمل في المجال الإلكتروني تحظى بالاهتمام الكافي، وأن الأنظمة التي تتجاوز كونها تقنية، كالعمليات التجارية والهياكل التنظيمية، داخلة ضمن علوم وتكنولوجيا الفضاء الإلكتروني.

4-3-7 سيكون ذلك الركيزة لابتكار منتجات وأنظمة وخدمات تكون جميعها "آمنة افتراضيا"، وتكون إجراءات الأمن الوافية قد أُخذت في الاعتبار منذ البداية، بحيث يصبح إبطال خاصية الأمن بناء على خيار واعٍ من المستخدمين.

5-3-7 سوف ننشر استراتيجية مفصلة عن العلوم والتكنولوجيا الإلكترونية بعد مشاورات مستفيضة مع الشركاء والجهات المعنية. ذلك يشمل معرفة مجالات العلوم والتكنولوجيا التي تعتبرها الحكومة وقطاع المعلوماتية والمؤسسات الأكاديمية مهمة، وكذلك تحديد الفجوات في القدرات الحالية للمملكة المتحدة لمعالجتها.

6-3-7 ستواصل الحكومة توفير التمويل والدعم لمراكز الإبداع الأكاديمية ومعاهد الأبحاث ومراكز التدريب على مستوى الدكتوراه. وعلاوة على ذلك، سننشئ مركزا جديدا للأبحاث يتخصص بموضوع واحد ذي أهمية استراتيجية. كما سوف نُموِّل المزيد من الابحاث في المجالات التي ترى فيها الاستراتيجية المقبلة للعلوم والتكنولوجيا الإلكترونية فجوات في القدرات. من بين المجالات الهامة اتي ستُؤخذ بالاعتبار: علم تحليل البيانات الضخمة، والأنظمة المستقلة، وأنظمة التحكم الصناعي الموثوقة، والأنظمة الفضائية-المادية، وإنترنت الأشياء، والمدن الذكية، والتحقق من الأنظمة الآلية، وعلوم أمن المعلوماتية.

7-3-7 سنستمر في رعاية طلاب درجة الدكتوراه البريطانيين في مراكز التميز الأكاديمي لزيادة عدد البريطانيين ممن لديهم خبرات إلكترونية.

8-3-7 ستعمل الحكومة مع عدة جهات، ومنها المركز البريطاني للابتكار (Innovate UK) ومجالس الأبحاث، لتشجيع العمل المشترك بين قطاع المعلوماتية والحكومة والمؤسسات الأكاديمية. ولدعم هذا التعاون، سوف نراجع أفضل الممارسات فيما يخص التصنيفات الأمنية، وننتقي الخبراء الذين خضعوا لتدقيق أمني، بما في ذلك الأكاديميين. فذلك يضمن أن العمل من المجال غير المصنف أمنياً إلى مجال تصنيفه أعلى من سري يمكن أن يكون تعاونيا إلى أقصى درجة ممكنة.

9-3-7 سوف تمول الحكومة "تحديا هائلا" لتحديد الحلول المبتكَرة وتوفيرها لمعالجة بعض من المشاكل الأكثر إلحاحاً في أمن المعلوماتية. وبرنامج الاستثمار بالمعلوماتية "CyberInvest"، وهي شراكة جديدة بين الحكومة وقطاع المعلوماتية لدعم الأبحاث المتطورة بمجال أمن المعلوماتية ولحماية المملكة المتحدة في الفضاء الإلكتروني، فستكون جزءا من مقاربتنا لتنمية الشراكة بين القطاع الأكاديمي والحكومة وقطاع المعلوماتية.

قياس النجاح

10-3-7 ستقيس الحكومة مدى نجاحها في توفير علوم وتكنولوجيا أمن المعلوماتية من خلال تقييم التقدم الذي تم إحرازه نحو تحقيق الغايات التالية:

- ارتفاع كبير في أعداد الشركات البريطانية التي تنجح في تحويل نتائج الأبحاث الإلكترونية الأكاديمية إلى منتجات تجارية، وانخفاض في الفجوات المعروفة في القدرات البحثية للمملكة المتحدة في مجال أمن المعلوماتية، واتخاذ اتخاذ خطوات فعالة لسد تلك الفجوات.
- أن يُنظر إلى المملكة المتحدة كإحدى الدول الرائدة في العالم في أبحاث وابتكارات أمن المعلوماتية.

4-7 مسح الأفق الفعال

1-4-7 يتوجب على الحكومة ضمان أن يأخذ واضعو السياسة في حسبانهم التغيرات المتواصلة في المجال الإلكتروني والجيوسياسي والتكنولوجي. ولتحقيق ذلك، علينا أن نستفيد بفعالية من مسح الأفق الواسع وأعمال التقييم. وسنحتاج لأن نستثمر في تحصين أنفسنا ضد الأخطار المستقبلية وأن نتوقع التغيرات في السوق التي من شأنها أن تؤثر سلباً على صمودنا الإلكتروني خلال خمس أو عشر سنوات القادمة. كما نحتاج إلى برامج لمسح الأفق يتمخض عنها توصيات للحكومة حول كيفية رسم السياسية الحالية والمستقبلية والتخطيط للبرامج.

الهدف

2-4-7 ستعمل الحكومة على ضمان أن برامج مسح الأفق تشمل تقييما دقيقا للمخاطر الإلكترونية، وأن يكون ذلك مدمجا في أمن المعلوماتية وغيره من مجالات تطوير سياسات التكنولوجيا، إلى جانب تقييم كافة مصادر الخطر والدلائل الأخرى المتوفرة. وسوف ندمج معا مسح الأفق بين الأمن القومي ومجالات السياسة الأخرى لضمان تقييم شامل للتحديات والفرص الناشئة.

مقاربتنا

3-4-7 سوف نقوم بما يلي:

- تحديد الفجوات في الجهود الحالية، وتنسيق العمل عبر كافة الحدود التنظيمية لتطوير مقاربة شاملة لمسح الأفق من أجل أمن المعلوماتية؛
- تشجيع تكامل أفضل بين الجوانب الفنية لأمن المعلوماتية وعلم السلوك؛
- دعم المراقبة الشديدة لسوق الجرائم الإلكترونية لكشف الأدوات والخدمات الجديدة التي قد تُسهِّل نقل التكنولوجيا لدول معادية وللإرهابيين أو المجرمين؛
- تحليل التكنولوجيات الناشئة للتحكم بالعمليات المرتبطة بالإنترنت؛
- توقع بروز نقاط ضعف فيما يخص العملات الرقمية؛
- مراقبة توجهات السوق في تكنولوجيات الاتصالات اللاسلكية بغرض تطوير دفاعات مبكرة ضد الاعتداءات المستقبلية المنتظرة.

4-4-7 ندرك أن مسح الأفق يتخطى الجانب الفني ليشمل الأبعاد السياسية والاقتصادية والتشريعية والاجتماعية والبيئية. وأمن المعلوماتية مجرد أحد أوجه المسائل التي يستطيع مسح الأفق المساعدة في معالجتها. وبالتالي، سوف نحرص على ضمان أنه حيثما نجري مسح الأفق لهذه الأوجه الأخرى من السياسات، فإننا سنأخذ بالاعتبار أية جوانب متعلقة بأمن المعلوماتية.

5-4-7 كما سنحرص على أن يتَّبع رسم السياسة الإلكترونية مقاربة قائمة على الشواهد، ويأخذ بالحسبان التقييمات من كافة المصادر المتوفرة. ذلك يشمل، على سبيل المثال:

- دليل فني محدد، مثل الدليل على إنترنت الأشياء، أو الدور المستقبلي للمواد المتقدمة؛
- التوجهات الدولية الاستراتيجية والمجتمعية وأثرها على الفضاء الإلكتروني.

6-4-7 سنحرص أن تتم مراعاة اعتبارات أمن المعلوماتية ضمن نطاق "خلية تحليل التكنولوجيا والابتكارات الناشئة"، وهي خلية حكومية سيتم إنشاؤها لتحديد التهديدات والفرص التكنولوجية المتعلقة بالأمن القومي، ومراعاة الفضاء الإلكتروني في هياكل مسح الأفق القائمة، التي تشمل المجموعة الحكومية للدراسات المستقبلية والمجموعة الاستشارية لمسح الأفق التابعة لوزير شؤون مجلس الوزراء.

قياس النجاح

7-4-7 ستقيس الحكومة مدى نجاحها في بناء قدرة فعالة لمسح الأفق من خلال تقييم ما تم احرازه من تقدم نحو تحقيق الغايات التالية:

- إدخال مسح الأفق وتقييم كافة المصادر في كل مؤسسات الحكومة في رسم سياسة الفضاء الإلكتروني؛
- احتساب تأثير أمن المعلوماتية في جميع أعمال مسح الأفق الحكومية.

8 العمل الدولي

1-8 إن ازدهارنا الاقتصادي ورفاهنا الاجتماعي يعتمدان بشكل متزايد على انفتاح وأمن شبكاتنا التي تمتد إلى خارج حدودنا. وبالتالي من الضروري أن نعمل مع شركائنا الدوليين لضمان استمرار توفر فضاء إلكتروني يتسم بالانفتاح والأمن والأمان، ويحقق هذه الفوائد. وأهمية ذلك تزداد لدى اتصال المليار مستخدم القادمين بالإنترنت في أنحاء العالم.

2-8 التعاون الدولي بمجال المعلوماتية أصبح يشكل جزءا ضروريا من الاقتصاد العالمي والنقاش الأمني الأوسع. والسياسات المتعلقة بها متغيرة سريعا، ولا توجد بشأنها أي رؤية دولية واحدة متفق عليها. وقد نجحت المملكة المتحدة وحلفاؤها في ضمان توفر بعض عناصر النظام الدولي القائم على القواعد: حيث هناك اتفاق بأن القانون الدولي ينطبق على الفضاء الإلكتروني؛ وأن حقوق الإنسان تنطبق أثناء استخدام الإنترنت تماما كما تنطبق في الحياة خارج الإنترنت؛ وإجماع واسع على أن اتباع مقاربة متعددة الأطراف هي أفضل سبيل لإدارة تعقيدات إدارة الإنترنت. لكن مع نمو الانقسام في كيفية معالجة التحدي المشترك المتمثل بتحقيق توافق ما بين الأمن القومي والحقوق والحريات الفردية، يظل تحقيق إجماع دولي في هذا المجال هشا.

"علينا التعاون دوليا للاتفاق على قواعد السبيل الذي يضمن أمن وازدهار المملكة المتحدة مستقبلا في الفضاء الإلكتروني."

وزير الخارجية، بوريس جونسون

الهدف

3-8 تهدف المملكة المتحدة إلى ضمان مستقبل طويل الأجل من الفضاء الإلكتروني الذي يتسم بالانفتاح والسلام والأمن، ويدفع النمو الاقتصادي، ويعزز الأمن الوطني للمملكة المتحدة. وعلى هذا الأساس، ستواصل المملكة المتحدة: مناصرة النموذج متعدد الأطراف لإدارة الإنترنت؛ والعمل لبناء قدرات شركائنا لتحسين أمن المعلوماتية لديهم. وسعيا لتقليل التهديد للمملكة المتحدة ولمصالحنا، وأغلبه يأتي من الخارج، سوف نسعى للتأثير في قرارات المعنيين بالجرائم الإلكترونية، والتجسس الإلكتروني، والنشاط الإلكتروني المسبب للعراقيل والتخريب، ونواصل بناء أطر تدعم التعاون الدولي.

مقاربتنا

4-8 لتحقيق ذلك، سوف نعمل لأجل:

- تقوية وترسيخ فهم مشترك للتصرف المسؤول من الدولة بمجال الفضاء الإلكتروني؛
- تنمية الاتفاق على أن القانون الدولي ينطبق على الفضاء الإلكتروني؛
- مواصلة ترويج الاتفاق بشأن تصرف الدولة الطوعي المسؤول وغير الملزم؛
- مساندة وضع وتطبيق تدابير لبناء الثقة؛
- تنمية قدرتنا على عرقلة نشاط مرتكبي الجرائم الإلكترونية المتواجدين في الخارج وملاحقتهم قضائيا، وخصوصا في مناطق الولايات القضائية التي يصعب الوصول إليها؛
- المساعدة في تهيئة بيئة تتيح للأجهزة الأمنية لدينا التعاون مع بعضها لضمان التضييق على مرتكبي الجرائم الإلكترونية لتقليل الأماكن التي يمكنهم ارتكاب نشاطهم فيها دون خشية مواجهتهم للتحقيق والملاحقة القضائية؛
- تعزيز صمود الفضاء الإلكتروني عن طريق بلورة المعايير الفنية التي تنظم التقنيات الجديدة التي تنشأ دوليا (بما فيها التشفير)، وجعل الفضاء الإلكتروني "آمنا بالأساس" (secure by design) بشكل أكبر، وتشجيع أفضل الممارسات؛
- العمل على تطوير مقاربات مشتركة بين الدول التي تشترك بتوجهاتها بمجال قدرات مثل التشفير القوي، والذي له آثار عابرة للحدود؛
- تنمية قدرات الآخرين لمواجهة التهديدات التي تهدد المملكة المتحدة ومصالحها في الخارج؛

- مواصلة مساعدة شركائنا في تطوير أمنهم الإلكتروني – حيث بما أننا نشترك بنفس الفضاء الإلكتروني، سوف نصبح أكثر قوة معا حيث تحسن كل دولة دفاعاتها؛

- ضمان كون حلف الناتو مستعدا لمواجهة صراعات القرن 21 التي تدور في الفضاء الإلكتروني وفي ساحات المعارك على حد سواء؛

- العمل مع حلفائنا لتمكين الناتو من العمل بفعالية في الفضاء الإلكتروني تماما كفعاليته على الأرض وفي السماء وفي البحار؛

- ضمان أن تستمر "عملية لندن" الناتجة عن المؤتمر الدولي لأمن المعلوماتية في تشجيع التوصل لإجماع عالمي بشأن أن ينعم الفضاء الإلكتروني بالانفتاح والأمان والأمن.

5-8 هناك مجموعة من العلاقات والأدوات التي سوف نستمر بالاستثمار بها لتحقيق وتعزيز كافة أهدافنا الإلكترونية الدولية؛ حيث ليس باستطاعتنا تحقيق أهدافنا بمعزل عن الآخرين. ذلك يشمل:

- العمل بالتعاون مع حلفاء تقليديين وشركاء جدد لتأسيس علاقات سياسية وعملياتية قوية ونشطة، وضمان استمراريتها؛ وتهيئة الظروف السياسية لبناء تحالفات عالمية قوية؛

- استغلال نفوذنا لدى منظمات متعددة الأطراف كالأمم المتحدة ومجموعة العشرين والاتحاد الأوروبي وحلف الناتو ومنظمة التعاون الاقتصادي والتنمية ومنظومة الكومنويلث، وكذلك ضمن مجتمع التنمية العالمي؛

- بناء علاقات أقوى مع جهات غير حكومية – قطاع المعلوماتية، والمجتمع الدولي، والقطاع الأكاديمي، والمجتمع التقني. فلهذه الجهات دور حيوي تستنير به السياسات الدولية ولمواجهتها، وتعزيز الرسائل السياسية بشأن مجموعة واسعة من المسائل الإلكترونية. وروابطنا الأكاديمية عالمية المستوى تتيح منصة تعاونية محايدة بالعمل مع شركائنا الدوليين.

قياس النجاح

6-8 ستقيس الحكومة مدى نجاحها في تحقيق مصالحنا الدولية بالمجال الإلكتروني من خلال تقييم التقدم الحاصل في تحقيق الغايات التالية:

- تعاون دولي قوي يقلل الأخطار الإلكترونية التي تتعرض لها المملكة المتحدة ومصالحها في الخارج؛

- فهم مشترك لتصرف الدولة المسؤول في الفضاء الإلكتروني؛

- تعزيز الشركاء الدوليين لقدراتهم بمجال أمن المعلوماتية؛

- تقوية الإجماع الدولي حول فوائد كون الفضاء الإلكتروني ينعم بالانفتاح والأمان والأمن.

9 المقاييس

1-9 أمن المعلوماتية مازال مجالا غير ناضج نسبيا حيث يتعلق الأمر بالنتائج والآثار – عادة ما يشار إليها بعبارة "المقاييس". وعلم أمن المعلوماتية غامض بفعل المبالغة، ويعرقله عدم توفر بيانات محسوبة. وذلك مصدر إحباط لصانعي السياسات والشركات على حد سواء الذين واجهوا صعوبة في قياس الاستثمار في مقابل النتائج المتحققة. وترى الحكومة حسب تقديرها بأن الاستخدام الفعال للمقاييس ضروري لتطبيق هذه الاستراتيجية والتركيز على الموارد التي تعززها.

2-9 سوف نضمن استناد هذه الاستراتيجية إلى مجموعة دقيقة وشاملة من المقاييس التي يمكننا أن نقيس بمقابلها التقدم تجاه النتائج التي نصبو إلى تحقيقها. وإلى جانب كون المركز الوطني لأمن المعلوماتية إنجازا كبيرا بحد ذاته بموجب هذه الاستراتيجية، فإن له دورا فعالا في تمكين أجزاء أخرى من الحكومة وقطاع المعلوماتية والمجتمع من تحقيق كل هذه النتائج الاستراتيجية المشار إليها في هذه الاستراتيجية.

3-9 الملحق 3 يستعرض كيف أن تدابير النجاح المشار إليها في الاستراتيجية تساهم في النتائج الاستراتيجية، والتي ستخضع لمراجعة سنوية لضمان أن تعكس بدقة أهدافنا ومتطلباتنا الوطنية. باختصار، النتائج الاستراتيجية هي كما يلي:

1. لدى المملكة المتحدة قدرة العمل، بفعالية، لكشف التهديد نتيجة النشاط الإلكتروني للجهات المعادية، والتحقيق به ومواجهته.
2. أثر الجرائم الإلكترونية على المملكة المتحدة ومصالحها منخفض إلى درجة كبيرة، وهناك ما يردع المجرمين الناشطين عبر الإنترنت عن استهداف المملكة المتحدة.
3. لدى المملكة المتحدة قدرة العمل بفعالية على إدارة الأحداث الإلكترونية والاستجابة لها بفعالية لتقليل الضرر الذي تتسبب به للمملكة المتحدة والتصدي للاعتداءات الإلكترونية.
4. شراكتنا مع قطاع الدفاع الإلكتروني تعني أن وقوع اعتداء كبير عبر التصيّد واستخدام البرامج الضارة لم يعد فعالا.
5. المملكة المتحدة أكثر أمنا بفضل منتجات وخدمات تقنية يدخل أمن المعلوماتية في تصميمها، ومُفعّلة افتراضيا.
6. الشبكات والخدمات الحكومية ستكون آمنة قدر الإمكان منذ لحظة تطبيقها. وسيكون باستطاعة المواطنين استخدام الخدمات الحكومية الرقمية بكل ثقة، وهم على يقين بأن معلوماتهم آمنة.
7. جميع المؤسسات في المملكة المتحدة، كبيرها وصغيرها، تدير بفعالية خطر الإنترنت لديها، وتدعمها نصائح عالية الجودة يقدمها المركز الوطني لأمن المعلوماتية، ويعززها مزيج مناسب من التنظيمات والحوافز.
8. تتوفر في المملكة المتحدة البيئة المناسبة لتطوير واستمرارية قطاع أمن معلوماتية يمكنه تلبية احتياجات الأمن القومي لدينا.
9. لدى المملكة المتحدة إمدادات مستمرة من محترفي الإنترنت الماهرين لتلبية الطلب المتنامي في اقتصاد رقمي بشكل متزايد، في كل من القطاعين العام والخاص، وفي الدفاع.

10. تشتهر المملكة المتحدة بكونها رائدة عالميا في الأبحاث والتطوير بمجال أمن المعلوماتية، وذلك تعززه مستويات عالية من الخبرة في قطاع المعلوماتية والقطاع الأكاديمي في المملكة المتحدة.

11. تعمل الحكومة البريطانية بالفعل على التخطيط والإعداد لتطبيق السياسات، مستبقة تقنيات وتهديدات المستقبل، وهي بذلك "مستعدة للمستقبل".

12. التهديد للمملكة المتحدة ولمصالحها في الخارج بات أقل بفضل نمو الإجماع الدولي والقدرات الدولية بشأن التصرف المسؤول من الدول في فضاء إلكتروني يتسم بالانفتاح والأمن والأمان.

13. تبسيط سياسات ومؤسسات وهياكل المملكة المتحدة لتحقيق أكبر اتساق وفعالية في استجابة المملكة المتحدة لأي تهديد إلكتروني.

4-9 ندرك بأن بعض طموحاتنا بشأن هذه الاستراتيجية تتجاوز جدولها الزمني الممتد على خمس سنوات. وكي يتمكن أي استثمار بأمن المعلوماتية مستقبلا لما بعد سنة 2021 من الاستمرار في تحقيق أكبر أثر إيجابي ممكن، نعتزم تعميم هذه النتائج على الأجل الأطول ما بعد 2021 على مختلف القطاعات والجهات التنظيمية والمدققين وشركات التأمين وغير ذلك من أجزاء القطاعين العام والخاص، حيث إن الإدارة الفعالة لأمن المعلوماتية تدخل كجزء لا يتجزأ من الإدارة العادية لدى الجميع.

10 الختام: أمن المعلوماتية ما بعد 2021

1-10 التغيير السريع في مجال الإنترنت يلقي أمامنا باستمرار تحديات جديدة مع تغير التكنولوجيا ولجوء أعدائنا لاستغلالها. إلا أن هذه الاستراتيجية تهدف إلى توفير مجموعة من السياسات والأدوات والإمكانات التي تكفل قدرتنا على الرد سريعا وبمرونة على كل من التحديات الجديدة حالما برزت أمامنا.

2-10 فشلنا بالتصرف بفعالية يعني أن يستمر التهديد في استباق قدرتنا على حماية أنفسنا منه. يمكننا أن نتوقع بركانا من القدرات للتهديد على كافة المستويات.

3-10 على العكس من ذلك، إن أدركنا هذه التحديات الطموحة، سوف تلعب الحكومة البريطانية والشركات والمجتمع دورهم في تحقيق أمن المعلوماتية عموما في البلاد. وإن استطعنا ضمان تصميم وإدماج الأمن، افتراضيا، في التكنولوجيات التجارية، سيكون لدى المستهلكين والشركات سبب أقل يستدعي القلق بشأن أمن المعلوماتية. وإن عززت المملكة المتحدة سمعتها كبيئة آمنة لأداء الأعمال عبر الإنترنت، فسوف يختار مزيد من الشركات العالمية والمستثمرون نقل أعمالهم إلى هنا. وسيكون أمن شبكات البنية التحتية الأساسية والقطاعات التي تحتل أولوية أكثر فعالية. وبالتالي سوف يُضطر المعتدون المحتملون الذين يتطلعون لتطوير أدوات وطرق للاعتداء على أنظمة تحتوي مهام وبيانات أساسية لبذل جهود أكبر لتجاوز مستويات الأمن المحيطة بها. ومن شأن ذلك أن يغير معادلة الخطر مقابل المكافأة بالنسبة لمجرمي الإنترنت والناشطين الذين يضمرون الشر لشبكاتنا، والذين عليهم أن يتوقعوا نفس مستوى الملاحقة الجنائية دوليا المطبقة بشأن الجرائم التقليدية. وإن نجحنا في تعميم أمن المعلوماتية على كافة أجزاء مجتمعنا، فذلك يعني أن يكون باستطاعة الحكومة نفسها التخلي عن هذا الدور البارز، وإتاحة الفرصة للسوق والتكنولوجيا لدفع التغيير بمجال أمن المعلوماتية في كافة قطاعات الاقتصاد والمجتمع.

4-10 حتى في أكثر السيناريوهات تفاؤلا، ربما تتطلب بعض التحديات التي تواجهها المملكة المتحدة بمجال الإنترنت، سواء من حيث حجمها أو تعقيدها، أكثر من خمس سنوات لمعالجتها. لكن مع ذلك، توفر هذه الاستراتيجية لنا السبل لتغيير أمننا مستقبلا، وحماية ازدهارنا في العصر الرقمي.

الملحق 1: المختصرات

CAA – مركز تقييم المعلوماتية. مقره في المركز الوطني لأمن المعلوماتية، ويختص في تقييم التهديد الإلكتروني لوزارات الحكومة البريطانية لتستند إليه في سياساتها.

CERT – الفريق الوطني للاستجابة لطوارئ الكمبيوتر

CERT-UK – الفريق الوطني للاستجابة لطوارئ الكمبيوتر في المملكة المتحدة

CESG – الهيئة الفنية الوطنية لضمان المعلومات في المملكة المتحدة. تقدم خدمات نيابة عن الحكومة البريطانية تستند إلى الأبحاث والمعلومات حول أمن المعلومات.

CNI – البنية التحتية الحيوية. تلك هي العناصر الحيوية في البنية التحتية (أي الممتلكات أو المرافق أو الأنظمة أو العمليات، وكل من له دور أساسي في تشغيلها وتسهيل عملها)، والتي تؤدي خسارتها أو الإضرار بها إلى:

أ. أثر ضار كبير على توفر الخدمات الأساسية أو سلامتها أو تقديمها – بما في ذلك الخدمات التي إن تضررت يمكن أن تؤدي إلى خسائر كبيرة بالأرواح أو عدد كبير من الإصابات – مع أخذ الآثار الاقتصادية أو الاجتماعية الكبيرة بعين الاعتبار؛ و/أو

ب. الأثر الكبير على الأمن القومي أو الدفاع الوطني أو عمل الدولة.

CPNI – مركز حماية البنية التحتية الوطنية. يقدم نصائح تهدف إلى خفض احتمال تعرض مؤسسات البنية التحتية الوطنية لأعمال الإرهاب والتخريب. كما يعمل المركز بالشراكة مع المركز الوطني لأمن المعلوماتية لتقديم نصائح أمنية وقائية شاملة بشأن التهديدات من الفضاء الإلكتروني.

وقد أسس مركز حماية البنية التحتية الوطنية شراكات قوية مع مؤسسات القطاع الخاص في كافة أجزاء البنية التحتية، الأمر الذي يوفر بيئة آمنة يمكن تبادل المعلومات من خلالها لما يعود بالنفع على الجميع. والعلاقات المباشرة تعززها شبكة موسعة تضم إدارات حكومية أخرى ومؤسسات خدمات محترفة.

DDoS – اعتداء الحرمان من الخدمة الموزّع. إرسال فيض من الطلبات لنظام معلومات يفوق قدرته، وبالتالي يتسبب بعدم قدرة المرخص لهم استخدامه على الاتصال بنظام المعلومات هذا.

GCHQ – القيادة المركزية الحكومية للاتصالات، وهو المركز المعني باستخبارات الإشارات في الحكومة والهيئة الفنية الوطنية للمعلوماتية (NTA)

ICT – تكنولوجيا المعلومات والاتصالات

MOD – وزارة الدفاع البريطانية

الناتو – حلف شمال الأطلسي

NCA – الوكالة الوطنية لمكافحة الجريمة، وهي إدارة حكومية غير وزارية

NCSC – المركز الوطني لأمن المعلوماتية

OSCE – منظمة الأمن والتعاون في أوروبا

SME – الشركات الصغيرة والمتوسطة

الملحق 2: معاني المصطلحات

مركز مكافحة الاحتيال Action Fraud – المركز الوطني في المملكة المتحدة للتبليغ عن جرائم الاحتيال والإنترنت، حيث يعتبر نقطة الاتصال لعامة المواطنين والشركات.

إجراءات تعزيز أمن الإنترنت active cyber defence – مبدأ تطبيق إجراءات أمنية لتعزيز أمن شبكات أو أنظمة المعلومات لجعلها أكثر صمودا بمواجهة محاولات الاعتداء.

إخفاء الهوية anonymisation – استخدام أدوات التشفير لإخفاء هوية المستخدم عبر الإنترنت.

التحقق authentication – عملية التحقق من هوية مستخدم أو عملية أو جهاز ما أو بيانات أخرى ذات صلة تتعلق بأي منهم

نظام التحقق الآلي automated system verification – تدابير لضمان عمل البرامج والأجهزة كما يجب، ودون أي أخطاء.

النظام المستقل autonomous system – جمع شبكات بروتوكولات الإنترنت (IP) التي يكون التحويل إليها من خلال كيان أو نطاق محدد.

البيانات الضخمة big data – مجموعات البيانات التي هي أكبر من أن تمكن معالجتها أو إدارتها باستخدام أدوات برنامج تجاري بالوقت المناسب، وتتطلب قدرات معالجة خاصة لإدارة حجمها وسرعة توفيرها وتعدد مصادرها.

بيتكُويْن Bitcoin – عملة رقمية ونظام الدفع بها.

برنامج ضار تجاري commodity malware – برنامج ضار متوفر على نطاق واسع ويمكن شراؤه أو تنزيله مجانا، وهو برنامج غير مُحصّص وتستخدمه مجموعة واسعة من مختلف مصادر التهديد.

استغلال شبكة الكمبيوتر computer network exploitation – التجسس الإلكتروني، استخدام شبكة كمبيوتر للتسلل إلى شبكة كمبيوتر مستهدفة وجمع معلومات منها.

سوق جرائم الإنترنت cybercrime marketplace – كافة المنتجات والخدمات التي تدعم بيئة جرائم الإنترنت.

علم التشفير cryptography – علم أو دراسة تحليل وفك تشفير الرموز والشيفرات؛ تحليل الشيفرات.

هجوم إلكتروني cyber attack – استغلال متعمد لأنظمة الكمبيوتر والشبكات والمؤسسات التي يعتمد عملها على الاتصالات الرقمية بهدف التسبب بأضرار.

جريمة إلكترونية cyber crime – الجريمة التي تعتمد على الإنترنت (أي التي يمكن ارتكابها فقط باستخدام أجهزة تعمل بتكنولوجيا المعلومات والاتصالات، حيث تكون تلك الأجهزة أداة لارتكاب الجريمة والهدف من ارتكابها)؛ أو الجرائم التي يمكن ارتكابها بمساعدة الإنترنت (أي التي يمكن ارتكابها دون استخدام أجهزة تعمل بتكنولوجيا المعلومات والاتصالات، كالاحتيال المالي، لكنها تغيرت إلى حد كبير جدا من حيث حجمها وانتشارها نتيجة استخدام أجهزة كهذه).

البيئة الإلكترونية cyber ecosystem – إجمالي البنية التحتية المترابطة والأشخاص والعمليات والبيانات والمعلومات وتقنيات الاتصال، إلى جانب البيئة والعوامل التي تؤثر في هذه التعاملات.

حادث إلكتروني cyber incident – حادث يهدد فعليا، أو يمكن أن يهدد، جهاز كمبيوتر أو جهاز متصل بالإنترنت أو شبكة متصلة بالإنترنت – أو بيانات تعالَج أو تخزَّن أو تُبَث عبر هذه الأنظمة – وقد يتطلب اتخاذ إجراء لتخفيف آثاره.

الاستثمار بالمعلوماتية CyberInvest – برنامج مشترك بين قطاع المعلوماتية والحكومة تكلفته 6.5 مليون جنيه إسترليني لدعم أبحاث متطورة بمجال أمن الإنترنت وحماية المملكة المتحدة بمجال الفضاء الإلكتروني.

النظام الإلكتروني-المادي cyber-physical system – أنظمة تضم عناصر حاسوبية ومادية متكاملة؛ أنظمة "ذكية".

الصمود الإلكتروني cyber resilience – القدرة العامة للأنظمة والمؤسسات على الصمود في مواجهة حوادث إلكترونية، والتعافي منها في حال وقوع ضرر.

أمن المعلوماتية cyber security – حماية الأنظمة المتصلة بالإنترنت (ذلك يشمل الأجهزة والبرامج والبنية التحتية ذات الصلة) والبيانات المحفوظة بها والخدمات التي تقدمها من أي محاولة للوصول إليها دون وجه حق أو التسبب بأضرار لها أو إساءة استخدامها. هذا يشمل أي ضرر متعمد يتسبب به مشغّل النظام، أو ضرر غير مقصود بسبب عدم اتباعه للإجراءات الأمنية أو حمله على التسبب بهذا الضرر.

اختبار المهارات بأمن المعلوماتية cyber security challenge – مسابقات تشجع الناس على اختبار مهاراتهم واتخاذ مهنة بمجال المعلوماتية.

الفضاء الإلكتروني cyberspace – الشبكة المترابطة من البنية التحتية لتكنولوجيا المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرّد.

التهديد الإلكتروني cyber threat – كل ما هو قادر على تقويض أو التسبب بأضرار لأنظمة المعلومات والأجهزة المتصلة بالإنترنت (ذلك يشمل الأجهزة والبرامج والبنية التحتية ذات الصلة) والبيانات المحفوظة بها والخدمات التي تقدمها، وذلك بطرق إلكترونية أساسا.

كشف المعلومات data breach – نقل أو كشف معلومات متوفرة على شبكة ما إلى طرف لا يحق له استلام أو الاطلاع على هذه المعلومات.

النطاق domain – اسم النطاق يحدد موقع مؤسسة أو كيان ما على الإنترنت، وهو مرتبط بعنوان بروتوكول الإنترنت.

نظام اسم النطاق domain name system – نظام تسمية الكمبيوترات وخدمات الشبكات بناء على تسلسل أسماء النطاق.

استقاء معلومات شخصية doxing – عملية البحث عن، أو قرصنة، معلومات شخصية محددة لشخص ما على الإنترنت ومن ثم نشرها.

التجارة الإلكترونية e-commerce – التجارة التي تتم عبر، أو بتسهيل من، الإنترنت.

التشفير encryption – تحويل البيانات المتوفر بشكل "نص بسيط" إلى شكل "نص إلكتروني" يخفي المعنى الأصلي للبيانات، وذلك للحيلولة دون كشفها أو استخدامها.

مسح الأفق horizon scanning – التدقيق المنهجي بالمعلومات لتحديد المخاطر والتهديدات المحتملة والإشكاليات التي قد تطرأ والفرص المتاحة، الأمر الذي يتيح الاستعداد بشكل أفضل وإدخال الجوانب المتعلقة بالاستغلال وتخفيف الأضرار في عملية وضع السياسة.

إدارة الحادث incident management – إدارة وتنسيق الجهد للتحقيق في، وتخفيف أثر، حادث إلكتروني معادٍ وقع أو محتمل وقوعه قد يؤدي لتقويض نظام أو شبكة والتسبب بأضرار.

الاستجابة للحادث incident response – جهود معالجة الآثار المباشرة قصيرة المدى نتيجة حادث ما، كما يمكن أن تساعد في التعافي على الأجل القصير.

نظام التحكم الصناعي industrial control system – نظام معلومات يستخدم للتحكم بالعمليات الصناعية، كالتصنيع والتعامل مع المنتجات والإنتاج والتوزيع، أو للتحكم بموارد البنية التحتية.

أنترنت الأشياء الصناعي industrial internet of things – استخدام تقنيات إنترنت الأشياء في الصناعة والتصنيع.

شخص داخلي insider – شخص يوثق به بالاطلاع على بيانات وأنظمة معلومات مؤسسة ما، لكنه يشكل تهديدا إلكترونيا سواء عن قصد أو بغير قصد أو عن غير دراية.

سلامة المعلومات integrity – كون المعلومات لم تتعرض للتغيير عن غير قصد، أو عن قصد، وهي معلومات دقيقة وتامة.

الإنترنت internet – شبكة كمبيوتر عالمية توفر مجموعة مختلفة من المعلومات وإمكانيات الاتصال، وتتألف من شبكات مترابطة باستخدام بروتوكولات موحَّدة للاتصالات.

إنترنت الأشياء internet of things – كافة الأجهزة والأدوات والمباني وغيرها من المواد التي تتضمن إلكترونيات وبرامج إلكترونية ومجسات يمكنها إيصال وتبادل المعلومات عبر الإنترنت.

عملية لندن London Process – تدابير ناتجة عن انعقاد مؤتمر لندن لأمن المعلوماتية في 2011.

برنامج ضار malware – برنامج إلكتروني أو رمز ضار، وذلك يشمل الفيروسات الثابتة والفيروسات المتنقلة (ديدان) وبرامج حصان طروادة وبرامج التجسس.

شبكة (كمبيوتر) network – مجموعة من الكمبيوترات المضيفة، إلى جانب شبكة فرعية أو شبكة داخلية، والتي يمكن تبادل معلومات من خلالها.

الهجوم الإلكتروني offensive cyber – استخدام قدرات إلكترونية لعرقلة عمل شبكات الكمبيوتر وأجهزة متصلة بالإنترنت، أو الحرمان من الاتصال بها أو إضعاف أدائها أو تخريبها.

التصحيح patching – هو عملية تحديث برامج إلكترونية لتصحيح الأخطاء ونقاط الضعف فيها.

اختبار الاختراق penetration testing – إجراءات الهدف منها اختبار مدى صمود شبكة في مواجهة القرصنة، وهي إجراءات تكون بموافقة أو رعاية المؤسسة التي يجري اختبارها.

التصيّد phishing – استخدام رسالة إلكترونية يبدو أن مرسلها مصدر موثوق بهدف خداع مستلم الرسالة بالطلب منه أن ينقر على رابط خبيث أو فتح مرفقات خبيثة محملة ببرامج ضارة، أو الطلب منه أن يرسل معلومات حساسة لطرف ثالث غير معروف.

برنامج طلب فدية ransomware – برنامج خبيث يحرم المستخدم من إمكانية الاطلاع على ملفاته أو تشغيل كمبيوتره أو جهازه إلا بعد دفع فدية.

الاستطلاع reconnaissance – مرحلة الاعتداء التي يجمع خلالها المعتدي المعلومات ويحدد نطاق الشبكات، إلى جانب تحليلها لكشف نقاط الضعف فيها بغرض قرصنتها.

الخطر risk – إمكانية أن يتمكن تهديد إلكتروني معين من استغلال نقاط الضعف في نظام معلومات والتسبب بأضرار.

الموجّه router – جهاز يربط شبكات مترابطة عن طريق إرسال معلومات لشبكات أخرى تبعا لعناوين بروتوكول الإنترنت.

صبي النص الجاهز script kiddie – شخص لا مهارات لديه يستخدم نصوصا أو برامج جاهزة يمكن العثور عليها على الإنترنت لتنفيذ اعتداء إلكتروني، مثل تشويه موقع إلكتروني.

آمن افتراضيا secure by default – استغلال الاستخدام الآمن لتقنيات تجارية يكون أمن المعلوماتية فيها متوفرا بشكل افتراضي للمستخدمين.

آمن بالأساس secure by design – برامج إلكترونية وأجهزة وأنظمة مصممة أصلا بمجملها لتكون آمنة.

انتحال الشخصية في الرسائل النصية SMS spoofing – تقنية تخفي مصدر رسالة نصية عن طريق استبدال رقم هاتف المرسل (هوية المرسل) بنص أبجدي-رقمي. يمكن أن يستخدم المرسل هذه التقنية بشكل مشروع لاستبدال رقم هاتفه باسمه، أو اسم شركته، على سبيل المثال. أو يمكن استخدامها بشكل غير مشروع لانتحال هوية شخص آخر، على سبيل المثال.

الهندسة الاجتماعية social engineering – طرق يستخدمها المعتدي لخداع والتأثير على الضحية لحمله على أداء فعل ما أو الإفصاح عن معلومات سرية. عادة ما تشمل هذه الطرق فتح موقع إلكتروني خبيث، أو فتح ملف مرفق غير مطلوب.

شريحة أمان trusted platform module (TPM) – معيار دولي لمعالج تشفير آمن، وهو عبارة عن معالج صغير مصمم لتأمين الأجهزة عن طريق إدخال مفاتيح تشفير فيها.

المستخدم user – شخص أو مؤسسة أو عملية أوتوماتيكية يتصلون بنظام ما، سواء كان بإذن أو دون إذن.

فيروس virus – الفيروسات هي برامج خبيثة تصيب الكمبيوتر ويمكنها أن تنتشر إلى ملفات أخرى.

التصيّد الصوتي vishing (voice phishing) – استخدام تقنية صوتية (هاتف أرضي، هاتف نقال، تسجيل بريد صوتي، إلخ) لخداع أشخاص بحملهم على كشف معلومات مالية أو شخصية حساسة لأشخاص غير مصرح لهم استلامها، عادة لغرض الاحتيال.

نقاط الضعف vulnerability – أخطاء في برامج إلكترونية يمكن للقراصنة استغلالها.

الملحق 3: برنامج تطبيق عناصر الاستراتيجية

الاستراتيجية الوطنية لأمن المعلوماتية 2016-2021

الرؤية المستقبلية: المملكة المتحدة آمنة وقادرة على الصمود في مواجهة التهديدات الإلكترونية، ومزدهرة وواثقة في هذا العالم الرقمي

النتائج الاستراتيجية	مؤشرات النجاح الدلالية	تساهم في
1. **لدى المملكة المتحدة قدرة العمل، بفعالية، لكشف التهديد نتيجة النشاط الإلكتروني للجهات المعادية، والتحقيق به ومواجهته.**	• الشبكات الأكثر قوة لتبادل المعلومات التي أسسناها مع شركائنا الدوليين، والاتفاقيات متعددة الأطراف الأوسع نطاقا لمساندة التصرفات القانونية والمسؤولة من قبل الدول، تساهم بدرجة كبيرة في قدرتنا على فهم التهديد والرد عليه، الأمر الذي يؤدي لحماية أفضل للمملكة المتحدة. • تدابير الدفاع والردع لدينا، إلى جانب استراتيجياتنا الخاصة بكل بلد، تجعل المملكة المتحدة هدفا أكثر صعوبة لنجاح الجهات الخارجية والإرهابيين الناشطين عبر الإنترنت باستهدافها. • تحسين فهم التهديد الإلكتروني من إرهابيين خارجيين، من خلال كشف التهديدات الإرهابية الإلكترونية التي تهدد المملكة المتحدة، والتحقيق بها. • ضمان أن تظل قدرات الإرهاب الإلكتروني منخفضة على الأجل الطويل، وذلك من خلال مراقبة دقيقة للقدرات، وعرقلة إمكانات ونشاط الإرهاب الإلكتروني في أقرب فرصة. • المملكة المتحدة رائدة عالميا في قدرات الهجوم الإلكتروني. • أسست المملكة المتحدة سلسلة من المهارات والخبرات لتطوير واستخدام قدراتنا السيادية بمجال الهجوم الإلكتروني. • قدراتنا السيادية في مجال التشفير فعالة في حماية أسرارنا ومعلوماتنا الحساسة ممن يحاولون الاطلاع عليها دون وجه حق.	**الردع**
2. **أثر الجرائم الإلكترونية على المملكة المتحدة ومصالحها منخفض إلى درجة كبيرة، وهناك ما يردع المجرمين الناشطين عبر الإنترنت عن استهداف المملكة المتحدة.**	• نحقق أثرا أكبر في عرقلة نشاط مجرمي الإنترنت الذين يعتدون على المملكة المتحدة، مع ارتفاع عدد من نعتقلهم وندينهم، إلى جانب تفكيك عدد أكبر من الشبكات الإجرامية بفضل تنفيذ القانون. • تحسّن في قدرات تنفيذ القانون، بما في ذلك: تنمية قدرات ومهارات المختصين المكرسين لهذا الغرض وكذلك مسؤولي تنفيذ القانون العاديين؛ وتعزيز قدرات تنفيذ القانون في الخارج. • تحسين فعالية، وتوسيع نطاق، تدابير التدخل المبكر ("المنع") تساهم في تثبيط نوايا المجرمين وإصلاحهم. • انخفاض في جرائم الإنترنت الصغيرة نتيجة زيادة صعوبة إمكانية الاستعانة بخدمات الإجرام الإلكتروني وتقليل فعاليتها.	**الردع**
3. **لدى المملكة المتحدة قدرة العمل بفعالية على إدارة الحوادث الإلكترونية والاستجابة لها بفعالية لتقليل الضرر الذي تتسبب به للمملكة المتحدة والتصدي للاعتداءات الإلكترونية.**	• يجري إبلاغ السلطات عن نسبة أكبر من الجرائم، الأمر الذي يؤدي لفهم أفضل لحجم ومدى انتشار التهديد الإلكتروني. • الجرائم الإلكترونية تدار بفعالية وكفاءة أفضل وبشكل أكثر تكاملا، وذلك بفضل تأسيس المركز الوطني لأمن المعلوماتية ليكون بمثابة آلية مركزية للتبليغ عن الجرائم الإلكترونية والاستجابة لها. • سوف نعالج مسببات الاعتداءات على المستوى الوطني، وبالتالي تقليل احتمال الاستغلال المتكرر الذي يستهدف عددا من الضحايا	**الدفاع**

والقطاعات.

النتائج الاستراتيجية	مؤشرات النجاح الدلالية	تساهم في
4. شراكتنا مع قطاع الدفاع الإلكتروني تعني أن وقوع اعتداء كبير عبر التصيّد واستخدام البرامج الضارة لم يعد فعالا.	• "التصيّد- phishing" في المملكة المتحدة أكثر صعوبة نظرا لأن لدينا دفاعات كبيرة ضد استخدام مواقع ضارة، وحماية واسعة أكثر تفاعلا لمكافحة التصيّد، ومن الأصعب الاستعانة بأشكال أخرى من الاتصالات - مثل "التصيّد الصوتي- vishing" وانتحال الشخصية في الرسائل النصية (spoofing) - لشن اعتداءات من نوع "الهندسة الاجتماعية". • يُحجب الآن عدد أكبر كثيرا من الاتصالات الضارة والخدع التقنية المرتبطة بالاعتداءات الإلكترونية والاستغلال الإلكتروني. • حركة الإنترنت والاتصالات في المملكة المتحدة أقل عرضة لإعادة التوجيه من قبل أطراف خبيثة. • قدرات القيادة المركزية الحكومية للاتصالات، والدفاع، والوكالة الوطنية لمكافحة الجريمة في الاستجابة لدى وقوع تهديدات إجرامية وبرعاية دول أخرى قد تطورت إلى حد كبير جدا.	**الدفاع**
5. المملكة المتحدة أكثر أمنا بفضل منتجات وخدمات تقنية يدخل أمن المعلوماتية في تصميمها، ومُفعّلة افتراضيا.	• غالبية المنتجات والخدمات المتوفرة في المملكة المتحدة في 2021 تجعلها أكثر أمنا، ذلك لأن إعداداتها الأمنية مُفعّلة افتراضيا، أو أن الخصائص الأمنية تدخل في تصميمها بالأساس. • الشعب البريطاني يثق بالخدمات الحكومية لأنها مطبقة بأمان قدر الإمكان، ومستويات الاحتيال الذي يستهدفها تقع ضمن المعايير المقبولة للخطر.	**الدفاع**
6. الشبكات والخدمات الحكومية ستكون آمنة قدر الإمكان منذ لحظة تطبيقها. وسيكون باستطاعة المواطنين استخدام الخدمات الحكومية الرقمية بكل ثقة، وهم على يقين بأن معلوماتهم آمنة.	• لدى الحكومة فهم متعمق لمستوى الخطر الذي يواجه أمن المعلوماتية في كافة الإدارات الحكومية والقطاع العام ككل. • الإدارات الحكومية وغيرها من الأجهزة الحكومية تحمي نفسها وفق مستوى الخطر لديها، ووفق حد أدنى من المعايير الحكومية المقبولة. • الإدارات الحكومية والقطاع العام ككل أكثر قدرة على الصمود، ويمكنهم الاستجابة بفعالية لأي حوادث إلكترونية، مع الاستمرار بمهامهم والتعافي سريعا بعد الحادث. • التقنيات والخدمات الرقمية الجديدة التي تطلقها الحكومة ستكون آمنة إلكترونيا بشكل افتراضي. • لدينا علم بكافة نقاط الضعف عبر الإنترنت في الأنظمة والخدمات الحكومية، ونعمل بكل جهد لتخفيف آثارها. • كافة الموردين للحكومة يلتزمون بمعايير أمن معلوماتية مناسبة.	**الدفاع**

النتائج الاستراتيجية	مؤشرات النجاح الدلالية	تساهم في
7. جميع المؤسسات في المملكة المتحدة، كبيرها وصغيرها، تدير بفعالية خطر الإنترنت لديها، وتدعمها نصائح عالية الجودة يقدمها المركز الوطني لأمن المعلوماتية، ويعززها مزيج مناسب من التنظيمات والحوافز.	• نفهم تماما مستوى أمن المعلوماتية في البنية التحتية الحيوية، ولدينا تدابير للتدخل – حيثما لزم الأمر – لإدخال تحسينات لما هو في المصلحة الوطنية. • تدرك أهم شركاتنا ومؤسساتنا مستوى التهديد، وتطبق ممارسات متناسبة تتعلق بأمن المعلوماتية. • أمن المعلوماتية في اقتصاد المملكة المتحدة بنفس مستوى، أو يفوق مستوى، اقتصادات أخرى متقدمة. • طرأ انخفاض في عدد وشدة وأثر الاعتداءات الإلكترونية ضد الشركات في المملكة المتحدة، ذلك نظرا لتطبيق إجراءات وقائية إلكترونية. • لدى المملكة المتحدة أمن معلوماتية متحسن باستمرار نظرا لفهم المؤسسات وعامة المواطنين لمستويات المخاطر الإلكترونية التي يمكن أن يتعرضوا إليها، ومعرفتهم بالإجراءات الوقائية الإلكترونية التي عليهم اتخاذها لإدارة هذه المخاطر.	**الدفاع**
8. تتوفر في المملكة المتحدة البيئة المناسبة لتطوير واستمرارية قطاع أمن معلوماتية يمكنه تلبية احتياجات الأمن القومي لدينا.	• نمو عالمي يفوق المتوسط في حجم أمن المعلوماتية في المملكة المتحدة سنة بعد سنة. • زيادة كبيرة في الاستثمار بالشركات التي مازالت في المراحل الأولى من تأسيسها.	**التطوير**
9. لدى المملكة المتحدة إمدادات مستمرة من محترفي الإنترنت الماهرين لتلبية الطلب المتنامي في اقتصاد رقمي بشكل متزايد، في كل من القطاعين العام والخاص، وفي الدفاع.	• هناك سبل فعالة وواضحة لدخول مهنة أمن المعلوماتية، وهي تلقى الاهتمام لدى مجموعات مختلفة من الناس. • بحلول سنة 2021 سيكون تعليم أمن المعلوماتية بفعالية جزءا لا يتجزأ من المواد الدراسية في النظام التعليمي، من المرحلة الابتدائية وحتى مرحلة التعليم العالي. • أمن المعلوماتية مهنة تشتهر على نطاق واسع بكونها راسخة وتتضمن مسارات عمل واضحة، وحصلت على اعتماد ملكي. • المعرفة المناسبة بأمن المعلوماتية تمثل جزءا لا يتجزأ من التطوير المهني المستمر بالنسبة لمحترفين أمنيين ذوي صلة لكنهم غير مختصين بالإنترنت، وفي كافة القطاعات الاقتصادية. • يتوفر للحكومة والقوات المسلحة مختصون بالإنترنت قادرون على ضمان استمرارية أمن وصمود المملكة المتحدة.	**التطوير**

النتائج الاستراتيجية	مؤشرات النجاح الدلالية	تساهم في
10. تشتهر المملكة المتحدة بكونها رائدة عالميا في الأبحاث والتطوير بمجال أمن المعلوماتية، وذلك تعززه مستويات عالية من الخبرة في قطاع المعلوماتية والمؤسسات الأكاديمية في المملكة المتحدة.	• عدد الشركات البريطانية التي نجحت في تحويل الأبحاث الأكاديمية بمجال الإنترنت إلى منتجات تجارية ارتفع بدرجة كبيرة. وبات هناك فجوات أقل معروفة ومتفق عليها في قدرات أبحاث أمن المعلوماتية في المملكة المتحدة، واتخذت إجراءات فعالية لسد هذه الفجوات. • تعتبر المملكة المتحدة رائدة عالميا في الأبحاث والابتكار بمجال أمن المعلوماتية.	**التطوير**
11. تعمل الحكومة البريطانية بالفعل على التخطيط والإعداد لتطبيق السياسات، مستبقة تقنيات وتهديدات المستقبل، وهي بذلك "مستعدة للمستقبل".	• وضع سياسات أمن المعلوماتية يجمع بين جهود بحث الآفاق في كافة الإدارات الحكومية وتقييم كافة المصادر. • وأثر أمن المعلوماتية يشكل جزءا من جهود بحث الآفاق في كافة الإدارات الحكومية.	**التطوير**
12. التهديد للمملكة المتحدة ولمصالحها في الخارج بات أقل بفضل نمو الإجماع الدولي والقدرات الدولية بشأن التصرف المسؤول من الدول في فضاء إلكتروني يتسم بالانفتاح والأمن والأمان.	• من شأن تعزيز التعاون الدولي أن يقلل التهديدات الإلكترونية للمملكة المتحدة ولمصالحها في الخارج؛ • وفهم مشترك للتصرف المسؤول من الدول في الفضاء الإلكتروني؛ • وتعزيز الشركاء الدوليين لقدراتهم بمجال أمن المعلوماتية؛ • وإجماع دولي قوي على فوائد كون الفضاء الإلكتروني يتسم بالانفتاح والأمن والأمان.	**العمل الدولي والنفوذ**
13. تبسيط سياسات ومؤسسات وهياكل المملكة المتحدة لتحقيق أكبر اتساق وفعالية في استجابة المملكة المتحدة لأي تهديد إلكتروني.	• مسؤوليات الحكومة بمجال أمن المعلوماتية مفهومة، وخدماتها متوفرة للجميع. • شركاؤنا يعلمون أفضل السبل للتفاعل مع الحكومة بمسائل تتعلق بأمن المعلوماتية.	**مشترك**