HM Government

الاستراتيجية الإلكترونية الوطنية 2022

ريادة مستقبل إلكتروني في كافة أرجاء المملكة المتحدة

الاستراتيجية الإلكترونية الوطنية 2022

ريادة مستقبل إلكتروني في كافة أرجاء المملكة المتحدة

جدول المحتويات

محتوى إضافي

مقدمة

المملكة المتحدة مجتمع منفتح وديمقراطي، وسجله في التعاون والابتكار يؤكد على نجاحنا كأمة عالمية منفتحة على الخارج. يتجلى ذلك في استجابتنا لحالات الطوارئ الصحية في العالم، وفي ترويجنا لأهداف الوصول بالانبعاثات الحرارية إلى الصفر. لكن أكثر مجال يظهر فيه تميزنا في هذا الإطار هو الفضاء الإلكتروني.

فسواء كان الأمر يتعلق بتحقيق الفوائد الجمة التي يوفرها الفضاء الإلكتروني لمواطنينا واقتصادنا في سعينا للارتقاء بالمناطق الأقل حظا في بلدنا وتوحيده بالكامل، أو فيما يخص العمل مع شركائنا تجاه فضاء إلكتروني يعكس قيمنا الوطنية، أو في استخدام الطاقة القصوى لقدراتنا الإلكترونية للتأثير في الأحداث العالمية، فإن المملكة المتحدة ترى الفضاء الإلكتروني وسيلة لحماية والسعي وراء مصالحنا في ساحة عالمية تتخذ طابعا جديدا بفضل التكنولوجيا.

إن الاستراتيجية الإلكترونية الوطنية الجديدة هي خطتنا لضمان أن تظل المملكة المتحدة واثقة وقادرة وصامدة في هذا العالم الرقمي الذي يشهد تغيرات سريعة، وأن نستمر في التكيّف والابتكار والاستثمار لكي نحمي ونسعى وراء مصالحنا في الفضاء الإلكتروني.

ينطلق هذا الفصل التالي من حيث توقفت استراتيجيتنا الرائدة – الاستراتيجية الوطنية لأمن المعلوماتية لعام 2016. وهو يقودنا إلى مستقبل تكون فيه المملكة المتحدة أكثر صمودا في وجه الهجمات الإلكترونية. وبصفتي الوزير المسؤول، سأكون واضحا بشأن اثنين من الأهداف الرئيسية لتلك الاستراتيجية: أولا، ينبغي علينا أن نقوّي قدراتنا في مجال التقنيات الضرورية للفضاء الإلكتروني؛ وثانيا، أن علينا أن نحدّ من اعتمادنا على مورّدين فرديين، أو على تقنيات جرى تطويرها تحت أنظمة سياسية لا تشاركنا نفس القيم.

سيكون قطاع العلوم والتكنولوجيا البريطاني بمثابة القوة الدافعة لهذا التغيير، بما يضمن أن يستمر الفضاء الإلكتروني في كونه ذُخرا وطنيا اقتصاديا واستراتيجيا، وأن تكون قدراتنا التكنولوجية أكثر جدارة بالثقة وأكثر قدرة على صد طائفة واسعة من الأعداء الإلكترونيين الذين كانت قدراتهم، حتى الأمس القريب، حكرا على الدول.

لقد تعهدنا كحكومة بإنفاق 22 مليار جنيه إسترليني على البحث والتطوير، وبأن نضع قطاع التكنولوجيا في صميم خططنا للأمن القومي. ولقد رأينا جميعا قدرة التكنولوجيا الرقمية على إحداث التحوّل؛ لكننا رأينا أيضا، كما الحال بالنسبة لشبكة الجيل الخامس (5G)، أنها قادرة على التسبب بعراقيل. وستساعدنا خططنا بالنسبة للذكاء الاصطناعي وسياسة البيانات في ضمان أن نكون في طليعة التكنولوجيا الرقمية، كما إن الخطوات التي ستُتخذ ضمن إطار الاستراتيجية الإلكترونية ستضمن أن تكون لدينا الثقة بأمن وصمود المورّدين والشركاء.

وقد شكّل إنشاء القوة الوطنية لأمن المعلوماتية في العام الماضي خطوة هامة في قدراتنا الهجومية الإلكترونية.

لكن الأمن الإلكتروني الأساسي يظل محور جهودنا فيما نسعى لتقوية ردنا على من يهاجمون المملكة المتحدة ومواطنينا. كما ينصب تركيزنا أيضا على جعل القطاع العام أكثر صمودا، ومساعدة المجالس المحلية في حماية أنظمتها والبيانات الشخصية للمواطنين من برامج انتزاع الفدية وغيرها من الهجمات الإلكترونية.

على نطاق المجتمع، الفضاء الإلكتروني متاح للجميع. ومن خلال هذه الاستراتيجية، تسعى الحكومة لفعل المزيد لحماية مواطني المملكة المتحدة وشركاتها وشركائها الدوليين - بما يساعد على تحقيق رؤيتها بأن يكون الفضاء الإلكتروني مساحة قوية الصمود وموثوقة من أجل ازدهار أعمال الأفراد والشركات.

النائب ستيف باركلي
مستشار دوقية لانكستر،
وزير شؤون مجلس الوزراء

تمهيد

الفرص والتحديات في العصر الرقمي

1. إن التقدم السريع في مجال التكنولوجيا وما صاحبه من انخفاض في تكاليفها قد جعل العالم أكثر اتصالا ببعضه البعض من أي وقت مضى، وأتاح مجالا استثنائيا للفرص والابتكار والتطور. وقد أدى تفشي جائحة فيروس كورونا (كوفيد-19) لتسريع هذا التوجه، إلا أننا ما زلنا على الأرجح في المراحل الأولى من تحول هيكلي طويل الأمد. والتوسع العالمي في مجال الفضاء الإلكتروني يغير طريقة حياتنا وعملنا وتواصلنا، كما يُحدث تحوّلا في الأنظمة الحيوية التي نعتمد عليها في مجالات عدة، مثل قطاعات التمويل والطاقة وتوزيع الغذاء والرعاية الصحية والنقل. خلاصة القول، أصبح الفضاء الإلكتروني اليوم أحد المكونات الأساسية لأمننا وازدهارنا مستقبلا. ومن شأن ذلك أن يخلق فرصا استثنائية للدول المتقدمة تقنياً مثل المملكة المتحدة لكي تسعى لتحقيق أهدافها الوطنية بأساليب جديدة.

2. إن نطاق وسرعة هذا التغير - والذي يسير عادة بخطى أسرع من قوانيننا وأعرافنا الاجتماعية ومؤسساتنا الديمقراطية - يخلق أيضا تعقيدات واضطرابات وأخطاراً غير مسبوقة. وقد شهد العام الماضي هجمات إلكترونية على مستشفيات وأنابيب نفط ومدارس وشركات، والتي توقف بعضها بالكامل من جراء برامج انتزاع الفدية، كما جرى استخدام برامج تجارية للتجسس في استهداف النشطاء والصحفيين والسياسيين. وكون الفضاء الإلكتروني عابرا للدول بطبيعته يعني أنه لا يُمكن مجابهة تلك التحديات دون تضافر الجهود الدولية، فضلا عن أنه يشكّل أيضا ساحة ذات أهمية متزايدة للمنافسة العامة، وتضارب المصالح والقيم والرؤى المتنافسة بالنسبة لمستقبلنا على مستوى العالم.

رؤيتنا: قوة إلكترونية دعما للأهداف الوطنية

3. في هذا السياق، تزداد أهمية القوة الإلكترونية كداعم أساسي لقوتنا الوطنية وكمصدر للتفوق الاستراتيجي. **القوة الإلكترونية هي القدرة على حماية والسعي وراء مصالحنا ضمن الفضاء الإلكتروني ومن خلاله.** فالدول الأكثر قدرة على إدراك الفرص والتحديات التي يخلقها العصر الإلكتروني ستكون أكثر أمنا، وأكثر صمودا، وأكثر ازدهارا في المستقبل. وتُعتبر المملكة المتحدة إحدى دول العالم الأكثر تقدما في المجال الرقمي، ولدى الحكومة البريطانية برنامج تكنولوجي طموح، في الداخل وفي الخارج. ذلك يعني أننا معرضون بوجه خاص لتحديات الفضاء الإلكتروني، لكننا أيضا نتميز بمكانة فريدة للريادة في مجال اغتنام الفرص التي يتيحها لمصلحة مواطنينا، ولصالح البشرية عموما.

4. على مدى السنوات العشر القادمة ستصبح للإنترنت والتكنولوجيا الرقمية والبنية التحتية التي تدعمهما أهمية أكبر لمصالحنا ولمصالح حلفائنا وأعدائنا.
وفيما نؤسس دورا جديدا للمملكة المتحدة في عصر أكثر تنافسية، فإن تعزيز قدرتنا الإلكترونية سيمكننا من أن نكون في الطليعة على مستوى هذا القطاع والدول الأخرى، وأن نستبق التغيرات التكنولوجية مُستقبلا، ونقلل من التهديدات، ونكتسب تفوقا استراتيجيا على أعدائنا ومنافسينا. وذلك سيجعل المملكة المتحدة أحد الاقتصادات الرقمية الأكثر أمنا وجاذبية للعيش والعمل والاستثمار فيها.

5. تتلخص رؤيتنا بأن **المملكة المتحدة في عام 2030 سوف تستمر بكونها قوة إلكترونية مسؤولة وديمقراطية، قادرة على حماية والسعي وراء ضمن الفضاء الإلكتروني ومن خلاله دعما للأهداف الوطنية**:

- دولة أكثر أمنا وصمودا، وأفضل استعدادا لمواجهة التهديدات والأخطار المتزايدة، مع استخدام قدراتنا الإلكترونية لحماية مواطنينا ضد الجريمة والاحتيال والتهديدات من دول أخرى
- اقتصاد رقمي مبدع ومزدهر، مع توزيع أكثر عدلا للفرص في كافة أرجاء البلاد ولمُختلف فئات الشعب
- قوة عظمى في مجال العلوم والتكنولوجيا، تُسخّر التكنولوجيا التحويلية بشكل آمن لدعم مجتمع أفضل صحة وأكثر حفاظا على البيئة
- شريك أكثر نفوذا ويحظى بتقدير أكبر على الساحة العالمية، بحيث نساهم في رسم آفاق المستقبل لنظام دولي منفتح ومستقر، مع الحفاظ بنفس الوقت على حرية تحركنا في الفضاء الإلكتروني

6. على مدى العقد الماضي، رسّخنا مكانة المملكة المتحدة كقوة إلكترونية، وأسسنا قدرات متطورة في مجال الأمن الإلكتروني وعملياته، وطوّرنا قطاعا رائدا في مجال الأمن الإلكتروني. ترتكز هذه الاستراتيجية على التقدم الكبير الذي أحرزناه من خلال الاستراتيجية الوطنية لأمن المعلوماتية 2016 - 2021، والاستنتاجات الهامة الثلاث في المراجعة المتكاملة للأمن والدفاع والتنمية والسياسة الخارجية. أولا، أن القوة الإلكترونية للمملكة المتحدة في العصر الرقمي ستكون أداة أهم من أي وقت مضى لتحقيق أهدافنا الوطنية. وثانيا أن الحفاظ على قوتنا الإلكترونية يتطلب استراتيجية أكثر شمولا وتكاملا، تأخذ بعين الاعتبار كامل نطاق أهدافنا وقدراتنا الإلكترونية. وثالثا أنه يجب أن تكون هذه مقاربة تشمل المجتمع بأكمله - أي أن ما يحدث في غرف اجتماعات مجالس الإدارة أو في صفوف المدارس له نفس الأهمية بالنسبة لقوتنا الإلكترونية كأهمية الخطوات التي يتخذها الخبراء والفنيون والمسؤولون الحكوميون، وأن العمل بالشراكة مع الأخرين سيكون في غاية الأهمية لنجاحنا.


CHELTENHAM
Science
Festival
18.2 Cyber Skills

الدعامات الخمس لاستراتيجيتنا

7. وضعت المراجعة المتكاملة خمس "أولويات عمل" لهذه الاستراتيجية، وسوف نستخدم تلك الأولويات كدعامات لإطارنا الاستراتيجي، **والتي ستنظم وتوجه الخطوات المحددة التي سنتخذها والنتائج التي نعتزم تحقيقها بحلول 2025**:

- **الدعامة 1: تقوية البيئة الإلكترونية في المملكة المتحدة،** والاستثمار في إمكانات المواطنين وفي المهارات، وتعميق الشراكة بين الحكومة والجامعات وقطاع الفضاء الإلكتروني
- **الدعامة 2: جعل المملكة المتحدة دولة رقمية مزدهرة وقادرة على الصمود،** وبالتالي تقليل المخاطر الإلكترونية بحيث تتمكن الشركات من جني أكبر الفوائد الاقتصادية من التكنولوجيا الرقمية، ويكون المواطنون أكثر أمنا على الإنترنت وهم مطمئنون أن بياناتهم محمية
- **الدعامة 3: أخذ زمام القيادة في مجالات التكنولوجيا الضرورية للقوة الإلكترونية،** وبناء قدراتنا في قطاع التكنولوجيا، وتطوير أطر خاصة من أجل حماية تقنياتنا المستقبلية
- **الدعامة 4: تطوير الدور الريادي للمملكة المتحدة ونفوذها العالمي في جعل النظام العالمي أكثر أمنا وازدهارا وانفتاحا،** وذلك بالعمل مع الحكومة والشركاء في القطاع، وتشارك الخبرات التي ترتكز عليها القوة الإلكترونية للمملكة المتحدة
- **الدعامة 5: كشف أعدائنا وعرقلة خططهم وردعهم لتعزيز أمن المملكة المتحدة في الفضاء الإلكتروني ومن خلاله،** واستخدام كل إمكانات المملكة المتحدة بشكل أكثر تكاملا وإبداعا وبوتيرة أكبر

8. يحدد الجزء الأول من هذه الوثيقة السياق الاستراتيجي الذي نتحرك ضمنه، وأهداف استراتيجيتنا، والمقاربة الاستراتيجية التي سنتبناها على مدى العقد القادم. أما الجزء الثاني فيبين الخطوات المحددة التي سنتخذها من أجل تحقيق أهدافنا بحلول عام 2025، والتي جرى ترتيبها وفقا لهذه الدعامات الخمس.

الرؤية

ستظل المملكة المتحدة في عام 2030 قوة إلكترونية مسؤولة وديمقراطية رائدة، وقادرة على حماية والسعي وراء مصالحها في الفضاء الإلكتروني ومن خلاله دعما للأهداف الوطنية.

الدعامات والأهداف

الدعامة 1

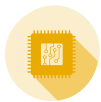
تقوية البيئة الإلكترونية في المملكة المتحدة

1. تقوية البُنى والشراكات والشبكات اللازمة لدعم مقاربة إلكترونية تشمل المجتمع بأكمله.
2. تعزيز وتوسيع نطاق المهارات الإلكترونية للدولة على كافة المستويات، بما في ذلك من خلال قطاع إلكتروني عالمي المستوى ومتنوع، والذي سيكون مصدر إلهام وإعداد للمواهب المستقبلية.
3. تعزيز قطاع أمن إلكتروني ومعلوماتي مُستدام ومبدع وقادر على المنافسة عالميا، وتقديم منتجات وخدمات عالية الجودة تلبي احتياجات الحكومة والبلد بصورة أعم.

الدعامة 2

جعل المملكة المتحدة دولة رقمية مزدهرة وقادرة على الصمود

1. تحسين القدرة على فهم الأخطار الإلكترونية من أجل اتخاذ خطوات أكثر فاعلية بشأن ضمان الأمن الإلكتروني والقدرة على الصمود.
2. إحباط ومقاومة الهجمات الإلكترونية بفاعلية أكبر من خلال تحسين إدارة المخاطر الإلكترونية في المؤسسات في المملكة المتحدة، وتوفير حماية أكبر للمواطنين.
3. تقوية القدرة على الصمود على المستويين الوطني والمؤسساتي من أجل الاستعداد للهجمات الإلكترونية والاستجابة لدى وقوعها والتعافي من أثرها.



الدعامة 3

أخذ زمام القيادة في مجالات التكنولوجيا الضرورية للقوة الإلكترونية

1. تحسين قدرتنا على توقع وتقييم التطورات العلمية والتكنولوجية ذات الأهمية القصوى لقوتنا الإلكترونية والتصرف على أساسها.
2. تعزيز والحفاظ على التفوق على مستوى الدولة ومع الشركاء في أمن التقنيات الضرورية للفضاء الإلكتروني.
3. توفير الجيل التالي من التقنيات والبنية التحتية المترابطة، وتقليل مخاطر الأمن الإلكتروني الناجمة عن الاعتماد على الأسواق العالمية، وضمان أن يتوفر للمستخدمين في المملكة المتحدة مصادر تقنيات متنوعة وموثوقة.
4. العمل مع أطراف معنية متعددة من أجل تطوير معايير تقنية رقمية عالمية في المجالات ذات الأولوية والأكثر أهمية من أجل الحفاظ على قيمنا الديمقراطية، وضمان أمننا الإلكتروني، وتعزيز التفوق الاستراتيجي للمملكة المتحدة من خلال العلوم والتكنولوجيا.
2أ. الحفاظ على نظام مفاتيح تشفير بيانات وطني بحيث يكون قويا وقادرا على الصمود، ويلبي احتياجات عملاء الحكومة البريطانية وشركائنا وحلفائنا، ويخفف بالشكل الملائم من أكبر المخاطر التي تهددنا، بما في ذلك خطر الهجمات من أعدائنا الأكثر تمكناً.

الدعامة 4

تطوير الدور الريادي للمملكة المتحدة ونفوذها العالمي

1. تقوية الأمن الإلكتروني والقدرة على الصمود لدى شركائنا الدوليين، ورفع وتيرة العمل الجماعي من أجل ردع الأعداء وتعطيل خططهم.
2. صياغة حوكمة عالمية لتطوير فضاء إلكتروني حر ومنفتح وسلمي وآمن.
3. استغلال وتصدير القدرات والخبرات الإلكترونية البريطانية من أجل تعزيز تفوقنا الاستراتيجي، والترويج بشكل أعمّ لسياستنا الخارجية ومصالحنا المتعلقة بازدهارنا.

الدعامة 5

كشف أعدائنا وعرقلة خططهم وردعهم

1. كشف فاعلين بالمجال الإلكتروني وأنشطتهم على مستوى الدول والمجرمين والأفراد وغيرهم من الفاعلين، وتبادل المعلومات مع الآخرين بشأنهم من أجل حماية المملكة المتحدة ومصالحها ومواطنيها.
2. ردع وتعطيل فاعلين بالمجال الإلكتروني وأنشطتهم على مستوى الدول، وكذلك المجرمين وغيرهم من الفاعلين الذين يستهدفون المملكة المتحدة ومصالحها ومواطنيها.
3. اتخاذ الخطوات اللازمة في الفضاء الإلكتروني ومن خلاله لدعم أمننا الوطني، والكشف عن الجرائم الخطيرة ومنع وقوعها.

مساندة الأهداف الوطنية

- الأمن والصمود
- قوة عظمى في العلوم والتكنولوجيا
- الازدهار الاقتصادي
- تشكيل النظام العالمي

الجزء 1:
الاستراتيجية

السياق الاستراتيجي

بريطانيا عالمية في عصر تنافسي

9. المراجعة المتكاملة للأمن والدفاع والتنمية والسياسة الخارجية، والتي نُشرت في مارس 2021، تستعرض رؤية الحكومة لدور المملكة المتحدة في العالم على مدى العقد القادم، والخطوات التي سنتخذها من الآن حتى عام 2025. ترى المراجعة أنه لكي تكون المملكة المتحدة مجهزة بشكل أفضل في عالم أكثر تنافسية، علينا أن نأخذ بنهج الابتكار في العلوم والتكنولوجيا لتعزيز ازدهارنا الوطني وتفوقنا الاستراتيجي. الاستراتيجية الإلكترونية الوطنية تستند إلى هذه المقاربة، ونشر هذه الاستراتيجية هو أحد الالتزامات ضمن هدف المراجعة الاستراتيجية المتكاملة من أجل "الحفاظ على التفوق الاستراتيجي من خلال العلوم والتكنولوجيا".

المشهد الإلكتروني

10. التحديات التي يمثلها الفضاء الإلكتروني بالنسبة للسياسات ليست تكنولوجية فحسب من حيث طبيعتها. فالمجال الإلكتروني بيئة من صنع الإنسان، ويبلوره أساساً السلوك البشري. وهو يجسّم ذلك السلوك بخيره وشره، ونشعر بتأثيراته عادة في العالم المادي. الفضاء الإلكتروني تملكه وتشغله شركات خاصة، وحكومات، ومؤسسات غير ربحية، ومواطنون أفراد، بل وحتى مجرمون. هذا يعني أن أي استجابة استراتيجية لهذا المضمون يجب أن تجمع ما بين الجانب الجيو-استراتيجي والأمن القومي، والعدالة الجنائية والتنظيمات المدنية، والسياسات الاقتصادية والصناعية. وتتطلب تلك الاستجابة فهما عميقا للمضامين الثقافية والاجتماعية المختلفة وأنظمة القيم المتفاعلة على شبكة الإنترنت.

11. كذلك الفضاء الإلكتروني يتجاوز الحدود الوطنية. حيث سلاسل توريد التكنولوجيا والموارد الحيوية الحساسة أصبحت عالمية بطابعها بشكل متزايد؛ ومرتكبو الجرائم الإلكترونية والفاعلون من الدول ينشطون من مختلف أنحاء العالم، وشركات التكنولوجيا القوية تصدّر منتجاتها وتضع المعايير لنفسها؛ بينما يجري تقرير القواعد والأعراف التي تضبط الفضاء الإلكتروني والإنترنت في منتديات دولية. كما إن الفضاء الإلكتروني يتغيّر بشكل مستمر مع تغيُّر التكنولوجيا وأساليب استخدام الناس لها، وذلك يتطلب منا تبني مقاربة مرنة وتستجيب لتلك المعطيات.

طبقات الفضاء الإلكتروني

ما هو الفضاء الإلكتروني؟

بالنسبة للعديد منا، الفضاء الإلكتروني هو العالم الافتراضي الذي نعيش فيه عندما ندخل على الإنترنت للتواصل مع الآخرين، وللعمل، ولتسيير مهامنا اليومية. وبتعبير فني، الفضاء الإلكتروني هو الشبكة المتداخلة من تكنولوجيا المعلومات التي تشمل الإنترنت، وشبكات الاتصالات اللاسلكية، وأنظمة الكمبيوتر، والأجهزة المتصلة بالإنترنت. أما بالنسبة للجانب العسكري، وعند النظر لجهودنا للتصدي للتهديدات في الفضاء الإلكتروني، فإن الفضاء الإلكتروني هو نطاق للعمليات، إلى جانب البر والبحر والجو والفضاء.

كيف هي تجربة الفضاء الإلكتروني؟ بحكم تعريفه، الفضاء الإلكتروني هو فضاء "مشترَك"، وبالنظر إلى تعقيده واتساع نطاقه، فإن تجربة كل شخص فيه فريدة بحد ذاتها. حيث يدخل الأفراد إلى الفضاء الإلكتروني عندما يطلعون على حساباتهم المصرفية على الإنترنت أو يشاهدون فيلما في المنزل. وتستخدم الشركات الفضاء الإلكتروني للربط بين موظفيها والموارد التي يحتاجون إليها، سواء كان ذلك للاطلاع على المعلومات أو التحكم بعمليات التصنيع. كما توفر الحكومات خدمات عامة لمواطنيها من خلال بوابات إلكترونية على الإنترنت. أما الخبراء بالمجال الإلكتروني، فيبحثون "خلف الكواليس" في التكنولوجيا والمعايير والبروتوكولات التي تجعل المجال الإلكتروني "يعمل" بالنسبة لمستخدميه. كل تلك المجموعات تستخدم الفضاء الإلكتروني بطرق مختلفة ولأغراض مختلفة، وقد أصبحنا جميعا نستفيد من استخدامه بشكل متزايد.

استخدامات الإنترنت

- حسابات البريد الإلكتروني
- حسابات الألعاب على الإنترنت
- حسابات التواصل الاجتماعي
- الدخول على الحسابات المصرفية
- بطاقات المواصلات التي تعمل باللمس
- أجهزة اللياقة الصحية الي يمكن ارتداؤها

البرمجيات والأنظمة والبيانات

- أنظمة المعلومات في الشركات
- قواعد البيانات، مثل سجلات سلطات الضرائب
- أنظمة التحكم الصناعي
- أنظمة التشغيل/ويندوز
- التطبيقات، مثل واتساب، وفيسبوك، وتيك توك
- لغات البرمجة، Python /C++

الأجهزة المادية والاتصالات

- الراوتر (router)، ومراكز الشبكات (hubs)
- الخوادم servers
- واي فاي وإيثرنت
- هوائيات اللاسلكي
- الثلاجات الذكية
- أجهزة قراءة بطاقات المواصلات
- الهواتف وأجهزة الكمبيوتر وغيرها من الأجهزة الشخصية

يُمكن توصيف الفضاء الإلكتروني على ثلاث مستويات:

افتراضي

هو الجزء من الفضاء الإلكتروني الذي يستخدمه غالبية الناس. وهو عبارة عن التعريف بالأفراد والمؤسسات بواسطة هويات افتراضية في فضاء افتراضي مشترك. التعريف الافتراضي يمكن أن يكون على شكل عنوان بريد إلكتروني، أو رمز التعريف بالمستخدم، أو حساب على وسائل التواصل الاجتماعي، أو اسم مستعار. ويُمكن أن يكون لفرد واحد، أو مؤسسة واحدة، عدة هويات على الإنترنت. وبالمقابل يمكن لعدد من الأفراد أو المؤسسات أيضا إنشاء هوية واحدة فقط يتشاركونها.

منطقي

هو الجزء من الفضاء الإلكتروني المكون من رموز أو بيانات، مثل أنظمة التشغيل والبروتوكولات والتطبيقات وبرمجيات أخرى. المستوى المنطقي لا يمكن أن يعمل دون المستوى المادي، وتنساب المعلومات فيه عبر الشبكات الموصولة أو الطيف الكهرومغناطيسي. المجال المنطقي، إلى جانب المجال المادي، يتيح للهويات الافتراضية التواصل والتفاعل فيما بينها.

مادي

المستوى المادي للفضاء الإلكتروني يشمل كافة الأجهزة التي يجري بث البيانات عليها، من الراوتر والأسلاك ومراكز الشبكات في المنزل وحتى أنظمة الاتصالات اللاسلكية المعقدة الضخمة التي تديرها شركات التكنولوجيا الكبرى. وإلى جانب البنية التحتية المادية، يشمل المستوى المادي أيضا الطيف الكهرومغناطيسي الذي تُبَث عليه البيانات مثل الواي فاي واللاسلكي.

القوة الإلكترونية

12. في صميم استراتيجيتنا مفهوم القوة الإلكترونية، والذي نعرّفه بأنه قدرة الدولة على حماية والسعي وراء مصالحها في الفضاء الإلكتروني ومن خلاله. ونحن نحدد هنا خمسة أبعاد واسعة النطاق للقوة الإلكترونية والتي تتسق مع دعامات هذه الاستراتيجية، وهي:

- الأفراد والمعرفة والمهارات والهياكل والشراكات التي تشكّل الأساس لقوتنا الإلكترونية، والتي ترتكز عليها كافة المكونات الأخرى وتدمجها في مقاربة وطنية
- القدرة على حماية مواردنا من خلال الأمن الإلكتروني والصمود من أجل تحقيق المنافع الكاملة التي يوفرها الفضاء الإلكتروني لمواطنينا واقتصادنا
- القدرات التقنية وقدرات القطاع للحفاظ على دورنا في تطوير التقنيات الإلكترونية الهامة، واستخدام التقنيات الجديدة لخدمة مصالح مجتمعنا
- التأثيرات والعلاقات والمعايير الأخلاقية العالمية اللازمة لوضع القواعد والقوانين للفضاء الإلكتروني بما ينسجم مع قيمنا ومصالحنا ويدعم الأمن والاستقرار الدوليين
- القدرة على العمل ضمن الفضاء الإلكتروني ومن خلاله لدعم الأمن القومي، والرخاء الاقتصادي، ومنع الجريمة. ذلك يشمل العمليات الإلكترونية لإحداث تأثير عالمي فعلي، والمساهمة في تحقيق التفوق الاستراتيجي، وعمليات إنفاذ القانون وتفعيل العقوبات الإلكترونية من أجل تقديم مرتكبي الجرائم الإلكترونية للعدالة وإحباط أنشطتهم.

13. القوة الإلكترونية تختلف عن أشكال القوة الأخرى التقليدية. حيث إنها تنطوي على المزج الكامل للقدرات الصلبة وعوامل التأثير الناعمة. وهي موزعة على نطاق أوسع، ويتعين على الحكومات أن تعمل مع الشركاء لكي تظفر بها وتمارسها. كما إن وتيرة التغير التكنولوجي تعني أنه يُمكن اكتساب القوة الإلكترونية وفقدانها بشكل أسرع، حيث القدرات التي كانت تعتبر حديثة في السابق يبطل استعمالها بفعل تطور التقنيات الجديدة.

14. تعكس استراتيجيتنا تلك الجوانب، إذ أنها تشرح كيف سنعمل مع شركائنا كلما أمكن كجزء من جهود تشمل المجتمع بأكمله. وسوف نفعل المزيد لمعالجة المشاكل من أساسها ونجد حلولا لجذور أسبابها، ولتوقع التوجهات المستقبلية، ووضع استجابات طويلة الأمد لها، ولكي نكون أكثر فاعلية في رسم معالم البيئة الجيوسياسية لا أن نكتفي بالاستجابة لتحدياتها.

المملكة المتحدة كقوة إلكترونية اليوم

15. تُعتبر المملكة المتحدة بالفعل قوة إلكترونية رائدة.[1] وقد بذلت الحكومة على مدى العقد المنصرم جهودا وطنية متواصلة لتقوية الأمن الإلكتروني في المملكة المتحدة، ولرفع درجة وعي عامة الناس بالأخطار الإلكترونية، وتنمية قطاع الأمن الإلكتروني، وتطوير قدرات واسعة النطاق في الفضاء الإلكتروني للاستجابة للتهديدات من الفاعلين المُعادين لنا. وفي حين أننا قد حققنا تقدما هائلا وأوجدنا لنفسنا مكانة قوية، فما زلنا نواجه تحديات كبيرة في الدعامات الخمس لهذه الاستراتيجية.

[1] تحتل المملكة المتحدة المرتبة الثانية على مؤشر الأمن الإلكتروني العالمي للاتحاد الدولي للاتصالات، وتأتي في المرتبة الثالثة على مؤشر القوى الإلكترونية لمركز هارفارد بلفر Harvard Belfer، وعلى الدرجة الثانية في تقييم قدرات القوى الإلكترونية الصادر عن المعهد الدولي للدراسات الاستراتيجية.

البيئة الإلكترونية والريادة التكنولوجية للمملكة المتحدة

16. شملت مقاربة المملكة المتحدة إزاء بناء قوتها الإلكترونية جهودا متضافرة لتطوير قاعدة المهارات الإلكترونية والقدرات التجارية في البلاد، حيث تعمل الحكومة البريطانية والحكومات المفوضة في إيرلندا الشمالية واسكتلندا وويلز بالتشارك معا وتتعلم من بعضها البعض. قطاع الأمن الإلكتروني في المملكة المتحدة يشهد نموا سريعا، ويضم ما يزيد عن 1400 شركة درّت دخلا قدره 8.9 مليار جنيه إسترليني العام الماضي، وتوفّر 46,700 وظيفة تتطلب مهارات عالية، وهي تجتذب استثمارات كبيرة من الخارج. يُعتبر هذا القطاع بالغ الأهمية لقوتنا الإلكترونية، فهو يدعم أمننا ونفوذنا الدولي ونمونا الاقتصادي. ولقد رسّخنا سمعة المملكة المتحدة كدولة رائدة عالميا في أبحاث الأمن الإلكتروني، حيث يتولى 19 مركزا أكاديميا مرموقا، إلى جانب 4 معاهد بحثية، معالجة التحديات الملحة التي تواجه أمننا الإلكتروني.

17. نمت قوة العمل في قطاع الأمن الإلكتروني بحوالي 50% في السنوات الأربع الأخيرة، وكان الطلب على المهارات عادة يفوق المعروض منها. وقد تواصلنا بشكل واسع مع هذا القطاع والمؤسسات المهنية والطلبة والأكاديميين وجهات العمل والمحترفين الحاليين بمجال الأمن الإلكتروني من أجل الوصول لفهم أفضل لطبيعة التحديات في مجال مهارات الأمن الإلكتروني. كما قدمنا مبادرات واسعة النطاق خارج المناهج الدراسية من أجل تشجيع الشباب على الانخراط في مهنة الأمن الإلكتروني. وفي الفترة من 2019 إلى 2020 أشركنا قرابة 57,000 من الشباب في برامجنا التعليمية CyberFirst وأيضا CyberDiscovery. وقد توسعنا في نطاق هذه الدورات لكي تشمل الطلاب الأصغر سنا، وكانت مسابقة CyberFirst Girls على الإنترنت قد اجتذبت 11,900 فتاة، وتنافست الفرق الأقوى في 18 موقعا في مختلف أنحاء المملكة المتحدة بنفس الوقت. كما اجتذب برنامج المنح الدراسية CyberFirst طلابا جامعيين موهوبين ومتحمسين. وفي العام الماضي كان هناك 750 طالبا مدرجا في هذا البرنامج، وقد حصل جميع الخريجين، وعددهم 56، على وظائف بدوام كامل في مجالات الأمن الإلكتروني.

18. على الرغم من هذه المبادرات، لا يزال توفر المهارات يشكّل تحديا ضخما لحوالي 1.32 مليون شركة عاملة في الاقتصاد بشكل عام، وقرابة 50% من تلك الشركات ما زالت تشكو من نقص في المهارات الفنية بمجال الأمن الإلكتروني.[2] ورغم أن قطاع الأمن الإلكتروني في المملكة المتحدة قد نما بشكل سريع، فإن معظم شركاته هي شركات ناشئة، ولا يزال تأسيس شبكة واسعة النطاق لتوفير السلع والخدمات لهذا القطاع يشكل صعوبة أمام اندماج الشركات على المستوى العالمي. وكما أظهرت التجربة مع شبكة الجيل الخامس 5G، فإن المملكة المتحدة وحلفاءها ليسوا في موقع ريادي في بعض مجالات قطاع التكنولوجيا الأوسع نطاقا. والدول التي بمقدورها الاضطلاع بدور قيادي في التقنيات الضرورية للقوة الإلكترونية ستكون بمكانة أفضل للتأثير في طريقة تصميم واستخدام تلك التقنيات، وستكون أكثر قدرة على حماية أمنها وتفوقها الاقتصادي، وأسرع في استغلالها الفرص في حال حدوث اختراقات علمية في مجال القدرات الإلكترونية.

الصمود الإلكتروني للمملكة المتحدة

19. على مدى العقد الماضي أطلقنا العديد من المبادرات المتنوعة التي تهدف لتقوية صمود المملكة المتحدة الإلكتروني. وقد تمكنا من ذلك بفضل الاستثمارات الكبيرة والمستمرة في بعض القدرات الإلكترونية الأساسية، ومنها المركز الوطني لأمن المعلوماتية، ومؤسسات تنفيذ القانون، وخبراؤنا المختصون في الأمن والسياسات في كافة قطاعات الحكومة، وكذلك شراكاتنا الواسعة محليا ودوليا.

[2] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة، مهارات الأمن الإلكتروني في سوق العمل في المملكة المتحدة 2021 (2021)

20. جهودنا الأكثر ابتكارا وتطورا كانت في اتخاذ خطوات واسعة النطاق، بما في ذلك من خلال تطوير برنامج تعزيز الدفاعات الإلكترونية والتوسع في تطبيقه. وقد تمكّن البرنامج في العام الماضي من إحباط 2.3 مليون هجمة خبيثة، ومنها 442 حالة تصيّد (phishing) باستخدام شعار الهيئة الوطنية للخدمات الصحية (NHS)، إلى جانب 80 تطبيقا غير قانوني باسم الهيئة الوطنية للخدمات الصحية متاحاً للتنزيل من خارج المتاجر الرسمية للتطبيقات.[3] كما لعبنا دورا رياديا على المستوى العالمي في الدفع نحو جعل المنتجات الاستهلاكية القابلة للاتصال بالإنترنت "آمنة بأساس التصميم"، وفي تطوير مدوّنة قواعد ممارسات للمملكة المتحدة في 2018 والتي جعلت الآخرين يحذون حذوها، وشكّلت أول معيار صناعي قابل للتطبيق على مستوى العالم بشأن أجهزة المستهلكين التي تتصل بالإنترنت.[4] [5]

21. كان للوائح الجديدة تأثير إيجابي على الأمن الإلكتروني، حيث أفادت 82% من المؤسسات أن التحسينات التي أدخلتها كانت نتيجة لبدء العمل بلوائح حماية البيانات العامة في المملكة المتحدة لعام 2018.[6] كما إن 77% من الشركات أصبحت الآن تعتبر الأمن الإلكتروني أولوية قصوى، ويمثل ذلك زيادة قدارها 12% منذ سنة 2016.[7] كذلك فإن بدء العمل باللوائح بشأن الشبكات وأنظمة المعلومات في 2018 أدى إلى أن تتخذ المؤسسات التي لها أهمية حيوية إجراءات لضمان أمن شبكاتها وأنظمة معلوماتها، وهذا بدوره أدى إلى انخفاض المخاطر الإلكترونية التي تواجهها الخدمات الرئيسية والخدمات الرقمية الهامة.[8] ومن الأمثلة الجيدة على تضافر الجهود بين الحكومات الأربع في المملكة المتحدة كانت التحسينات التي أدخلتها على مُجمل القطاع الصحي، بما في ذلك تطبيق اللوائح بشأن الشبكات وأنظمة المعلومات.

22. قدمنا مشورة وإرشادات شاملة بشأن الأمن الإلكتروني إلى المؤسسات العاملة في الاقتصاد، كما وفرنا دعما مخصصا حسب الحاجة للقطاعات الحساسة خلال فترة تفشي جائحة فيروس كورونا (كوفيد-19). أما بالنسبة لعامة الجمهور، فإن حملة التوعية بالأمن الإلكتروني التي أطلقناها وفرت المشورة بشأن الخطوات التي يمكن للأفراد أن يتخذوها لحماية أنفسهم على الإنترنت. وعندما وقعت هجمات إلكترونية، استخدمنا ما لدينا من قدرات عالمية المستوى للاستجابة لتلك الحوادث من أجل توفير دعم مباشر للحالات الأكثر خطورة. كما إن استثمارنا في خبراء إنفاذ القانون المحليين يعني أننا نستجيب لكل حادثة إلكترونية تقع اليوم.

23. أنشأنا وحدات إلكترونية من المتخصصين في إنفاذ القانون في مختلف أرجاء المملكة المتحدة، بالإضافة إلى شبكة الحماية الإلكترونية PROTECT، ووحدة رعاية ضحايا الجرائم الاقتصادية، والمراكز الإقليمية للصمود الإلكتروني. وبالنسبة للأفراد والمؤسسات الصغيرة ومتوسطة الحجم، تعني تلك المبادرات أنه يوجد أحد ما في مكان قريب، أو يمكن الاتصال به بسهولة، لديه المهارات والمعرفة المحلية لتقديم الدعم والإرشاد لتحسين الصمود الإلكتروني لمن يحتاجه.

24. إلا أنه لدينا أدلة متزايدة عن وجود ثغرات في صمودنا على المستوى الوطني، حيث هناك ارتفاع متزايد في مستويات الجرائم والانتهاكات الإلكترونية التي تؤثر على أعمال الحكومة والشركات والأفراد، وكذلك الجرائم التي تُستخدم فيها القدرات الإلكترونية كالاحتيال.[9] [10] وأصبحت أنظمة تكنولوجيا المعلومات القديمة، ونقاط الضعف في سلاسل التوريد، ونقص المتخصصين بالأمن الإلكتروني تشكل جميعها مصدر قلق متزايد. فقد أبلغت 4 من كل 10 شركات (39%) و26% من الهيئات الخيرية عن انتهاكات لأمنها الإلكتروني أو تعرضها لهجمات في العام الماضي، كما

---

[3] المركز الوطني لأمن المعلوماتية: المراجعة السنوية 2021 (2021)

[4] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة، مدونة الممارسات لأمن إنترنت الأشياء للمستهلكين (2018)

[5] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة DCMS، المعايير الصناعية بناء على مدونة الممارسات في المعهد الأوروبي لمعايير الاتصالات السلكية واللاسلكية (2019)

[6] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة/ RSM، تأثير لوائح حماية البيانات العامة GDPR على مخرجات الأمن الإلكتروني (2020): لوائح حماية البيانات العامة، والتي بدأ تطبيقها ضمن القانون البريطاني في عام 2018 قد حل محلها الآن أحكام بديلة خاصة بالمملكة المتحدة.

[7] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة، استطلاع حول انتهاكات الأمن الإلكتروني 2021 (2021)

[8] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة، مراجعة ما بعد تطبيق اللوائح بشأن الشبكات وأنظمة المعلومات 2018 (2020)

[9] جرى تعريفه كمخالفة لقانون إساءة استخدام الكمبيوتر

[10] المكتب الوطني للإحصاء، الجريمة في إنجلترا وويلز: السنة المنتهية في يونيو 2021 (2021)

إن العديد من المؤسسات (خاصة الشركات الصغيرة والمتوسطة) تفتقر إلى القدرة على حماية نفسها والاستجابة للحوادث.[11] ونعلم من مصادر في هذا القطاع أن العديد من تلك المؤسسات لا تدرك المخاطر الإلكترونية التي تواجهها، وأن الحوافز التجارية للاستثمار في الأمن الإلكتروني ليست واضحة، وأنه غالبا لا يكون لدى المؤسسات الدافع الكافي للإبلاغ عن الانتهاكات والهجمات الإلكترونية.

ريادة المملكة المتحدة وتأثيرها العالمي

25. تلقى خبرات المملكة المتحدة في المجال الإلكتروني تقديرا عاليا على المستوى العالمي من قبل شركائنا. وقد لعبت المملكة دورا بالغ الأهمية في زيادة القدرات الدولية، وفي العزم على مواجهة النشاطات الإلكترونية الخبيثة. وذلك عزز الاستخدام المسؤول لقدراتنا الإلكترونية الهجومية المنسجمة مع كل من القوانين البريطانية والدولية، ومع مواقفنا المُعلنة، خلافا للأنشطة العشوائية لبعض من أعدائنا.

26. خلال فترة رئاستنا لمجموعة الكومنولث، وضعت المملكة المتحدة الإعلان الإلكتروني لمجموعة الكومنولث وقادت الجهود لتطبيقه. هذا الإعلان كان التزاما مشتركا تجاه أمننا وازدهارنا وقيمنا في الفضاء الإلكتروني. وقد عززت الشبكة العالمية للوكالة الوطنية لمكافحة الجريمة من شراكاتنا الخارجية فيما يخص تطبيق القوانين المتعلقة بالمجال الإلكتروني بالاعتماد على العلاقات التي طورناها عبر تاريخ طويل من التعاون في مجال الاستجابة العملياتية. كما رفعت المملكة المتحدة من أعداد موظفي الأمن الإلكتروني والتكنولوجي في شبكتها الخارجية في كافة القارات الخمس، وشرعت في بناء القدرات في 100 بلد من أجل تنمية الصمود وتعزيز تأثير المملكة المتحدة ونشر قيمها.

27. أنشأ برنامج "سفير الأمن الإلكتروني" علاقات طويلة الأمد، وساعد الشركات البريطانية في الحصول على عقود دولية كبرى. وكانت المبادرات التنموية الدولية للمملكة المتحدة، مثل برنامج توفير الخدمات الرقمية للجميع، قد تعاونت بنجاح مع دول شريكة في أفريقيا وآسيا وأمريكا اللاتينية من خلال تقديم المشورة الفنية لتعزيز قدرات الأمن الإلكتروني لحكومات تلك الدول ولقطاع الشركات وللمستخدمين - بما في ذلك من خلال تحسين مهارات الممارسات الإلكترونية السليمة في المجتمعات التي لا تتوفر فيها خدمات جيدة من أجل تمكين الجهات الأكثر عرضة للأخطار الإلكترونية من حماية نفسها من الأخطار والتحديات التي تواجهها على الإنترنت.

28. إلا أننا نواجه منافسة دولية، حيث إن المنافسين الأساسيين مثل الصين وروسيا يواصلون الدعوة إلى سيادة وطنية أكبر على الفضاء الإلكتروني كأحد الحلول للتحديات الأمنية. إن الحرية على الإنترنت تتراجع على المستوى العالمي، كما إن مفهوم الإنترنت كفضاء مشترك يدعم تبادل المعرفة والبضائع بين المجتمعات المنفتحة أصبح معرضا للخطر.

[11] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة، استطلاع حول انتهاكات الأمن الإلكتروني 2021 (2021)

التصدي للتهديدات الإلكترونية للمملكة المتحدة وردع أعدائنا

29. التهديدات التي نواجهها في الفضاء الإلكتروني ومن خلاله ازدادت كثافة وحدّة وتعقيداً في السنوات الأخيرة. والهجمات الإلكترونية ضد المملكة المتحدة تنفذها مجموعة متنامية من الفاعلين من الدول، والجماعات الإجرامية (والتي تعمل أحيانا بتوجيه من دول أخرى أو بموافقتها الضمنية)، والنشطاء الذين يعملون لأغراض التجسس وتحقيق المكاسب التجارية والتخريب والتضليل الإعلامي. هذه الهجمات تسبب خسائر مالية فادحة، وسرقة الملكية الفكرية، وتوترا نفسيا شديدا، وانقطاعا للخدمات والموارد، ومخاطر لبنيتنا التحتية الوطنية الحيوية ومؤسساتنا الديمقراطية ووسائل إعلامنا. كما يمكنها أن تلحق الضرر بثقة المستثمرين والمستهلكين، وأن تزيد من حالات عدم المساواة والتضرر. وخلال فترة جائحة كوفيد-19 تعاظمت درجة العنف القائم على التحيز الجنسي من خلال الهجمات على الإنترنت. وهجمات برامج انتزاع الفدية مستمرة في كونها أكثر تعقيدا وتسبب ضرراً أكبر. وفي حين أن المستوى الإجمالي للتهديدات الإلكترونية من الفاعلين المعادين خلال فترة جائحة كوفيد-19 قد ظل ثابتاً، إلا أنهم استغلوا ذلك كفرصة وحولوا عملياتهم الإلكترونية للتركيز على سرقة اللقاحات والأبحاث العلمية، ولتقويض دول أخرى تعاني أصلاً من الأزمة. كذلك فإن الاعتماد المتزايد على التقنيات الرقمية من أجل العمل عن بُعد وإجراء تعاملات على الإنترنت قد زاد من درجة التعرض للأخطار. وإلى جانب ذلك، فإن الفجوة في مهارات استخدام التكنولوجيا الرقمية خلقت أيضا خللا في نسبة الحصول على الخدمات عبر الإنترنت، وعرّضت الناس للاستغلال والضرر على الإنترنت نتيجة ضعف معلوماتهم الرقمية وقلة وعيهم بإجراءات الأمن الإلكتروني التي يمكننا جميعا أن نتخذها لنحمي أنفسنا على الإنترنت.[12]

30. اتخذت الحكومة الخطوات اللازمة للتصدي لتلك التهديدات المتنامية. فالارتفاع الكبير في الاستثمار في قدراتنا المخابراتية أدى إلى زيادة فهمنا للتهديدات، ومكّننا من تنفيذ المزيد من الحملات السرية المضادة الفعالة. وقد طورنا استجابة متكاملة بشأن إنفاذ القانون إزاء الجرائم الإلكترونية، تحت قيادة الوكالة الوطنية لمكافحة الجريمة، وخصصنا فرقا إلكترونية داخل الوحدات الإقليمية لمكافحة الجريمة المنظّمة وقوات الشرطة المحلية في كل من إنجلترا وويلز وإيرلندا الشمالية واسكتلندا. وقد عزز ذلك من تفوقنا العملياتي والاستقصائي على مرتكبي الجرائم الإلكترونية وغيرهم من الأعداء. كما تعمل الحكومة على تقوية أمن العدد المتزايد من حلول الهوية الرقمية عن طريق تطوير إطار الثقة المتعلق بالهوية الرقمية والخصائص للمملكة المتحدة.[13] وسيساهم ذلك أيضا في معالجة الجرائم التي تتضمن إساءة استخدام بيانات الهوية. كما إن برنامج الخيارات الإلكترونية للوكالة الوطنية لمكافحة الجريمة يساعد الناس على أن يبنوا خياراتهم على معلومات صحيحة، ويبعدهم عن الجوانب الإجرامية لكي يستخدموا مهاراتهم الإلكترونية بطريقة إيجابية ومشروعة.

31. استثمرنا بشكل كبير في قدراتنا الهجومية الإلكترونية، وذلك أولا من خلال البرنامج الوطني للهجمات الإلكترونية، ومؤخرا من خلال إنشاء القوة الوطنية لأمن المعلوماتية. تستقطب هذه القوة فرقة العاملين فيها من القيادة الحكومية المركزية للاتصالات، ومن وزارة الدفاع، ومن المخابرات الخارجية (التي تُعرف أيضا باسم MI6)، ومختبر العلوم والتكنولوجيا الدفاعية، وذلك تحت قيادة موحّدة للمرة الأولى. تعمل تلك القوة ضمن الفضاء الإلكتروني ومن خلاله للحفاظ على سلامة الدولة، ولخدمة مصالح المملكة المتحدة في الداخل والخارج.

[12] المركز الوطني لأمن المعلوماتية، الوعي الإلكتروني CyberAware

[13] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة، إطار الثقة المتعلق بالهوية الرقمية والخصائص للمملكة المتحدة (2021)

32. من خلال التنسيق مع حلفائنا، عملنا أيضا على رفع التكلفة التي يتكبدها مرتكبو النشاط العدائي الذي ترعاه الدول في الفضاء الإلكتروني عن طريق التعرف على الأطراف التي تنفّذ الهجوم - مثلما فعلنا في الهجوم الأخير الذي حصل على منصة SolarWinds وخوادم Microsoft Exchange - ومحاسبة المسؤولين عن الهجوم. كما إن تطوير نظام مستقل للعقوبات الإلكترونية في المملكة المتحدة قد أضاف أداة تعطيل أخرى استخدمناها في الاستجابة لحوادث إلكترونية، كما في حالة هجوم WannaCry وهجوم NotPetya.
لكن رغم كل ذلك، فإن أسلوبنا في الردع الإلكتروني لا يبدو أنه قد أفلح بعد في جعل المهاجمين يغيرون حساباتهم للمخاطر بشكل جوهري. نعطي أدناه بعض الأمثلة الحديثة عن الهجمات الإلكترونية الكبيرة.

دراسات حالة حول هجمات إلكترونية وقعت مؤخرا

خلال عام 2021، واصلت المملكة المتحدة العمل مع شركائها الدوليين للكشف عن الأخطار المشتركة وإحباطها، وكانت غالبية الأخطار المستمرة تأتي من روسيا والصين. وبالإضافة إلى التهديدات المباشرة للأمن الإلكتروني التي مصدرها الدولة الروسية، أصبح واضحا أن العديد من عصابات الجريمة المنظّمة التي تشن هجمات باستخدام برامج انتزاع الفدية ضد أهداف غربية تتخذ من روسيا مقرا لها. كذلك تظل الصين فاعلا بالغ الحنكة في الفضاء الإلكتروني، ولديها طموحات متزايدة لفرض نفوذها خارج نطاق حدودها، كما إن لها اهتمامات مؤكدة في الأسرار التجارية للمملكة المتحدة. وسيكون الدافع الأوحد والأكبر لتطوير الأمن الإلكتروني للمملكة المتحدة مستقبلا هو معرفة كيف ستطور الصين نشاطها في العقد القادم. ورغم أن إيران وكوريا الشمالية أقل حنكة من روسيا والصين، إلا أنهما آخذتان في استخدام الهجمات الرقمية لتحقيق غاياتهما، بما في ذلك عن طريق السرقة والتخريب.

استخدام مرتكبي الجرائم الإلكترونية لبرامج انتزاع الفدية في مهاجمة قطاع الخدمات العامة

أصبحت برامج انتزاع الفدية أكبر تهديد إلكتروني واجهته المملكة المتحدة في عام 2021. ونظرا للتأثير المحتمل لهجوم ناجح على الخدمات الرئيسية أو البنية التحتية الوطنية الحيوية، رأى المركز الوطني لأمن المعلوماتية أن برامج انتزاع الفدية لا تقل ضررا عن عمليات التجسس التي ترعاها الدول.[14]

ففي أكتوبر 2020، تعرّض مجلس بلدية هاكني لهجوم ببرنامج انتزاع الفدية، والذي تسبب بتعطيل عمل المجلس لشهور عديدة، فيما كلّف إصلاح الأضرار ملايين الجنيهات الاسترلينية. وخلال الوقت الحساس الذي كان فيه المجلس يتعامل مع تأثيرات كوفيد-19، حُجبت عنه بيانات هامة وتعطل العديد من خدماته، بما في ذلك خدمات دفع المزايا الاجتماعية والضرائب. كما تعرضت هيئات محلية أخرى لهجمات مماثلة، وكذلك العديد من المؤسسات في قطاع التعليم.

[14] المركز الوطني لأمن المعلوماتية، تخفيف أثر هجمات البرامج الضارة وبرامج انتزاع الفدية (2021)

وفي مايو 2021 تسبب هجوم ببرنامج انتزاع الفدية على الجهاز التنفيذي للخدمات الصحية الإيرلندية في تعطيل شبكات تكنولوجيا المعلومات في جهاز الرعاية الصحية الإيرلندية والمستشفيات لما يزيد عن 10 أيام، ما أدى إلى نتائج ضارة للمرضى وعائلاتهم. كما نُشر بعض بيانات المرضى المسروقة على الإنترنت. وقد لجأ الجهاز التنفيذي للخدمات الصحية الإيرلندية، والذي يقدم خدمات الرعاية الصحية والاجتماعية في إيرلندا، إلى إغلاق شبكاته الوطنية والإقليمية بنفس اليوم لاحتواء الحادث. كذلك جرى اكتشاف نشاطات إلكترونية خبيثة على شبكة وزارة الصحة الإيرلندية، لكن نظرا لاستخدام أدوات إلكترونية خلال عملية التحقيق، تم الكشف عن محاولة استخدام برنامج طلب فدية وايقافه. كما كان لهذا الهجوم تأثير على إيرلندا الشمالية، حيث أعاق القدرة على الاطلاع على البيانات التي يحتفظ بها الجهاز التنفيذي للخدمات الصحية الإيرلندية لبعض خدمات المرضى خارج الحدود.

لكن من المهم الإشارة أنه لم تُدفع فدية في أي من الحالتين. **إن أجهزة إنفاذ القانون لا تشجع ولا توافق على ولا تتقبل طلبات دفع الفدية. ففي حال دفعت فدية:**

- **ليس هناك ضمان أنه سيمكنك استرجاع بياناتك أو الدخول إلى جهاز الكمبيوتر**
- **سيظل جهازك مصابا بالفيروس**
- **ستكون قد دفعت الأموال لمجرمين**
- **على الأغلب سوف يستهدفك المجرمون ثانية في المستقبل**

ينشر المركز الوطني لأمن المعلوماتية دليلا إرشاديا حول كيفية دفاع المؤسسات عن نفسها ضد هجمات البرامج الضارة أو برامج طلب الفدية. ويشمل ذلك كيفية الاستعداد لحادث إلكتروني، والخطوات التي يجب اتخاذها في حال أصيبت مؤسسة بفيروس.

استغلال الدول لنقاط الضعف الاستراتيجية وسلاسل التوريد

إن الضرر الذي لحق بشركة البرمجيات SolarWinds واستغلال خوادم Microsoft Exchange قد سلط الضوء على مخاطر الهجمات التي تأتي من سلاسل التوريد. هذه الهجمات المعقدة، والتي استهدف فيها الفاعلون عناصر أقل أمنا - مثل مقدمي الخدمات المُدارة أو منصات البرمجيات التجارية - في سلاسل التوريد للمؤسسات الاقتصادية والحكومية والأمنية، كانت من أخطر الهجمات الإلكترونية التي شهدها المركز الوطني لأمن المعلوماتية.

ففي مطلع ديسمبر 2020، اكتشفت شركة الأمن الإلكتروني الأمريكية FireEye أن أحد المهاجمين قد تمكن من إدخال تعديل ضار على أحد المنتجات التي تستخدمها هذه الشركة والعديد من المؤسسات غيرها حول العالم. أتاح ذلك التعديل للمهاجم أن يرسل أوامر على مستوى مدير البرنامج لأي جهاز مصاب بالفيروس من ذلك المنتج، والذي يمكن استخدامه لتوجيه المزيد من الهجمات على الأنظمة المتصلة به. وقد جرى تنفيذ الهجوم الأولي على سلسلة التوريد من خلال برنامج اسمه أوريون Orion، وهي أداة لمراقبة شبكة تكنولوجيا المعلومات طورتها شركة **SolarWinds**. وتمكن المهاجم من زرع رمز خبيث في ملف محدّث للبرنامج يعود تاريخه إلى مارس 2020. وفي إبريل 2021، كشف المركز الوطني لأمن المعلوماتية بالاشتراك مع نظرائه في الولايات المتحدة للمرة الأولى أن المخابرات الخارجية الروسية هي التي تقف خلف ذلك الهجوم - والذي كان أحد أخطر الهجمات الإلكترونية في السنوات الأخيرة.[15] وقد أكدت شركة SolarWinds أن 18,000 مؤسسة في مختلف أرجاء العالم، بما فيها وزارات في الحكومة الأمريكية، قد تضررت من ذلك الهجوم. كان ذلك الحادث جزءا من نموذج أوسع انتشارا للهجمات الإلكترونية التي تنفذها المخابرات الخارجية الروسية، والتي حاولت سابقا أن تدخل إلى شبكات تكنولوجيا المعلومات للدول الأعضاء في حلف الناتو وحكومات في مختلف أرجاء أوروبا.

[15] وزارة الخارجية والكومنويلث والتنمية البريطانية، روسيا: المملكة المتحدة والولايات المتحدة تكشفان حملة عالمية من النشاطات الخبيثة تنفذها المخابرات الروسية (2021)

وفي 2 مارس 2021 أعلنت شركة مايكروسوفت أن بعض الفاعلين الماهرين قد هاجموا عددا من خوادم **Microsoft Exchange** التي تستخدمها مؤسسات في مختلف أرجاء العالم لإدارة بريدها الإلكتروني وترتيب المواعيد، وفي التعاون مع الآخرين. وحسب تقدير مايكروسوفت، الهجمات الأولية بدأت في يناير 2021 وكانت برعاية الحكومة الصينية. وردا على ذلك، أطلقت مايكروسوفت العديد من التحديثات الأمنية للخوادم المصابة بالفيروس. وفي يوليو 2021 انضمت المملكة المتحدة إلى شركاء يشاطرونها القيم في تأكيد أن فاعلين تدعمهم الحكومة الصينية هم المسؤولون عن الهجمات التي ألحقت الضرر بما يزيد عن ربع مليون من الخوادم في مختلف أرجاء العالم.[16] وهناك احتمال كبير أن يكون الهجوم قد أتاح المجال لعملية تجسس واسعة النطاق، بما في ذلك الحصول على معلومات شخصية عن الأفراد وملكيات فكرية. كان الهجوم على خوادم Microsoft Exchange قد أعطى المهاجم موطئ قدم للتوغل أكثر داخل شبكات المعلومات للضحايا. حين وقع الهجوم سارعت الحكومة إلى تقديم المشورة وأوصت بالإجراءات التي يجب أن يتخذها الذين تضرروا من الحادث. وقالت شركة مايكروسوفت إنه حتى نهاية مارس كان 92% من عملائها قد صححوا وضع شبكاتهم ضد تلك الثغرة الأمنية.

[16] وزارة الخارجية والكومنويلث والتنمية البريطانية، المملكة المتحدة وحلفاؤها يحمّلون الصين المسؤولية عن نموذج قرصنة واسع النطاق (2021)

دوافع التغيير

33. سيشهد العقد القادم **استمرار التوسع السريع في التواصل المعلوماتي والرقمي تقريبا في كل مناحي حياتنا**. حيث إن النمو العالمي الهائل في الاتصال بشبكة الإنترنت واستخدامها، بمساندة البيانات والبنية التحتية التي يعتمد عليها استخدام البيانات، يفتح أسواقا جديدة ويزيد من سهولة الاتصالات وكثرة خياراتها وزيادة كفاءتها. إلا أن ذلك أيضا يجعل الدول أكثر اعتمادا على أنظمة رقمية متصلة ببعضها البعض، ما يُفسح مجالا أكبر للنشاطات الخبيثة ولإحداث ضرر بالغ في العالم المادي. وفيما يستمر التقاء التقنيات الحساسة وغير الحساسة في العديد من القطاعات، فإن تلك المخاطر تنتشر لتصل إلى مجالات جديدة في اقتصادنا. كما إن حركة البيانات والخدمات السحابية - وعادة خارج المملكة المتحدة - تزيد من انكشافنا على تلك المخاطر.

34. نشهد المزيد من التفاعل بين الشركات العريقة في القطاعات الخاضعة للتنظيم، مثل قطاعي الاتصالات اللاسلكية والطاقة، وشركات جديدة أغلبها غير خاضع للتنظيم، مثل تلك التي تولّد الطاقة على نطاق مصغّر أو شواحن المركبات الكهربائية أو إمكانات "المجتمعات المتصلة بالإنترنت". وستصبح البنى التحتية الحيوية موزعة بشكل أكبر وأكثر انتشاراً، وهذا سيغير بشكل جذري تأثير التنظيم على أمن الخدمات والوظائف الحساسة التي نعتمد عليها. كما سيؤثر ذلك التنوع على أمننا الوطني بشكل أعم، ما سيجعل الحصول على المعلومات أكثر صعوبة سواء بالنسبة لأجهزة إنفاذ القانون أو لغرض الأمن الإلكتروني. وهذا التغير في البيئة سوف يؤثر أيضا على المنتجات والخدمات على نطاق أوسع خارج البنى التحتية الوطنية الحيوية التقليدية.

35. هذا **التعقيد المتزايد في البيئة الإلكترونية** سيزيد من الصعوبات التي تواجهها الدول والشركات والمجتمع في فهم الأخطار التي تهددهم، وما يمكنهم ويجب عليهم أن يفعلوه لحماية أنفسهم. والاعتماد المتزايد على مورّدي الخدمات التي يديرها طرف ثالث، والتي عادة ما تكون لها أفضلية الاتصال بأنظمة المعلومات للآلاف من العملاء، يخلق أخطارا جديدة لا بد من معالجتها. وستكون الأجهزة والشبكات متصلة مع الإنترنت بشكل متزايد كمقياس اعتيادي، ما يجعل الفضاء الإلكتروني يمتد لداخل بيوتنا ومركباتنا ومدننا وبيئتنا التحتية الصناعية. كما ستنطمس الحدود بشكل متزايد بين أنشطتنا على الإنترنت وخارجها بفضل المجسات والأجهزة الصغيرة التي نرتديها والأجهزة الطبية والبيومترية. وستصبح الأخطار الإلكترونية أكثر انتشارا، وما يصاحب ذلك من زيادة في حجم البيانات الحساسة والشخصية والضرر المحتمل في حال تعرض الأنظمة للاختراق.

36. على هذه الخلفية، ستستمر **التهديدات في الفضاء الإلكتروني في تطورها وتنوعها**، حيث ستتحول القدرات الإلكترونية الفائقة إلى سلع، وسيكثر انتشارها على نطاق أوسع من الدول والمجموعات الإجرامية. كما سيزداد عدد الفاعلين الذين لديهم المقدرة والنية لمهاجمة المملكة المتحدة في الفضاء الإلكتروني، وستستخدم الدول نطاقا أوسع من الأدوات لتنفيذ نشاطات معرقِلة، بما في ذلك بالاستعانة بفاعلين يعملون لصالحها. كما إن الانتقال المتسارع إلى طرق العمل الموزّع بين المكتب والمنزل، والقيود على السفر بين الدول بفعل تفشي الجائحة، قد أدى إلى المزيد من الاعتماد على الخدمات الرقمية، وشجع جماعات الجريمة المنظمة على ارتكاب الجرائم الإلكترونية. وقد بدأنا نرى بالفعل الدلائل على هذا التوجه من خلال أحدث استطلاع بشأن الجرائم، والذي يشير إلى أن عدد الجرائم الإلكترونية قد ارتفع بشكل كبير بين عامي 2019 و2021.[17] وهذا التحدي لن تنفرد به المملكة المتحدة، لأنه يخلق نقاط ضعف متبادلة بالنسبة لكل من يعتمد على الفضاء الإلكتروني.

[17] المكتب الوطني للإحصاء، الجرائم في إنجلترا وويلز: السنة المنتهية في يونيو 2021 (2021)

37. سيكون هناك المزيد من التنافس على الفضاء الإلكتروني، حيث يسعى الفاعلون من الدول ومن غير الدول لتحقيق مزايا استراتيجية في الفضاء الإلكتروني ومن خلاله. وسوف تزداد أهمية العمليات الإلكترونية لإبراز القوة دون عتبة الصراع المسلح، وكذلك في المواقف التي تسبق الصراع. وستشهد الصراعات في المستقبل زيادة في استخدام القدرات الإلكترونية. ولكي تتصرف المملكة المتحدة بشكل فعال، سنحتاج لمستويات أعلى من الصمود الإلكتروني ضمن قدراتنا الدفاعية. وسيتوجب إدماج العمليات الإلكترونية مع عناصر القوة الأخرى من أجل دحر التهديدات وتمكين الأنشطة الدفاعية الأوسع نطاقا. وسيصبح الفضاء بشكل متزايد مجالا للعمليات، كما هو مبين في الاستراتيجية الوطنية للفضاء، ما يفتح مجالات جديدة للأخطار، لكنه سيخلق أيضا فرصا للمملكة المتحدة لاستغلال قدراتها الإلكترونية من أجل تحقيق التفوق بطرق جديدة.[18]

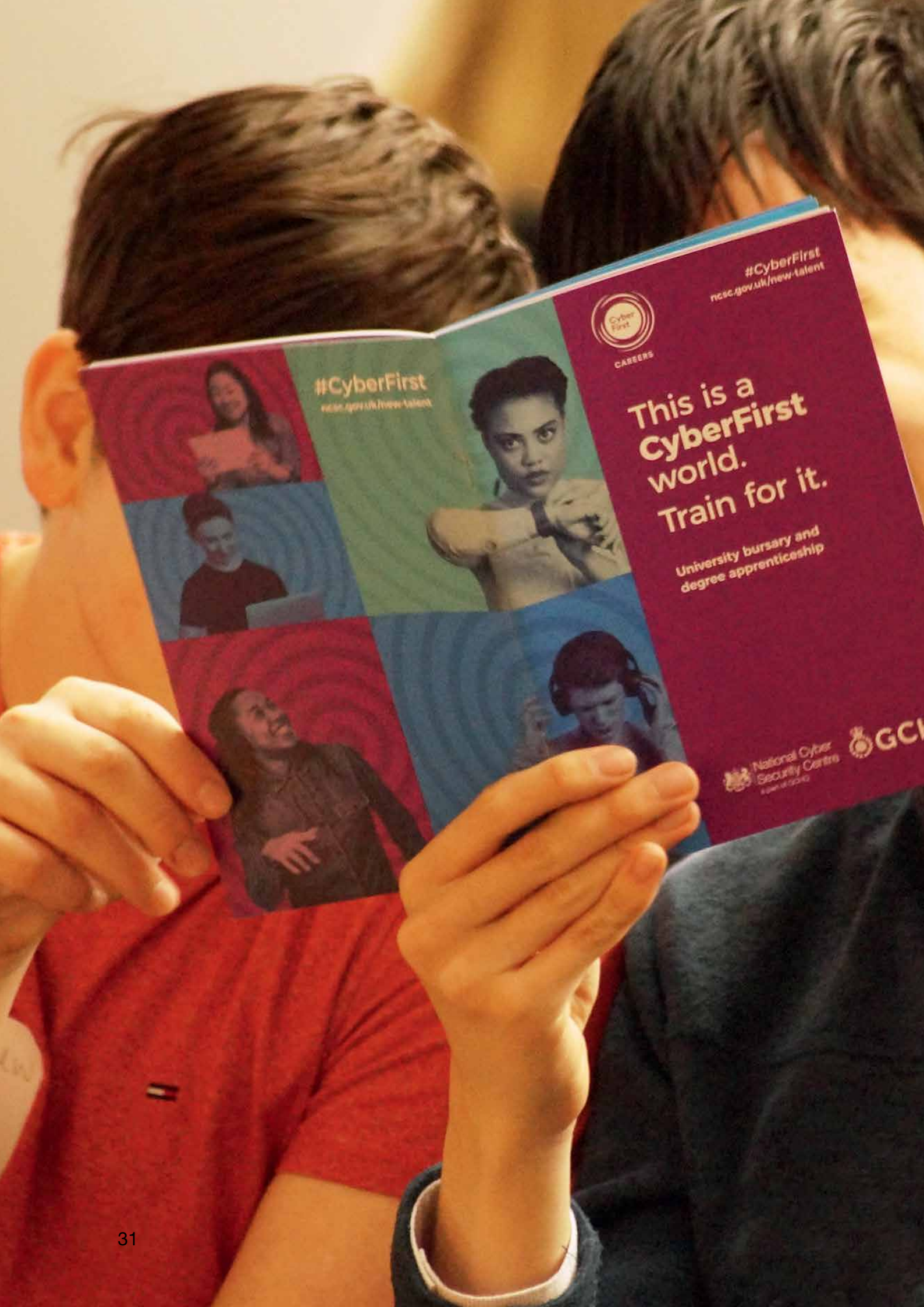
38. ستصبح النقاشات بشأن القواعد التي تحكم الفضاء الإلكتروني ساحة **لمنافسة أساسية بين القوى العظمى،** إلى جانب تصادم في القيم بين الدول التي تريد أن تحافظ على نظام مبني على المجتمعات المفتوحة، ومنافسين أساسيين مثل الصين وروسيا اللتين تدعمان المزيد من سيطرة الدولة كأسلوب وحيد لضمان أمن الفضاء الإلكتروني. من شأن ذلك أن يشكّل ضغطا على الإنترنت الحر والمنفتح، فيما تشجع الدول وشركات التكنولوجيا الكبرى وغيرها من الفاعلين على مقاربات متنافسة بشأن المعايير التقنية وعلى حوكمة الإنترنت.

39. سيتفاقم ذلك الوضع **بفعل التنافس للسيطرة على الساحة التكنولوجية الآخذة في التطور بشكل سريع.** ففي حين أن التكنولوجيا الرقمية أصبحت داخلة في كل مناحي حياتنا اليومية، وفي الشركات والبنية التحتية، فإن بعض أنواع التكنولوجيا أصبح حيوياً حقا لمختلف وظائف المجتمع. وستتركز القوة بشكل متزايد في يد الدول التي لديها تفوق استراتيجي في العلم والتكنولوجيا، والبيانات التي تحفّز الابتكار، الأمر الذي سيمكّن تلك الدول من ممارسة نفوذها على الآخرين، ومن بلورة معايير عالمية بطرق تخدم مصالحها الخاصة الاقتصادية والسياسية.

40. التكنولوجيا الناشئة مثل التوائم الرقمية، واستخدام الحاسوب الكمي، والأنظمة الضخمة المستقلة - وما يولده كل ذلك من بيانات - سوف تخلق فرصا وتولّد مخاطر جديدة، وتفتح المجال لقدرات إلكترونية جديدة سواء للمهاجمين أو للمدافعين، تماما كاستغلال العملات الرقمية من قبل عصابات برامج انتزاع الفدية. وقد أصبحت الريادة التكنولوجية موزعة على نطاق أوسع، ولن تتمكن المملكة المتحدة من تطوير قدرات سيادية في كافة أنواع التكنولوجيا الضرورية. ومن المعروف أن الدول والشركات تستفيد من المعايير الفنية لخدمة مصالحها الخاصة. ونحن نواجه خطر تطوير أنواع أساسية من التكنولوجيا على أيدي أولئك الذين لا يشاركوننا نفس القيم.

41. تعمل المملكة المتحدة منذ أكثر من عقد على وضع استراتيجية طموحة للأمن الإلكتروني الوطني، وقد حافظت على مستوى كبير من الاستثمارات، ما جعلها رائدة عالميا في المجال الإلكتروني. وكما يتضح من التحليل أعلاه، لا زالت توجد تحديات وفرص كبيرة. في الأقسام التالية نستعرض استجابتنا الوطنية.

[18] حكومة المملكة المتحدة، الاستراتيجية الوطنية للفضاء (2021)


#CyberFirst
ncsc.gov.uk/new-talent
CyberFirst
CAREERS
#CyberFirst
ncsc.gov.uk/new-talent
This is a CyberFirst world. Train for it.
University bursary and degree apprenticeship
National Cyber Security Centre

استجابتنا الوطنية

42. في هذه البيئة الاستراتيجية، يتعين على المملكة المتحدة أن تحدد خيارها. قد يمكننا أن نهدف ببساطة لمجاراة التهديدات والتحديات التي نجابهها في فضاء إلكتروني يزداد تعقيدا، وتعزيز التقدم الذي أحرزناه في السنوات الخمس الماضية، ومعالجة المسائل الأكثر إلحاحا حيثما استطعنا. لكن هذه المقاربة تنطوي على خطريْن اثنين. الأول هو أننا لا نحقق كامل إمكانات المملكة المتحدة في الفضاء الإلكتروني لدعم الأولويات الوطنية، وبالتالي تضيع علينا الفرص. والثاني، وهو الخطر الأكثر شدة، هو أن نصل إلى نقطة توقّف تكنولوجي، ونكتشف أن أعداءنا ومنافسينا هم الذين يشكلون أساسات مستقبل اقتصادنا ومجتمعنا، وأن علينا العمل بجهد أكبر لضمان أمننا.

43. في تقديرنا أنه فيما يصبح الفضاء الإلكتروني أساسيا بشكل متزايد لمصالحنا ومصالح حلفائنا وأعدائنا، توجد **ضرورة استراتيجية لأن نعزز تفوقنا التنافسي في التحرك على هذه الساحة**. ولعل ذلك سيمكّننا ليس فقط من ضمان أمننا اليوم، بل أيضا من رسم معالم عالم الغد والاستفادة منه.

رؤيتنا وأهدافنا ومبادئنا

44. تتلخص رؤيتنا بأن المملكة المتحدة في عام 2030 ستظل **قوة إلكترونية رائدة ومسؤولة وديمقراطية، قادرة على حماية مصالحها والترويج لها في الفضاء الإلكتروني ومن خلاله دعماً لأهدافها الوطنية**.

45. لتحقيق هذه الرؤية، سنسعى إلى تحقيق خمسة أهداف استراتيجية. وكل منها يهدف إلى تعزيز قوتنا الوطنية في واحد من الأبعاد الخمسة للقوة الإلكترونية. وستعمل تلك الأهداف مجتمعة على دعم قدرتنا على أن يكون لدينا فضاء إلكتروني يعكس قيمنا ومصالحنا. هذه الأهداف الخمسة - أو الدعامات - تشكّل إطارا استراتيجيا تستهدي به أنشطتنا. ويبين الجزء الثاني من هذه الاستراتيجية الخطوات التي سنتخذها بالنسبة لكل واحد من تلك الأهداف من الآن وحتى 2025.

- **الدعامة 1: تقوية البيئة الإلكترونية في المملكة المتحدة**، الاستثمار في إمكانات المواطنين وفي المهارات، وتعميق الشراكات بين الحكومة والجامعات والقطاع

- **الدعامة 2: جعل المملكة المتحدة دولة رقمية ومزدهرة وقادرة على الصمود**، وتقليل المخاطر الإلكترونية حتى تتمكن الشركات من تحقيق أكبر مكاسب الاقتصادية من التكنولوجيا الرقمية، ولكي يكون المواطنون آمنين على الإنترنت، وواثقين أن بياناتهم محمية

- **الدعامة 3: أخذ زمام القيادة في مجالات التكنولوجيا الضرورية للقوة الإلكترونية** وبناء قدراتنا في قطاع التكنولوجيا، وتطوير أطر خاصة من أجل حماية تقنياتنا المستقبلية

- **الدعامة 4: تطوير الدور الريادي للمملكة المتحدة ونفوذها العالمي في جعل النظام العالمي أكثر أمنا وازدهارا وانفتاحا**، وذلك بالعمل مع الحكومة والشركاء في القطاع، وتشارك الخبرات التي ترتكز عليها القوة الإلكترونية للمملكة المتحدة

- **الدعامة 5: كشف أعدائنا وعرقلة خططهم وردعهم لتعزيز أمن المملكة المتحدة في الفضاء الإلكتروني ومن خلاله**، واستخدام كل إمكانات المملكة المتحدة بشكل أكثر تكاملا وإبداعا وبوتيرة أكبر

46. هذه الأهداف مصممة بحيث تدعم بعضها بعضا. على سبيل المثال، سيكون تحقيق مستويات أعلى من الأمن والصمود الإلكتروني محليا بمثابة ركيزة أساسية لموقف أكثر فاعلية على المستوى الدولي. وبالتالي، فإن سلاسل توريدنا العالمية والأخطار التي نواجهها من الخارج تعني أننا لن نتمكن من ضمان أمننا دون بذل جهد أكبر لضبط سلوك الفاعلين الدوليين. وقدرتنا على التأثير في النقاش العالمي بشأن الفضاء الإلكتروني والإنترنت والتكنولوجيا ستعتمد على الحفاظ على تفوقنا التقني، وبناء بيئة للابتكار تؤدي إلى تفوق حقيقي في مجالات التكنولوجيا الأكثر أهمية.

47. محور رؤيتنا هو **تطوير فضاء إلكتروني حر ومنفتح وسلمي وآمن**. واهتمامنا الاستراتيجي بالقوة الإلكترونية لا يُقصد به تأجيج الصراعات أو جعل المملكة المتحدة تحقق مكاسب على حساب الغير. وكما أوضحت المراجعة المتكاملة، فإن العالم الذي تتمكن فيه المجتمعات والاقتصادات المنفتحة من الازدهار هو أفضل ضامن لازدهارنا وسيادتنا وأمننا في المستقبل. وستعمل المملكة المتحدة مع الدول التي تشاطرها المبادئ لنشر قيمنا المشتركة في الانفتاح والديمقراطية، **سعيا لمقاربة مسؤولة وديمقراطية تجاه القوة الإلكترونية**. ذلك يعني أنه بالعمل نحو تحقيق هذه الأهداف الاستراتيجية الخمسة سنطبق **المبادئ** التالية:

- سوف نعطي الأولوية لقدرة المواطنين والشركات على العمل في الفضاء الإلكتروني بشكل آمن بحيث يتمكنوا من تحقيق أكبر المكاسب الاقتصادية والاجتماعية من التكنولوجيا الرقمية، ومن ممارسة حقوقهم القانونية والديمقراطية

- سنعمل على جعل الإنترنت متاحة لأكبر عدد من الناس وعلى نحو أكثر عدلا باعتبار ذلك نموذجا لدعم الازدهار والرفاه العالميين، ولمقاومة الضغوط من جانب الدول ذات الأنظمة المستبدة التي تهدف إلى فرض قيود على الإنترنت، وفرض رؤيتها بشأن سيادة الدولة على الإنترنت

- سنستخدم قدراتنا الإلكترونية بشكل قانوني ومتناسب ومسؤول، يدعمنا في ذلك الإشراف الواضح والتواصل مع عامة الناس ومع حلفائنا، وسوف نحاسب الآخرين على التصرفات الطائشة والعشوائية في الفضاء الإلكتروني

- سوف نتخذ الإجراءات الضرورية بكافة السبل المتاحة ضد استخدام الفضاء الإلكتروني لأغراض إجرامية، وسنعمل على كشف الجهات التي تستخدم مجرمين بالوكالة أو تؤوي مجموعات إجرامية في أراضيها، وعلى منع وصول التقنيات الإلكترونية المتطورة إلى أيدي المجرمين

- سنتبنى مقاربة شاملة متعددة الأطراف المعنية في النقاشات بشأن مستقبل الفضاء الإلكتروني والتكنولوجيا الرقمية، وحماية حقوق الإنسان في الفضاء الإلكتروني، والتصدي للتحركات التي تهدف إلى الاستبداد الرقمي وفرض سيطرة الدولة

تحولات أساسية في مقاربتنا

48. سترتكز استراتيجيتنا في نواحٍ عديدة على مقاربتنا الحالية في السعي لتعزيز وتوسيع جهودنا أو تعديلها حسبما تقتضيه الضرورة. الفروق الرئيسية عن الاستراتيجية الوطنية لأمن المعلوماتية للفترة 2016 - 2021 مبينة أدناه، وتعكس طموحنا الأكبر لترسيخ مكانة المملكة المتحدة كقوة إلكترونية رائدة.

49. الالتزام بإبقاء المملكة المتحدة رائدة في مجال القدرات الإلكترونية. ستستثمر الحكومة 2.6 مليار جنيه إسترليني في مجال التقنيات الإلكترونية واستبدال أنظمة تكنولوجيا المعلومات القديمة على مدى السنوات الثلاث القادمة. يُضاف ذلك إلى الاستثمار الضخم في القوة الإلكترونية الوطنية الذي أُعلن عنه في مراجعة الإنفاق لعام 2020. يتضمن الاستثمار زيادة مقدارها 114 مليون جنيه إسترليني في البرنامج الوطني لأمن المعلوماتية. وسيكون ذلك بالإضافة إلى الزيادات في الاستثمار المعلنة سابقا في مجالات البحث والتطوير، والمعلومات الاستخباراتية، والدفاع، والابتكار، والبنية التحتية، والمهارات، والتي ستساهم جزئيا في بناء القوة الإلكترونية للمملكة المتحدة. الاستثمارات في مجال القدرات الإلكترونية التي أُعلن عنها في مراجعة الإنفاق لعام 2020 وعام 2021 تتجاوز لحد بعيد مبلغ 1.9 مليار جنيه إسترليني الذي تعهدت المملكة المتحدة بإنفاقه على مدى خمس سنوات في الاستراتيجية السابقة.[19]

50. استراتيجية إلكترونية وطنية أكثر شمولا. يظل الأمن الإلكتروني في صميم هذه الاستراتيجية، لكنه يستجمع الآن كامل قدرات المملكة المتحدة داخل الحكومة وخارجها. وهو يولي أهمية أكبر للتكنولوجيا الحساسة والبنية التحتية اللتين تشكلان الدعامة الأساسية للفضاء الإلكتروني، ويدعم الشركات البريطانية في القطاع الإلكتروني لكي تنمو محليا وتنافس دوليا، ويرفع من وتيرة العمل الدولي لرسم معالم الفضاء الإلكتروني في المستقبل والتأثير به، كما أنه يدمج الهجوم الإلكتروني كأحد الدعائم للقوة الإلكترونية. وهذا يتطلب مقاربة استراتيجية وطنية تتضافر فيها الجهود حقاً. توزع هذه الاستراتيجية المسؤوليات بالنسبة للقيادة والتنسيق على نطاق الوزراء، وتُشرك الحكومات المفوّضة في إيرلندا الشمالية واسكتلندا وويلز بشكل وثيق أكثر. ويرتكز ذلك على نجاحنا في تنسيق الجهود في مختلف وزارات الحكومة، وهذه إحدى نقاط القوة الرئيسية للمملكة المتحدة.

[19] وزارة الخزانة، الميزانية ومراجعة الانفاق لخريف 2021 (2021)

51. جهد يشمل المجتمع بأكمله. هدفنا هو اتباع مقاربة وطنية استراتيجية يسترشد بها صُنّاع القرار في المؤسسات في كافة أرجاء البلاد، وتوفر الأساس لتعاون أقوى مع شركائنا في المملكة المتحدة وحول العالم. هناك المزيد من العمل الذي يجب القيام به لتحقيق ذلك. الخطوات التي ستُتخذ على المدى القصير سوف تشمل: (أ) تشكيل مجلس استشاري وطني جديد للقطاع الإلكتروني، ودعوة كبار القادة من القطاع الخاص وقطاعات أخرى لمناقشة ودعم مقاربتنا والمساهمة في بلورتها؛ (ب) إعادة توجيه برامجنا المخصصة للابتكار في القطاع الإلكتروني بعيدا عن المبادرات الضخمة، والتي غالبا ما تتمركز في لندن، وتوجيهها نحو نموذج يُنفّذ إقليميا ويكون مؤسَّسا بالشراكة مع القطاع الإلكتروني والمبتكرين وأجهزة إنفاذ القانون والقطاع الأكاديمي على المستوى المحلي؛ (ج) اتخاذ الخطوات اللازمة لزيادة التنوع في القوة العاملة في المجال الإلكتروني - مع إدراكنا بأن القدرة على توظيف ورعاية المواهب والمهارات لعامة الشعب هو أمر في غاية الأهمية بالنسبة لأمننا القومي. لقد تشكلت الاستراتيجية بحد ذاتها عن طريق التواصل مع الحكومات المفوضة في إيرلندا الشمالية واسكتلندا وويلز، والقطاع الإلكتروني، وأجهزة إنفاذ القانون، والجهات التنظيمية، والقطاع الأكاديمي، والمجتمع المدني، والشركاء الدوليين. وغايتنا هي إبقاء تلك الحوارات مفتوحة طوال فترة تطبيق الاستراتيجية.

52. مقاربة استباقية لتعزيز وحماية تفوقنا التنافسي في مجالات التكنولوجيا الضرورية للفضاء الإلكتروني. المراجعة المتكاملة وما تلاها من استراتيجيات قد بدأت بالفعل تطبيق هذه المقاربة في عدة مجالات، مثل الذكاء الاصطناعي والتقنيات الكمية والبيانات. وتتضمن هذه الاستراتيجية تعهدات جديدة في مجالات تصميم معالجات دقيقة آمنة، وأمن التقنيات العملية، والتشفير. كما تعلن عن إنشاء مختبر وطني لأمن التقنيات العملية كمركز جديد متميّز يُركّز على بناء أعلى مستوى من الصمود الإلكتروني بالمشاركة مع القطاعين الإلكتروني والأكاديمي. كذلك تعلن هذه الاستراتيجية أيضا عن التوسع في القدرات البحثية للمركز الوطني لأمن المعلوماتية، بما في ذلك مركز الأبحاث التطبيقية الجديد في مانشستر، مع التركيز على التكنولوجيا الناشئة مثل المجتمعات المتصلة بالإنترنت، والنقل. كما استندت الاستراتيجية إلى عملنا الناجح لتطوير مقاربات تدمج الأمن في أنواع التكنولوجيا الجديدة بحيث تجعلها "آمنة بأساس التصميم". ذلك يعني الاستثمار والاستفادة بشكل أكبر من الأدوات التنظيمية والتشريعية المساندة عند الضرورة من أجل تطوير سلاسل لتوريد تكنولوجيا أكثر تنوعا وأمنا وقدرة على الصمود، مثلما فعلنا في قطاع الاتصالات.

53. تقوية جهودنا الأساسية بشكل كبير لتطوير الأمن الإلكتروني تحت قيادة الحكومة. سنستثمر أكثر من أي وقت مضى في إجراء مراجعة جذرية شاملة وسريعة للأمن الإلكتروني للحكومة، مع وضع معايير واضحة للوزارات، ومعالجة البنية التحتية القديمة لتكنولوجيا المعلومات. وستجري تقوية مختلفة وظائف الحكومة الحيوية بشكل كبير ضد الهجمات الإلكترونية بحلول عام 2025، وسوف نعمل على ضمان أن تكون كافة مؤسسات الحكومة - في مختلف أرجاء القطاع العام - قادرة على الصمود إزاء نقاط الضعف المعروفة والهجمات المعادية بحلول عام 2030. وسنبذل المزيد من الجهود لحماية مواطنينا وإشراكهم في تلك الجهود، مع إزالة أكبر قدر ممكن من العبء عنهم. كما سنقوّي البيئة الرقمية لحماية المواطنين من الجرائم الإلكترونية والاحتيال مع وضع المزيد من المسؤولية على المصنّعين، والبائعين، ومقدمي الخدمات، والقطاع العام من أجل رفع معايير الأمن الإلكتروني. كما سوف نرفع مستوى مشاركة القطاع الخاص واستثماره في الصمود الإلكتروني من خلال جعل الأحكام والقواعد تتسق مع الحوافز في كافة مجالات الاقتصاد، مع توفير المزيد من الدعم. كذلك سيزداد تركيزنا على مخاطر سلاسل التوريد، بحيث نختبر عدة مبادرات لمساعدة المؤسسات على إدارة مخاطر الأمن الإلكتروني التي تنجم عن الموردين، وضمان تطبيق أفضل الممارسات على مختلف مراحل سلسلة التوريد.

54. مزيد من الحملات المتكاملة والمتواصلة لردع وتعطيل نشاطات أعدائنا ولحماية وتطوير مصالح المملكة المتحدة في الفضاء الإلكتروني. سوف تستفيد هذه الحملات من كافة الأدوات الدبلوماسية والسياسية والعملية على نطاق الحكومة بأكملها. وستكون مرتكزة لحد بعيد على إنشاء وتوسيع القوة الوطنية لأمن المعلوماتية والتي سيكون مقرها في ساملزبيري في لانكاشير (إنجلترا). وسوف نستعين بوتيرة أكبر من قدرات هذه القوة لإحباط التهديدات التي قد تأتي من الدول ومن الفاعلين من غير الدول، ولدعم مصالح الأمن القومي الأعم للمملكة المتحدة. كما ستستفيد حملاتنا من استثمارات كبيرة جديدة في القدرات المتطورة في مجال إنفاذ القانون على المستويات الوطنية والإقليمية والمحلية. من شأن ذلك أن يساعدنا في التصدي للتهديدات الكبيرة من برامج انتزاع الفدية، ومن مرتكبي الجرائم الإلكترونية الذين يطورون مهاراتهم بشكل متزايد. وسنستمر أيضا باستغلال نظام العقوبات الإلكترونية المستقل للمملكة المتحدة وعملية التحقق من خصائص المستخدم من أجل فرض تكلفة عالية على أعدائنا والكشف عن الهجمات الخبيثة والمتهورة.

55. وضع القوة الإلكترونية في صميم أجندة السياسة الخارجية للمملكة المتحدة، مع مراعاة أن كل جزء من هذه الاستراتيجية يتطلب مشاركة دولية. سنقوي تحالفاتنا الأساسية ونُشرك معنا نطاقا واسعا من الدول لمجابهة انتشار الاستبداد الرقمي. وعلى مدى السنوات القليلة القادمة، سنزيد من استثماراتنا في البرامج الدولية لدعم الدول الشريكة لمساعدتها في بناء صمودها وتعزيز قدراتها في مجابهة التهديدات الإلكترونية. وسنستغل بشكل أفضل كافة أشكال نقاط القوة المحلية، بما في ذلك خبراتنا العملية والاستراتيجية في مجال الاتصالات، من خلال ريادتنا وعلاقاتنا التجارية وشراكاتنا في القطاع لدعم أهدافنا الدولية.

الأدوار والمسؤوليات في أنحاء المملكة المتحدة

56. سيكون أساس استراتيجيتنا أن تكون مقاربتنا في التعامل مع الفضاء الإلكتروني تشمل المجتمع بأكمله. وسيكون علينا بناء شراكات مستدامة ومتوازنة على امتداد القطاعين العام والخاص وغيرهما من القطاعات، بحيث يلعب كل منهم دورا هاما في جهودنا الوطنية.

المواطنون

57. تهدف هذه الاستراتيجية إلى رفع أكبر قدر ممكن من عبء الأمن الإلكتروني عن كاهل المواطنين، لكن سيظل لكل منا دور هام يؤديه. وفي حين أن الحكومة ستفعل ما بوسعها لوقف الهجمات الإلكترونية قبل وقوع الضرر على الأفراد، سوف يجد بعض مصادر التهديد من الفاعلين طرقا للالتفاف على أساليب الحماية التي توفرها الحكومة. يمكننا جميعا أن نعمل على تحسين أمن مواردنا الثمينة في كل من العالمين المادي والافتراضي.[20] ذلك يعني أداء واجبنا في اتخاذ كافة الخطوات المعقولة لحماية ليس فقط أجهزتنا - مثل هواتفنا الذكية وغيرها من الأجهزة - بل أيضا البيانات والبرمجيات والأنظمة التي تمنحنا الحرية والمرونة والراحة في حياتنا الخاصة والمهنية. لدعم ذلك، تقدم الحكومة المشورة الفنية الدقيقة والقابلة للتطبيق في الوقت المناسب. كما تلعب مؤسسات المجتمع المدني ومجموعات مجتمعية أخرى دورا هاما في مساعدة الناس لفهم الأخطار الإلكترونية وحماية أنفسهم منها. فمثلا هنالك جمعيات خيرية عديدة تقدم الدعم الموجَّه والمشورة وحملات التوعية لفئات الناس المعرضة للخطر.

[20] حملة التوعية بالأمن الإلكتروني هي المشورة التي تقدمها الحكومة للأفراد لكي يكونوا آمنين على الإنترنت

الشركات والمؤسسات

58. تقع على عاتق الشركات والمؤسسات مسؤولية إدارة مخاطرها الإلكترونية بشكل فعال، وتطوير قدرتها على الصمود إلكترونيا، ودعم عملائها والأفراد الذين يستخدمون خدماتها. فالشركات والمؤسسات تعتمد بشكل متزايد على التكنولوجيا الرقمية وخدمات الإنترنت في عملها ونموها وابتكاراتها. ومن شأن ذلك أن يحسّن الخدمات، لكنه أيضا يخلق مخاطر وتحديات جديدة، مثل الكم الضخم من البيانات الشخصية والموارد الرقمية التي تقع تحت مسؤوليتها. ذلك يُحتّم على المؤسسات والشركات حماية تلك البيانات والموارد، مع الحفاظ بنفس الوقت على استمرارية خدماتها. وإن توانت عن فعل ذلك، ستواجه عواقب وخيمة تضر بسمعتها وأعمالها، وتلحق الأذى بعملائها. وتقع مسؤوليات خاصة على عاتق مشغلي الخدمات الضرورية ومقدمي الخدمات الرقمية الهامة (مثل الخدمات السحابية) من أجل التصدي للأخطار الإلكترونية التي يواجهونها، وأداء التزاماتهم المبينة في اللوائح بشأن الشبكات وأنظمة المعلومات. والمشورة والإرشادات التي يقدمها المركز الوطني لأمن المعلوماتية تساهم في توفير الدعم لكافة الشركات والمؤسسات لكي تحمي نفسها ومعلوماتها ومواردها وأنظمتها. كما إن مكتب المفوض المعني بالحقوق المتعلقة بالمعلومات يقدم النصح أيضا للمؤسسات بشأن التزاماتها تجاه الأمن الإلكتروني بموجب لوائح حماية البيانات العامة في المملكة المتحدة.

قطاع الأمن الإلكتروني وشركات التكنولوجيا الكبرى

59. لقطاع الأمن الإلكتروني المتنامي في المملكة المتحدة دور حيوي في الاستجابة للتهديدات الإلكترونية الناشئة والتحديات التي تواجه بلادنا. فالانتشار السريع للمنتجات القابلة للاتصال بالإنترنت، والتحول الرقمي المتسارع للشركات والمؤسسات يوفران الفرصة لهذا القطاع لينمو ويبتكر، وليقدم خدمات ومنتجات جديدة. تستعرض هذه الاستراتيجية كيف ستواصل الحكومة دعم نمو قطاع الأمن الإلكتروني في المملكة المتحدة، والاستفادة من قدراته وخبراته من خلال الحفاظ على شراكاتنا وتقويتها. كما إننا نرغب أيضا بتقوية الشراكات الأشمل بين القطاع الأكاديمي والمؤسسات التقنية والقطاع الخاص لضمان أن نستفيد تماما من الخبرات التقنية في المملكة المتحدة.

60. شركات التكنولوجيا الكبرى التي تقدم خدمات رقمية لها دور حيوي في ضمان بيئة آمنة للشركات والمؤسسات البريطانية لكي تعمل ضمنها. ويصح ذلك بوجه خاص بالنسبة لمقدمي الخدمات المدارة، والشركات التي تدير منصات تدمج عددا من الخدمات. يلزم على تلك الشركات أن تضمن أن الخدمات التي تقدمها "يُفترض أنها آمنة" وألا تعتمد أكثر مما ينبغي على أن يتخذ عملاؤها خطوات وقائية. كما تقع على عاتق شركات التكنولوجيا الكبرى مسؤولية خاصة لإعطاء الأولوية لصمودها الإلكتروني. حيث إن تزايد اعتماد الشركات والحكومة والمجتمع على الخدمات السحابية والإنترنت يؤدي إلى زيادة في اعتمادها على بعضها البعض ويخلق نقاط ضعف فريدة.

الحكومة

61. **الحكومة البريطانية** بمكانة فريدة تؤهلها لجمع المعلومات الضرورية لفهم أكثر التهديدات تعقيدا، ولوضع القوانين وتطبيقها، وتحديد المعايير الوطنية، والتصدي للتهديدات من الفاعلين المعادين، بما في ذلك تنفيذ هجمات إلكترونية. من خلال هذه الاستراتيجية سنستثمر في تقوية قدراتنا الإلكترونية الوطنية. كما إن وزارات الحكومة ومؤسسات القطاع العام مسؤولة أيضا عن حماية شبكاتها وأنظمتها الخاصة بها. ولكونها تحتفظ بكمّ كبير من البيانات وتقدم الخدمات، ستتخذ الحكومة إجراءات صارمة لحماية البيانات التي لديها. وأخيرا، تقع على عاتق الحكومة أيضا مسؤولية هامة بأن تقدم المشورة للمواطنين والشركات والمؤسسات وأن تخبرهم بما يحتاجون لفعله لحماية أنفسهم على الإنترنت. وحسبما تقتضي الضرورة، سيشمل ذلك وضع المعايير التي نتوقع من الشركات والمؤسسات الكبرى أن تلتزم بها لحمايتنا جميعا.

62. معظم مجالات السياسة الإلكترونية وغالبية الإجراءات التي تعرضها هذه الاستراتيجية متعلقة بمسائل محاطة بالتحفظ، مثل الأمن القومي، والشؤون الخارجية، والدفاع، والاتصالات اللاسلكية، ومعايير وسلامة المنتجات، وحماية المستهلك. لكن تطوير وتطبيق هذه الاستراتيجية سيظل يعتمد على مساهمات وأفعال واستثمارات **الحكومات المفوضة في إيرلندا الشمالية واسكتلندا وويلز** . وينطبق ذلك بوجه خاص حينما يتعلق الأمر بسياسات تلك الحكومات، والتي تقع بشكل أساسي ضمن دعامات "البيئة الإلكترونية" و"الصمود" في هذه الاستراتيجية، مثل التعليم وجهاز الشرطة، والصمود الإلكتروني لقطاعات حساسة معينة، بما في ذلك القطاع الحكومي في كل من تلك البلدان. إن التعاون والتنسيق بين الحكومات الأربع للمملكة المتحدة بالغ الأهمية من أجل ضمان تحقيق التأثير الأكبر على مستوى المملكة المتحدة بأكملها. ويتطلب ذلك تواصلا منتظماً ومبكراً بين وزارة شؤون مجلس الوزراء وغيرها من وزارات الحكومة البريطانية ونظرائها في ويلز واسكتلندا وإيرلندا الشمالية من أجل تبادل المعلومات بشأن الأولويات والخطط. ويساعد ذلك أيضا في تفادي ازدواجية الجهود، وفي الحصول على أعلى مردود من التمويل العام. ستواصل الحكومات المفوضة تطوير استراتيجياتها الإلكترونية والخطط الخاصة بها، وتنسقها مع هذه الاستراتيجية لحكومة المملكة المتحدة.

المركز الوطني لأمن المعلوماتية

"المساهمة في جعل المملكة المتحدة المكان الأكثر أمنا للعيش فيها والعمل على الإنترنت"

تأسس المركز الوطني لأمن المعلوماتية رسميا في 2017 كجزء من القيادة الحكومية المركزية للاتصالات ليكون الهيئة البريطانية الوطنية المعنية ببيئة الأمن الإلكتروني: لنشر المعرفة، ومعالجة نقاط الضعف الأساسية، وتوفير القيادة بشأن المسائل الهامة المتعلقة بالأمن الإلكتروني الوطني.[21] وقد أسهم إنشاء المركز الوطني لأمن المعلوماتية في تبسيط عمل الهياكل العملية للحكومة، وطوّر قدرة المملكة المتحدة على الاستجابة للحوادث الإلكترونية على المستوى الوطني، وبادر إلى تعميم الخدمات الرقمية المبتكرة التي أسهمت في جعل المؤسسات والأفراد أكثر أمنا بشكل تلقائي على الإنترنت.

نحن نعمل على ضمان أن يكون المركز الوطني لأمن المعلوماتية مهيأ للتحديات في العقد القادم عن طريق توضيح القدرات المستدامة والخصائص التي يرتكز عليها في عمله، وتمويلها على أساس مستدام، والتركيز على استخدامها في المواقع التي نعرف من خبرتنا العملية حتى الآن أنه سيكون لها أكبر تأثير على المستوى الوطني.

القدرات المستدامة والخصائص التي يرتكز عليها عمل المركز الوطني لأمن المعلوماتية هي:

- خبرات فنية عالمية المستوى في أنظمة الأمن الإلكتروني والتخصصات التي تحتاجها المملكة المتحدة؛
- فهم معمّق لا نظير له بشأن التهديدات الإلكترونية الحالية والمحتملة لمصالح المملكة المتحدة - بما في ذلك نوايا الأعداء وقدراتهم؛
- الاستفادة من كامل نطاق قدرات المملكة المتحدة والسلطات المسؤولة عن أهداف الأمن الإلكتروني؛
- التواصل المباشر مع مؤسسات الأمن الإلكتروني بالترتيب مع الشركاء في القطاعين الأكاديمي والإلكتروني وفي الخارج؛
- التواصل المباشر مع مؤسسات الأمن الإلكتروني بالترتيب مع الشركاء في القطاعين الأكاديمي والإلكتروني وفي الخارج.

وستكون المسؤوليات الأساسية للمركز الوطني لأمن المعلوماتية في ظل هذه الاستراتيجية الجديدة على النحو التالي:

- **اتخاذ إجراء مباشر للإقلال من تعرض المملكة المتحدة للأضرار الإلكترونية** عن طريق توفير الحماية على نطاق واسع من خلال الخدمات الرقمية (مثل تعزيز الدفاعات الإلكترونية)، وإحداث تغييرات في التكنولوجيا، وإدارة الاستجابة للحوادث الإلكترونية الهامة على المستوى الوطني، والتصدي بشكل مباشر للعمليات الإلكترونية التي ينفذها بالتعاون مع القوة الوطنية لأمن المعلوماتية.
- **دعم كافة شرائح المجتمع في المملكة المتحدة لحماية أنفسها** عن طريق تزويدها بخبرات مصممة خصيصا، ومعلومات فريدة يمكن للأفراد والشركات والمؤسسات في مختلف أرجاء المملكة المتحدة استخدامها لحماية أنفسهم، وتساهم في جعل المملكة المتحدة مكانا أكثر أمنا لكل من يستخدم الإنترنت.

[21] الحكومة البريطانية، الاستراتيجية الوطنية لأمن المعلوماتية 2016 - 2021 (2016): الفقرة 1(9)

- **تقديم مساهمات فنية في سياسات وتنظيمات الحكومة البريطانية بشأن القضايا الأكثر أهمية للأمن الإلكتروني**، وذلك من خلال توفير المسؤولين عن رسم السياسات في كافة قطاعات الحكومة، وتقديم مساهمات فنية موثوقة، وتقييم للمخاطر مشتق من القدرات الأساسية للمركز الوطني لأمن المعلوماتية، ودعم تطوير وتطبيق السياسات واللوائح لأجل الحفاظ على الأمن الرقمي لمواطني المملكة المتحدة ومؤسساتها ومصالحها.

- **توفير قدرات سيادية للمملكة المتحدة** من خلال المركز الوطني للتشفير National Crypt-Key Centre التابع للمركز الوطني لأمن المعلوماتية، والذي يحمي المعلومات والخدمات الحساسة التي يعتمد عليها الجيش البريطاني وقطاع الأمن القومي، بما في ذلك الحماية من الهجمات من أعدائنا الأكثر قدرة.

- **دعم النمو في الاستثمار والمهارات الإلكترونية** عن طريق توفير الخبرات الفنية اللازمة لكل مستويات التعليم الإلكتروني، وإشراك القطاع الإلكتروني ودعمه، وتحفيز الاستثمار في القطاع الإلكتروني.

كما سيساهم المركز الوطني لأمن المعلوماتية في **تقييم التقدم** الحاصل مقارنة بأهداف هذه الاستراتيجية الإلكترونية الوطنية من خلال التقييمات التي يجريها، وهي تقييمات إلكترونية مستقلة في المملكة المتحدة.

القوة الوطنية لأمن المعلوماتية

القوة الوطنية لأمن المعلوماتية التي تأسست في 2020 مسؤولة عن العمل في الفضاء الإلكتروني ومن خلاله للتصدي للذين يقصدون إلحاق الأذى بالمملكة المتحدة وحلفائها، ولإحباط خططهم واعتراضهم من أجل الحفاظ على سلامة البلاد، ولحماية مصالح المملكة المتحدة والترويج لها في الداخل والخارج. تتألف هذه القوة من أفراد من وزارة الدفاع والمخابرات بعدد متساوٍ تقريبا، وتجمع خبراتهم ومواردهم ومعرفتهم تحت هيكل قيادة واحدة، وسيكون مقرها في سالمزبيري في لانكاشير (إنجلترا).

تقدم القوة الوطنية لأمن المعلوماتية نطاقا واسعا من الخدمات لحماية الأمن القومي، مثل الدعم لقطاع الدفاع، وضمان سلامة الاقتصاد البريطاني، ومنع الجرائم الخطيرة. وتتراوح أنشطة هذه القوة بين المهام التكتيكية والاستراتيجية ضد الفاعلين من الدول أو من غير الدول. ويقع عملها تحت ثلاث فئات رئيسية:

- التصدي للتهديدات من الإرهابيين والمجرمين والدول الذين يستخدمون الإنترنت لتنفيذ عمليات إلكترونية عبر الحدود لإلحاق الأذى بالمملكة المتحدة والدول الديمقراطية الأخرى
- التصدي للتهديدات التي تنتهك سرية الخدمات في الفضاء الإلكتروني وكذلك سلامتها وتوفرها (مثلا دعم الأمن الإلكتروني)
- المساهمة في عمليات الدفاع البريطانية، والمساعدة في تطبيق أجندة السياسة الخارجية البريطانية (كالتدخل مثلا في أزمة إنسانية من أجل حماية المدنيين)

يمكن استخدام عمليات القوة الوطنية لأمن المعلوماتية للتأثير على الأفراد والجماعات، ولتعطيل أنظمة الاتصالات والأنظمة التي تعتمد على الإنترنت، وإفشال عمل الأنظمة المادية. يُشار عادة لهذا النوع من الأعمال بالهجمات الإلكترونية.

يجري تنفيذ عمليات القوة الوطنية لأمن المعلوماتية ضمن إطار قانوني راسخ يشمل قانون أجهزة المخابرات لعام 1994، وقانون صلاحيات التحقيق لعام 2016. وقد سبق أن أوضحت المملكة المتحدة أنها تطور وتستخدم القدرات وفقا للقوانين الدولية، ومنها قانون الصراعات المسلحة حيثما ينطبق ذلك. عمليات هذه القوة تكون رهناً بموافقة وزارية وتحت إشراف قضائي وتخضع لمراجعة من جانب البرلمان، الأمر الذي يجعل نظام حوكمة العمليات الإلكترونية في المملكة المتحدة واحدا من أقوى الأنظمة في العالم.

المملكة المتحدة لا تتحدث دائما عن العمليات الإلكترونية الفردية، لكن الأنشطة العملياتية التي تقوم بها القوة الوطنية لأمن المعلوماتية تشمل ما يلي:

- منع الجماعات الإرهابية من تنفيذ خططها عن طريق عرقلة اتصالات القيادة والسيطرة لديها، والحد من قدرتها على نشر مواد إعلامية متطرفة
- خفض الضرر الذي يمكن أن تتعرض له القوات المسلحة البريطانية عن طريق إبطال منظومات أسلحة الأعداء
- الدفاع عن الديمقراطية والانتخابات الحرة والنزيهة والمنفتحة من خلال التصدي لحملات المعلومات المضلِلة التي تشنها الدول الأخرى بقصد تقويض تلك الانتخابات
- منع الجماعات الإجرامية من الانتفاع من أنشطتها عن طريق عرقلة استخدامها لمنصات وخدمات الإنترنت
- المساعدة في تطبيق العقوبات الدولية عن طريق إحباط كل محاولة للتهرب منها
- حماية المملكة المتحدة وغيرها من الدول من الهجمات الإلكترونية من خلال تعطيل البنية التحتية التي يستخدمها الأعداء لتنفيذ تلك الهجمات
- حماية المدنيين في الأزمات الإنسانية عن طريق الحفاظ على قدرتهم على الحصول على معلومات حيوية

القوة الوطنية لأمن المعلوماتية، باعتبارها مركزا وطنيا للعمليات المؤثرة على مستوى الفضاء الإلكتروني ومن خلاله، سترفع من قدرة المملكة المتحدة على تطوير وتكامل واستخدام هذه القدرات إلى جانب غيرها، ورفع درجة كفاءتها لتحقيق الأثر المطلوب.

الشبكة الوطنية لمكافحة الجريمة الإلكترونية التابعة لجهاز إنفاذ القانون

تأسست الشبكة الوطنية لمكافحة الجريمة الإلكترونية خلال فترة الاستراتيجية الوطنية لأمن المعلوماتية 2016-2021، وقد طورت استجابة متكاملة كليا للجرائم الإلكترونية، وهي مستعدة لتوفير استجابة مستندة للمعلومات لكافة أشكال الهجمات الإلكترونية التي تُشن ضد الأفراد والمؤسسات أو قطاعات بأكملها. تُعتبر الشبكة نظاما يغطي البلاد بأكملها. وهي تعمل على المستويات الوطنية والإقليمية والمحلية، وتقدم الرعاية للضحايا وتساعد الشركات والأفراد لحماية أنفسهم وعلى التعافي بسرعة، وتسعى لتحقيق العدالة الجنائية ضد مرتكبي الهجمات.

الوحدة الوطنية لمكافحة الجريمة الإلكترونية التابعة للوكالة الوطنية لمكافحة الجريمة توفر القيادة والتنسيق على المستوى الوطني للاستجابة للهجمات، تدعمها في ذلك شبكة من **الوحدات الإقليمية لمكافحة الجريمة الإلكترونية** في تسعة أجهزة شرطة إقليمية في كل من إنجلترا وويلز، وبالتشارك مع نظرائها في شرطة اسكتلندا وإيرلندا الشمالية، وكذلك مع وحدة الجرائم الإلكترونية التابعة لشرطة مدينة لندن.

وهذه الوحدات تساندها **وحدات محلية لمكافحة الجريمة الإلكترونية** ملحقة بكل واحدة من قوى الشرطة الثلاث وأربعين، ويجري تنسيقها عن طريق منسق إقليمي. بإمكان هذه الوحدات المحلية والإقليمية التحقيق في الجرائم ومطاردة مرتكبيها، ومساعدة الشركات وضحايا الاعتداءات في حماية أنفسهم من الهجمات، كما تعمل الوحدات مع الشركاء لمنع استدراج الأشخاص الضعفاء لأجل ارتكاب جرائم إلكترونية.

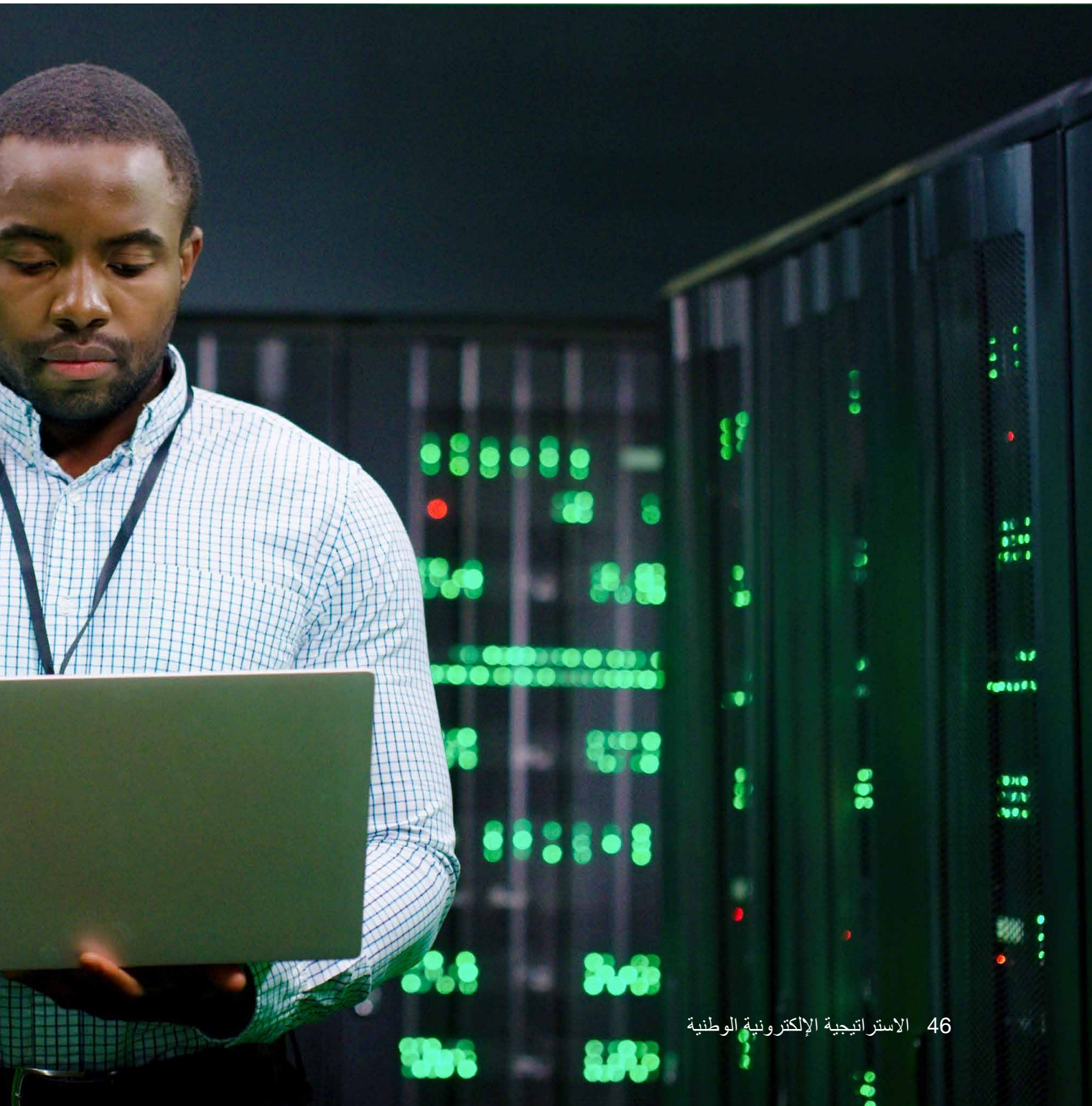
أما الإبلاغ عن الجرائم مركزياً وتقييمها وتحليلها فيتولاه **مركز مكافحة الاحتيال** الذي يتبع **شرطة مدينة لندن**. بعد ذلك تُحال الجرائم الأكثر خطورة وتعقيدا إلى الوكالة الوطنية لمكافحة الجريمة وللشبكة الإقليمية لمتابعة التحقيق بها. أما باقي الحالات، فيجري توزيعها على قوات الشرطة المحلية. كما تنسق شرطة لندن أعمال دعم الضحايا، بما في ذلك من خلال **وحدة رعاية ضحايا الجرائم الاقتصادية**.

يجري إدماج الأنظمة مع قدرات التحليل الجنائي والمخابرات وتبادل المعلومات من أجل تأسيس منصة واحدة بحيث يُتاح للوحدات الوطنية والإقليمية الاستفادة من القدرات والأدوات المتخصصة المتقدمة التي يجري تطويرها لمكافحة الجريمة. ذلك يشمل القدرة على العمل المشترك بشكل فعال مع الشركاء في أجهزة الأمن والمخابرات، وخاصة بالنسبة للاستجابة للتهديدات من الجماعات الإجرامية والدول. واستمرارا للعمل بمبدأ "لتأسيسها مرة واحدة، يلزم تأسيسها على المستوى الوطني لتستفيد منها كامل شبكة منع الجريمة الإلكترونية"، فإن تلك القدرات مُتاحة أيضا للوحدات المحلية لمكافحة الجريمة الإلكترونية من خلال المنسقين الإقليميين. هذه المقاربة الشاملة توفر بالفعل استجابة أقوى بكثير لتهديدات الجرائم الإلكترونية.

وستستمر الشبكة الوطنية لمكافحة الجريمة الإلكترونية في قيادة استجابة العدالة الجنائية للنشاطات الخبيثة في الفضاء الإلكتروني، وبصرف النظر عمن يقف خلف التهديد على المستوى الدولي أو الوطني أو الإقليمي أو المحلي. وذلك تدعمه مجموعة من السبل الأخرى المُحبطة للتهديدات، ومنها ما يلي على سبيل المثال لا الحصر:

- تطوير قدرات إلكترونية متخصصة ومتطورة لأعمال التحقيق وإحباط الهجمات
- الاستفادة من الشبكة الدولية الواسعة للوكالة الوطنية لمكافحة الجريمة من أجل دعم جهود الدول الشريكة من خلال تقديم المعلومات الاستخباراتية والأدلة
- منع الجماعات الإجرامية من الانتفاع من أنشطتها، وذلك بإحباط استغلالها لأسواق الجريمة والخدمات التي تُسهّل عملها
- حماية المملكة المتحدة وغيرها من الدول من الجرائم الإلكترونية عن طريق إفشال وتعطيل عمل البنية التحتية المستخدمة في تنفيذ الجرائم
- الإسهام في فرض العقوبات على منفذي الهجمات، وتحميلهم المسؤولية علنا حتى ولو كانوا على أعلى مستوى
- مصادرة العملات الرقمية وغيرها من الأرصدة كونها من عائدات الجريمة الإلكترونية

الجزء 2:
التطبيق



الدعامة 1:
البيئة الإلكترونية في المملكة المتحدة

تقوية البيئة الإلكترونية في المملكة المتحدة

63. لكي تنجح هذه الاستراتيجية، علينا ضمان أن يكون لدى المملكة المتحدة المختصون والمعرفة والشراكات المناسبون. ويجب أن تتوفر لدينا قوى عاملة متنوعة وعالية المهارة الفنية، ومجتمع بحثي حيوي، وقطاع إلكتروني منافس عالمياً، وبيئة ابتكارية إقليمية مزدهرة تمكننا من أن نكون في الطليعة في مجالات التكنولوجيا الحيوية، وأن يكون كل ذلك مرتكزاً على شراكات متينة بين الحكومة والقطاع والجامعات.

64. يحتاج نمو البيئة الإلكترونية لأن يكون مستداما بذاته، أي ألا يكون معتمدا على المبادرات الحكومية. وعلى مدى هذه الاستراتيجية، سوف ننتقل من تمويل مجموعة من المهارات وبرامج الابتكار المتخصصة والمُدارة مركزيا إلى مقاربة إقليمية عامة أكثر استدامة. وسنرتكز على الإصلاحات الحكومية الأوسع للمهارات وأنظمة التعليم من أجل دعم وتحفيز المزيد من الأفراد على اكتساب المهارات التي يحتاجونها لامتهان العمل في المجال الإلكتروني. وسنعطي الأولوية لمجموعة من الإجراءات الملموسة لزيادة تنوع قوة العمل في القطاع الإلكتروني. ذلك لا يعني فقط ضمان أن تكون تلك الوظائف والمهن متاحة للجميع، بل أيضا أن تكون حيوية لأمننا الوطني، بما يضمن أن نسخّر مواهب ومهارات جميع فئات الشعب. وسوف نعمل أيضا على ضمان أن يعود نمو القطاع الإلكتروني بالفائدة على كامل أنحاء المملكة المتحدة وليس فقط لندن ومنطقة جنوب شرق إنجلترا التي تحتضن قرابة 45% من العاملين في هذا القطاع وتستقطب 85% من الاستثمارات الخارجية.[22]

65. بشكل عام، سوف نتبنى دورا أكثر استراتيجية، حيث سنسهّل الجمع بين قيادات القطاع الإلكتروني، والأكاديميين، والمبتكرين، وأجهزة إنفاذ القانون، والمعنيين بالأمن القومي وغيرهم ممن يرغبون بالعمل معا لجعل المملكة المتحدة أكثر صمودا في وجه التهديدات الإلكترونية. كما سننسق ما هو متاح للحكومة لدعم البيئة الإلكترونية، بدءا من كيفية تدريس المجال الإلكتروني في المدارس إلى كيفية مساندة اللوائح الاقتصادية للمعايير من أجل ضمان أن تتمكن المملكة المتحدة من تطوير القدرات الحيوية الضرورية لحماية نفسها ضد التهديدات في المستقبل.

[22] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة، تحليل قطاع الأمن الإلكتروني 2021 (2021)

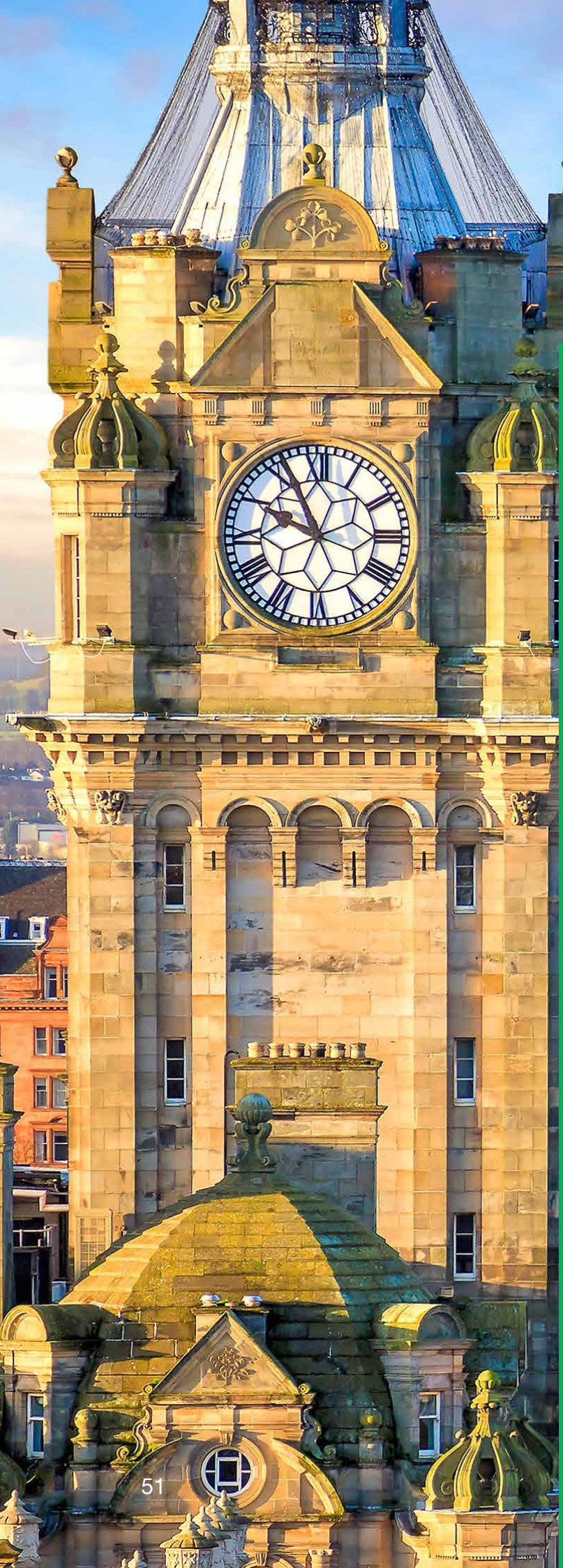
الهدف 1:
تقوية الأسس والشراكات والشبكات اللازمة لدعم مقاربة قوة إلكترونية تشمل المجتمع بأكمله

66. القوة الإلكترونية تتطلب مقاربة تعتمد على إشراك المجتمع بأكمله. وتفوقنا التنافسي سيكون بفضل قدرتنا على تطوير وتسخير المواهب في كافة أنحاء المملكة المتحدة، وبأن يكون لدينا الأفراد المناسبين الذين يعملون معا بالأساليب المناسبة في كافة أنحاء القطاع العام والقطاع الإلكتروني والجامعات لحشد المجتمع الإلكتروني بأكمله. وسيكون علينا تشكيل شراكات للتنفيذ متكاملة فعليا مع القطاع وضمان مقاربة جغرافية واسعة الإطار في مختلف بلدان ومناطق المملكة المتحدة، والعمل بشكل وثيق مع الحكومات المفوضة في إيرلندا الشمالية واسكتلندا وويلز، واغتنام الفرص التي توفرها القوة الإلكترونية للارتقاء بالمناطق الأقل حظا. سوف نحقق النتائج التالية بحلول 2025:

67. حوار إلكتروني وطني استراتيجي أكثر شمولا مع القطاع والجامعات والمواطنين من خلال تأسيس مجلس استشاري وطني للقطاع الإلكتروني، وهو مجلس جديد عالي المستوى، والبناء على أسس الشبكات القوية أصلا للنمو الإلكتروني، وشراكات الصمود، ومراكز التميز الجامعية للأبحاث والتعليم بمجال الأمن الإلكتروني.

68. إنشاء **شبكات إلكترونية إقليمية أكثر تكاملا وفاعلية في أنحاء المملكة المتحدة** ذلك يتيح تأسيس شراكات أقوى بين الحكومة والشركات والجامعات لدعم نمو القطاع الإلكتروني وصمود الشركات. وسنعمل مع المراكز الإلكترونية الإقليمية، ومع مؤسسة تعاون التجمعات الإلكترونية في المملكة المتحدة (مؤسسة تعاون التجمعات الإلكترونية UKC3) التي أُنشئت مؤخرا، ومع العدد المتنامي من تجمعات الابتكار الإلكتروني الإقليمية، ومراكز الصمود الإلكتروني، بما يقوي الروابط بين الشركات المحلية ومراكز التميز الجامعية وأجهزة إنفاذ القانون.

69. هذه الخطوات سوف تركز على مجموعة من العلاقات القائمة بين المركز الوطني لأمن المعلوماتية والأطراف المرتبطة به، وبين وزارات الحكومة والجهات الرسمية وقطاعات الاقتصاد التي تمثلها، بما في ذلك البنية التحتية الوطنية الحيوية، والجهات التنظيمية، والحوار الحكومي الأوسع نطاقا مع القطاع الإلكتروني والقطاع الرقمي والتكنولوجي.



كيارا ميتشيل، رئيسة قسم الفضاء الإلكتروني في مؤسسة ScotlandIS

كيارا هي أيضا مدير التجمع الإلكتروني في اسكتلندا، وعضو مجلس إدارة مؤسسة تعاون التجمعات الإلكترونية.

"لعب التجمع الإلكتروني الإسكتلندي دورا هاما في دعم مجتمع الأمن الإلكتروني في اسكتلندا. وهناك فهم متزايد للخبرات في اسكتلندا بشأن إدارة التجمعات والفرص للاعتماد على قطاع إلكتروني مزدهر. وبما أنه بات يوجد تقدير أكبر لأهمية التجمعات، أتشرف بأن يكون لي دور أساسي في مؤسسة تعاون التجمعات الإلكترونية كمسؤولة تطوير البيئة الإلكترونية. من خلال هذه المؤسسة سوف ينصب التركيز بشكل أكبر على التعاون والابتكار وتطوير المهارات، ما سيوفر منصة لنمو قطاع الأمن الإلكتروني في المملكة المتحدة."

المؤسسات الإلكترونية (ممثلو المواقع)

التجمعات الإلكترونية في المملكة المتحدة

1. التجمّع الإلكتروني في بريستول وباث
2. التجمّع الإلكتروني في الشمال
3. التجمّع الإلكتروني في ويلز
4. التجمّع الإلكتروني في تشيلتنهام
5. تجمّع الأمن الإلكتروني في شرق إنجلترا
6. التجمّع الإلكتروني في ميدلاندز
7. التجمّع الإلكتروني في اسكتلندا ScotlandIS
8. تجمّع الأمن الإلكتروني في جنوب غرب إنجلترا
9. تجمّع الأمن الإلكتروني في يوركشاير
10. التجمّع الإلكتروني في إيرلندا الشمالية
11. تجمّع الأمن الإلكتروني في شمال غرب إنجلترا
12. التجمّع الإلكتروني في غرب إنجلترا

- مركز التميز الأكاديمي لتعليم الأمن الإلكتروني
- القيادة الحكومية المركزية للاتصالات/ موقع المركز الوطني لحماية المعلوماتية
- مركز التميز الأكاديمي للتغيير بمجال أبحاث الأمن الإلكتروني*
- مؤسسات الحكومات المفوضة

*النقطة الحمراء والخط الأسود يشيران إلى كل من تعليم الأمن الإلكتروني وأبحاث الأمن الإلكتروني.

1. مركز صمود الأعمال لمنطقة شمال شرق إنجلترا
2. مركز الصمود الإلكتروني لمنطقة وسط إنجلترا
3. مركز الصمود الإلكتروني لمنطقة إيست ميدلاندز
4. مركز الصمود الإلكتروني لمنطقة ويست ميدلاندز
5. مركز الصمود الإلكتروني لمنطقة جنوب شرق إنجلترا
6. مركز الصمود الإلكتروني لمنطقة جنوب غرب إنجلترا
7. مركز الصمود الإلكتروني في ويلز
8. مركز الصمود الإلكتروني لمنطقة شرق إنجلترا
9. مركز الصمود الإلكتروني لمدينة لندن


مركز صمود الأعمال الاسكتلندي
جامعة أبرتاي
جامعة إدنبرة نابيير
جامعة إدنبرة
شراكة اسكتلندا الإلكترونية
جامعة كوينز، بلفاست
جمعة نورثمبريا
جامعة نيوكاسل
مركز الأمن الإلكتروني في إيرلندا الشمالية
جامعة لانكاستر
القيادة الحكومية المركزية للاتصالات، سكاربورو
القوة الوطنية لأمن المعلوماتية
القيادة الحكومية المركزية للاتصالات، مانشستر
جامعة برمنغهام
جامعة دي مونفورت
القيادة الحكومية المركزية للاتصالات/ المركز الوطني لحماية المعلوماتية، تشيلتنهام
جامعة ووريك
جامعة جنوب ويلز
جامعة كامبريدج
جامعة كارديف
جامعة أكسفورد
جامعة غرب إنجلترا
جامعة بريستول
كينغز كوليدج لندن
إمبريال كوليدج لندن
يونيفيرسيتي كوليدج لندن
القيادة الحكومية المركزية للاتصالات، بود
جامعة كنت
رويال هولواي
جامعة كنغزتون
جامعة سَري
جامعة ساوثامبتون

الهدف 2:
تعزيز وتوسيع نطاق المهارات الإلكترونية في البلاد على كافة المستويات، بما في ذلك من خلال تطوير مهنة الأمن الإلكتروني بحيث تكون متنوعة وعالمية الطراز وقادرة على إلهام وتأهيل المواهب المستقبلية.

70. سيكون جزءا أساسيا من طموحات المملكة المتحدة أن توفر موارد مستدامة ومتنوعة من ذوي المهارات العالية للعمل في القطاع الإلكتروني، بحيث يكونون قادرين على توفير العناصر الأساسية للاقتصاد الرقمي، إلى جانب ابتكار وتطوير مقاربات جديدة. من شأن ذلك أن يدعم هدفنا بأن نكون القدوة من خلال اكتشاف الخبرات والحفاظ عليها في كافة أنحاء القطاع العام، وزيادة قدراتنا في مؤسسات إنفاذ القانون والدفاع والأمن، بما في ذلك القوة الوطنية لأمن المعلوماتية. وكما هي الحال بالنسبة لأجزاء أخرى من هذه الاستراتيجية، سنعمل مع الحكومات المفوضة في اسكتلندا وويلز وإيرلندا الشمالية لضمان اتباع مقاربة ثابتة في كافة أنحاء البلاد بشأن مبادرات الحكومة البريطانية حول القضايا التي تهم ويلز وإيرلندا الشمالية واسكتلندا، مثل التعليم والمهارات. سوف نحقق النتائج التالية بحلول 2025:

71. ارتفاع كبير في أعداد الأفراد الذين لديهم المهارات التي يحتاجونها للانضمام لقوة العمل الإلكترونية، وذلك بالاستناد إلى العمل الذي يجري في البلدان الأربعة في المملكة المتحدة من أجل أن تلبي سياسات التعليم والمهارات احتياجات الأفراد وجهات العمل. سننجز ذلك من خلال عدد من الإجراءات التي تشمل توسيع نطاق برامج التدريب لمن تزيد أعمارهم عن 16 سنة بما ينسجم مع احتياجات قوة العمل الإلكترونية، وتمويل مجموعة من دورات التدريب على المهارات في مجال الأمن الإلكتروني، وتعميم برنامج معاهد التكنولوجيا على المستوى الوطني، والاستمرار في برنامج CyberFirst للمنح الدراسية للطلاب الجامعيين. ذلك يبني على أسس عمل الحكومة في تنسيق معظم التعليم والتدريب لمن هم فوق 16 سنة وفقا لمعايير معززة تضعها جهات العمل، وذلك بحلول 2030. وسيجري تطوير تلك المعايير بالاشتراك مع المجلس البريطاني لأمن المعلوماتية في المملكة المتحدة لصالح القطاع الإلكتروني الأشمل، وهي ستدعم برامج التدريب في العمل، والجهود لتوفير تدريب فني، ومنح مؤهلات فنية جديدة بمستوى أعلى. من شأن ذلك ضمان أن يكون لجهات العمل دور محوري في تصميم وتطوير المؤهلات والتدريب.

72. مهنة أمن إلكتروني أعلى جودة وأكثر رسوخا وتنظيما ومعترفا بها على نطاق أوسع.
المجلس البريطاني لأمن المعلوماتية، يدعمه الامتياز الملكي الذي حصل عليه، سيضع معايير مهنية ومسارات تؤدي إلى امتهان العمل في القطاع الإلكتروني، بالاعتماد على مشروع بنك المعرفة حول الأمن الإلكتروني (CyBOK)، وهو مشروع رائد عالمياً. كما سنسعى لتوظيف جميع الإمكانات الحكومية، بما فيها التشريعات، لترسيخ هذه المعايير في كافة قطاعات هذه المهنة، وضمان تقدير تميُّز وخبرات كافة العاملين في القطاع الإلكتروني بوضوح وبشكل دائم.

73. قوة عمل إلكتروني أكثر تنوعا، وإعطاء شرائح المجتمع ضعيفة التمثيل - وتلك التي من مجتمعات محرومة في كافة أرجاء المملكة المتحدة - دعما فعالا أكبر لكي تمتهن العمل في القطاع الإلكتروني وتنجح فيه. مجموعة الإجراءات التي سنتخذها ستشمل تقديم الدعم لمزيد من النساء لدخول قوة العمل بالقطع الإلكتروني، ولمبادرات محددة تدعم المجموعات ضعيفة التمثيل لكي تترقى إلى مستويات عليا. وسوف نعتمد على نجاحات أنشطة خارج المناهج التعليمية، تُقدّم من خلال برنامجنا الرائد CyberFirst، بما في ذلك مسابقة CyberFirst للفتيات. كما سنزيد من فرص الحصول على التعليم والعمل للشباب المعرضين للخطر من خلال برنامج الخيارات الإلكترونية Cyber Choices الذي تديره الوكالة الوطنية لمكافحة الجريمة، بحيث نبعدهم عن النشاط الإلكتروني غير المشروع، وندفعهم باتجاه فرص إيجابية تتيح لهم استغلال مواهبهم وحماسهم.

74. تدفق متواصل ومتنوع من الأفراد الموهوبين الذين يتخرجون من نظامنا التعليمي. سوف نشجع وندعم مزيدا من الشباب للانخراط في المجالات التكنولوجية من خلال التعليم. ذلك يشمل زيادة أعداد وتنوع المرشحين لهذه المجالات الذين يدرسون علوم الكمبيوتر ضمن موادهم في المرحلة 10 و11 وما يعادلها من مؤهلات في اسكتلندا، والذين سيواصلون دراستهم للحصول على مؤهلات مثل المؤهل العلمي الفني في إنجلترا، والتدريب أثناء العمل وفرص التعليم العالي. كما سنعمل أيضا على رفع مهارات المعلمين في إنجلترا من خلال المركز الوطني لتعليم الكمبيوتر، وضمان أن تتوفر لهم الموارد وفرص التطوير التي تساعدهم في تنمية الاهتمام لدى المزيد من الطلبة للتخصص في هذا المجال.

75. جعل الحكومة أكثر قدرة على التعرف على خبراء المجال الإلكتروني الذين تحتاج إليهم، ومن ثم توظيفهم وتدريبهم والاحتفاظ بهم. ولكون الحكومة وقطاعها العام أحد أكبر المستخدمين للخبراء بالمجال الإلكتروني، فإنها تحتاج لأن تكون القدوة بحيث تدعم الإجراءات المبينة أعلاه وتبني عليها. وسنتبع مقاربة أكثر تماسكا وفعالية في كامل القطاع العام، وفي نفس الوقت سنتخذ إجراءات محددة لرفع مهارات موظفي الحكومة والقيادات العليا، ونطور قدراتنا في الدفاع والأمن، مثل القوة الوطنية لأمن المعلوماتية، والمركز الوطني لأمن المعلوماتية، ومؤسسات إنفاذ القانون. ذلك يشمل الاستثمار في المواهب الشابة عن طريق توسيع نطاق برنامج المسار السريع لتطوير المهارات الإلكترونية، وتوفير المزيد من فرص التدريب بالعمل بمجال الأمن الإلكتروني، ودعم برامج المهارات المتخصصة ضمن إطار الوكالة الوطنية لمكافحة الجريمة، بما في ذلك توظيف الخريجين والمتدربين، وبرامج مصممة خصيصا مثل برنامج شمول الأفراد من جميع القدرات الذهنية، وبرنامج التدريب الصيفي للأفراد من جميع الخلفيات. وسيرتكز ذلك على النجاحات التي حققتها كلية الدفاع الإلكتروني عن طريق رفع مستواها إلى أكاديمية الدفاع الإلكتروني، والتي ستقدم تدريبا أشمل عن القدرات الإلكترونية الدفاعية والهجومية، والتعاون بنفس الوقت مع الجامعات والقطاع والشركاء الدوليين.

المجلس البريطاني لأمن المعلوماتية

تأسس المجلس البريطاني لأمن المعلوماتية في مارس 2021، وهو الأول من نوعه في العالم ومتخصص بالأمن الإلكتروني. مهمة المجلس أن يكون ناطقا باسم هذه المهنة، وأن يوفر الرؤية الواضحة والهيكلية لقوة العمل الإلكترونية المتنامية، ويمنح العديد من المؤهلات والشهادات المتوفرة في هذا المجال. يُعتبر تأسيس المجلس خطوة جوهرية تنبع من إدراكنا أن المهن الإلكترونية تضم قطاعا واسعا من التخصصات والخبرات الفنية وغير الفنية التي تغطي كامل قطاع الاقتصاد، وتماثل في اتساعها المهن الأكثر عراقة مثل الطب والقانون.

للمجلس أربع غايات هي:

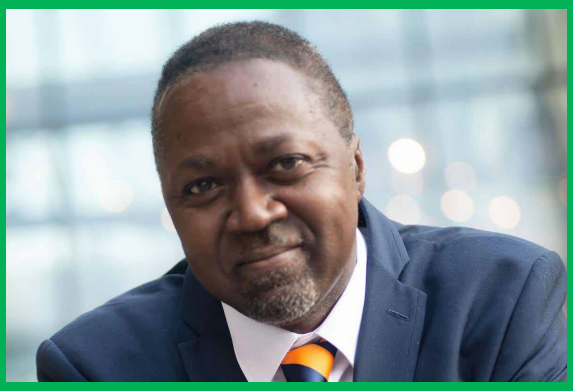
- القيادة الفكرية والمعايير المهنية: قيادة الجهود الهادفة إلى وضع المعايير التي تحدد نطاق الأمن الإلكتروني والاتفاق بشأنها
- الوظائف والتعلم: دعم جهات العمل والأفراد في عملية اتخاذ القرار في اختيار المهنة، مع تقديم المشورة بشأن مهارات الأمن الإلكتروني والتطور المهني والتميز به
- الأخلاقيات المهنية: توفير مبادئ إرشادية يتمكن من خلالها محترفو المهنة والمؤسسات من إظهار الممارسات الأخلاقية في مجال الأمن الإلكتروني
- التنوع والشمولية: الترويج للأمن الإلكتروني كفرصة مهنية للأفراد من كافة الأعمار والخلفيات الاجتماعية، مع بذل الجهود لإزالة العوائق التي تمنع الأفراد من الانخراط في هذه المهنة

يطمح المجلس لأن يتطور ويرسخ مصداقيته واستدامته كسلطة مهنية على امتداد فترة هذه الاستراتيجية. وهو سيضم مجموعة من المؤسسات المهنية الحالية والجهات التي تمنح التراخيص. وسيعمل على تحديد وتمكين مؤسسات الخبرة التي يمكنها أن تقدم الإرشاد بشأن متطلبات التطور والكفاءة للداخلين الجدد إلى هذا المجال، وللممارسين الحاليين، ولجهات العمل على حد سواء.

وكانت الملكة قد وافقت على منح المجلس البريطاني لأمن المعلوماتية الامتياز الملكي في نوفمبر 2021. من شأن ذلك أن يمنحه، للمرة الأولى، اعتمادا معترفا به مخصصا للأمن الإلكتروني، ويغطي العديد من التخصصات في هذا القطاع.

ندرك أن هناك المزيد مما يلزم عمله من أجل ترسيخ المعايير والمسارات المهنية في كامل نطاق البيئة الإلكترونية، بما في ذلك كل المؤسسات الحكومية، وقطاعي الدفاع وإنفاذ القانون. وسيلعب المجلس دورا هاما في هذا المجال، بحيث يدعم الأفراد وأولئك الذين يسعون إلى تغيير مهنهم لينتقلوا إلى العمل في المجال الإلكتروني.

سايمون هيبورن، المدير التنفيذي للمجلس البريطاني لأمن المعلوماتية



ينطوي عملي على تطوير المجلس البريطاني لأمن المعلوماتية لكي يصبح "الناطق باسم مهنة الأمن الإلكتروني". يعتبر المجلس مؤسسة ذاتية التنظيم لمهنة الأمن الإلكتروني في المملكة المتحدة. ونحن نسعى لتوحيد هذا القطاع لكي يطور وينشر ويوجه معايير معتمدة على المستوى الوطني للقطاع الإلكتروني من أجل جعل المملكة المتحدة المكان الأكثر أمنا للعيش فيه وللعمل على الإنترنت. تأسس المجلس رسميا في مارس 2021 عقب مشروع تأسيس ناجح، وقد فتحنا الآن الباب لطلبات العضوية. وتعتبر الاستراتيجية الإلكترونية الوطنية عنصرا بالغ الأهمية من أجل ضمان أن يتمكن الأفراد والمؤسسات من العمل بأسلوب يطور المهنة، والمجلس هو أحد المنسقين الأساسيين لتلك الجهود.

الهدف 3:
رعاية نمو قطاع أمن إلكتروني وأمن معلوماتية بحيث يكون مستداما ومبتكرا وقادرا على المنافسة عالميا، ويقدم منتجات وخدمات عالية الجودة تلبي احتياجات الحكومة والاقتصاد بشكل أعم.

76. لتعزيز قوتنا الإلكترونية الوطنية، ودعم النمو والصادرات الرقمية، تحتاج المملكة المتحدة لقطاع إلكتروني حيوي مكون من شركات عالية الجودة وجديرة بالثقة. والشركات البريطانية رائدة عالمياً بما تقدمه من تقنيات وتدريب ومشورة لكل من القطاع الإلكتروني والحكومات في المملكة المتحدة وفي أنحاء العالم. لكن لتطوير أرقى التقنيات، تحتاج بعض الشركات للدعم وللحصول على الاستثمار لكي تبلغ المرحلة التي يمكنها فيها أن تقدم منتجات مجدية اقتصاديا.

77. كما تحتاج الشركات لأن تشعر بالثقة بأنها تبتكر بما ينسجم مع المعايير المُعتمدة من قبل الحكومة، والتي تتبعها المؤسسات الأخرى أيضا. وهناك المزيد مما يمكننا فعله لمساعدة المشترين على إيجاد ما يرغبون به في هذه الساحة المعقدة، والتي تتوفر فيها تشكيلة هائلة من المنتجات والخدمات المتفاوتة في جودتها. وهذا بدوره سينشّط الطلب في البيئة الإلكترونية ويدعم النمو. سوف نحقق النتائج التالية بحلول 2025:

78. قطاع إلكتروني يكون قد حقق نموا عالميا سنويا فوق المعدل بما في ذلك من خلال التجارة والصادرات الإلكترونية. وسوف نساعد شركات القطاع الإلكتروني لدخول أسواق جديدة في الداخل والخارج، وذلك من خلال دعم فعاليات إلكترونية رائدة عالميا في المملكة المتحدة، ودعوة شركاتنا الأكثر ابتكارا في القطاع الإلكتروني لتشارك في البعثات التجارية والمعارض الإلكترونية الدولية. وسنستخدم مشتريات القطاع العام بشكل أكثر فعالية، ونؤسس دليلا شاملا بمقدمي الخدمات المعتمدين من المركز الوطني لأمن المعلوماتية لتحفيز الطلب على منتجات وخدمات الأمن الإلكتروني عالية الجودة.

79. قطاع إلكتروني أكثر إبداعا ويشهد ارتفاعا بالاستثمار في مراحله الأولى، وعددا أكبر من شركات القطاع الإلكتروني التي تمكنت من إطلاق نشاطها وتنمية وتوسيع عملها. برنامجنا الجديد Cyber Runway يوفر للشركات نقطة مركزية وحيدة لتقديم الدعم، وذلك بالاستفادة من الدروس التي تعلمناها من برامجنا السابقة مثل برنامج Tech Nation Cyber، وبرنامج Cyber101، وبرنامج HutZero. وسنحول مركز تشيلتنهام للابتكار - الذي يضم "المركز الوطني لأمن المعلوماتية للشركات الناشئة"، وهو مُسرّع لشركات القطاع الإلكتروني - إلى مركز عالمي حقيقي للابتكار: المركز الوطني للابتكار الإلكتروني. وسنستفيد من خبرات المؤسسات القائمة حاليا لتطوير وتمكين عمليات الإنشاء المشتركة للمؤسسات، مثل المؤسسة الوطنية لتكنولوجيا الأمن وتبادل الابتكارات. وسنشجع الاستثمارات عالية الخطورة في شركات القطاع الإلكتروني الناشئة في مراحلها الأولى، بما في ذلك من خلال صندوق الاستثمار الاستراتيجي بالأمن القومي، بالتشارك مع بنك الأعمال البريطاني.

80. اقتصاد إلكتروني بريطاني تطوّر بشكل كبير، مع نمو متزايد خارج جنوب شرق إنجلترا، الأمر الذي يساهم في تعافي الاقتصاد من فيروس كورونا (كوفيد-19)، ويدعم النشاطات الاقتصادية الإقليمية. كما سننشئ مركز قيادة دائم للقوة الإلكترونية الوطنية في ساملیسبیري Samlesbury في الشمال الغربي من إنجلترا، بما يدفع النمو في القطاعات التكنولوجية والرقمية والدفاعية خارج لندن، ويساعد في خلق شراكات جديدة في المنطقة. سوف نرفع من دعمنا للمبتكرين ورجال الأعمال خارج لندن وفي جنوب شرق إنجلترا من أجل تطوير منتجاتهم وخدماتهم، وتنمية أعمالهم واستخدام موظفين ذوي مهارات. ويشمل ذلك مجمع غولدن فالي Golden Valley بقيادة مجلس تشيلتنهام، والمخصص لدعم نمو شركات تكنولوجيا الأمن الإلكتروني. وسنزيد من قدرات التصدير لدى الشركات الإلكترونية في مختلف أرجاء المملكة المتحدة من خلال المشاركة مع المجموعات الإلكترونية الإقليمية، وتنظيم معارض ومنتديات لإظهار المزيد من مواهب قطاعنا الإلكتروني للمشترين الدوليين.

81. عدد أكبر من الشركات القادرة على تقديم تقنيات ومنتجات وخدمات الأمن الإلكتروني التي تستوفي معايير الجودة المعتمدة بشكل مستقل، وبالتالي رفع ثقة المستخدمين. سننجز ذلك بما ينسجم مع الورقة البيضاء للمركز الوطني لأمن المعلوماتية بشأن مستقبل ضمان التكنولوجيا ونشرها في سبتمبر 2021، حيث سنستخدم اسم المركز الوطني لأمن المعلوماتية وخبراته لبناء سوق جديرة بالثقة لتساعد المستهلكين في المملكة المتحدة على شراء الخدمات بثقة، وعلى وتحسين أمنهم، ورفع كفاءة الأمن الإلكتروني على المستوى الوطني.[23]

[23] المركز الوطني لأمن المعلوماتية، ورقة بيضاء: مستقبل ضمن التكنولوجيا في المركز الوطني لأمن المعلوماتية (2021)

بيرتا بابنهايم، المدير التنفيذي والمؤسس لشركة سايبرفيش Cyberfish

شاركت شركة سايبرفيش في برنامج حكومي لتعزيز التقنيات الإلكترونية. مهمتنا هي مساعدة الشركات وفرق العمل بالحكومة للاستعداد للتعامل بشكل أفضل مع حالات توقف العمل، مثلا بسبب حوادث إلكترونية. ونفعل ذلك من خلال إجراء تمارين محاكاة للحوادث مع تلك الشركات والفرق، ومراقبة تصرفاتهم في العمل الجماعي تحت الضغط النفسي للحادث، ومن ثم إرشادهم لكيفية إدخال التحسينات. الكثير من المستشارين يتقنون إما الجانب الفني من الاستجابة للحوادث أو الجانب السلوكي للقيادة وصناعة القرار. أما نحن، فنفعل الاثنين معا، ولدينا خبرة معرفية في كلا الجانبين. وقد ساعدت تمارينا 500 من قياديي القطاع ممن يعملون ضمن فرق عمل حيوية في مختلف أرجاء العالم على تغيير منظورهم وتحسين عملهم الجماعي، الأمر الذي يؤدي إلى رفع كفاءة استجابتهم للأزمات، وتحسين آلية اتخاذ القرار.

هل لديك اهتمام في الانضمام للقوى العاملة بالمجال الإلكتروني أو تأسيس شركتك الخاصة بهذا المجال؟

82. كانت استراتيجيتنا السابقة قد أعطت اهتماما كبيرا لبناء قاعدة المهارات الإلكترونية وقطاع خدمات الأمن الإلكتروني في المملكة المتحدة. وكما هو مبين في السياق الاستراتيجي، أحرزنا تقدما كبيرا في **تنمية القطاع وزيادة الصادرات** :

مساعدة شركات القطاع الإلكتروني على إيجاد أسواق دولية. صدّرت المملكة المتحدة خدمات إلكترونية بقيمة 4.2 مليار جنيه إسترليني في عام 2020.

موقع Cyber Exchange (التبادل الإلكتروني)، بوابتنا الإلكترونية على الإنترنت، وهو تجمع شركات القطاع الإلكتروني من كافة أرجاء المملكة المتحدة.

شراكات النمو الإلكتروني تجمع الحكومة والقطاع في العمل معا من أجل إزالة العوائق أمام النمو.

83. قدمنا الدعم للمبتكرين من أجل تنمية أعمالهم والارتقاء بها ، ما أدى إلى ازدهار البيئة الإلكترونية في المملكة المتحدة على مدى السنوات الخمس الماضية:

برنامج المركز الوطني لأمن المعلوماتية لدعم الشركات الناشئة ينبه المبتكرين إلى أكثر التحديات الاستراتيجية صعوبة، وقد شارك أكثر من 160 شركة ناشئة في تجارب جديدة.

مكتب لندن للتقدم السريع في الأمن الإلكتروني LORCA ساعد 72 شركة من المبتكرين بالمجال الإلكتروني في جمع استثمارات تفوق 200 مليون جنيه إسترليني، وتحقيق عوائد تزيد عن 37 مليون جنيه.

برنامج Cyber Runway يقدم الدعم للمبتكرين من أجل إطلاق وتنمية وتوسيع شركاتهم - بالبناء على نجاح برنامج HutZero وبرنامج Cyber101.

84. نواصل العمل لتلافي نقص سنوي يبلغ 10,000 في أعداد المهنيين **الذين ينضمون إلى قوة العمل بالقطاع الإلكتروني** :[24]

برنامج CyberFirst للمنح الدراسية يدعم طلاب الجامعات، ويوفر المئات من الأفراد الذين لديهم الخبرة العملية للانضمام إلى قوة العمل بالقطاع الإلكتروني كل عام.

هناك الآن أربعة معايير للتدريب بالمجال الإلكتروني مصممة من قبل القطاع، وثلاثة عروض بهذا المجال للمخرجات الأولية للتعلم التي تُقدَّم من خلال مبادرة "دورات من أجل الوظائف" التابعة لوزارة التعليم.

توجد تسع دورات تدريب إلكتروني يدعمها الصندوق الوطني للمهارات الذي تأسس مؤخرا، وهذه الدورات تعرّف الأفراد على مهن مشوقة في القطاع الإلكتروني، وهناك خطط لتنظيم المزيد من هذه الدورات كل سنة خلال فترة الإنفاق التالية.

85. نعمل على **رفع حرفية القوى العاملة في القطاع الإلكتروني** من أجل تبسيط الأمر بالنسبة للمؤسسات لفهم ما تحتاجه من مهارات، وللتسهيل على الأفراد في البحث عما يلزمهم أن يعرفوه:

يعتبر المجلس البريطاني لأمن المعلوماتية جهة مهنية هي الأولى من نوعها في العالم في أمور الأمن الإلكتروني. وقد بدأ المجلس بوضع معايير مهنية واضحة وثابتة اعتمادا على العمل الذي أنجزته لحد الآن الهيئات المهنية القائمة. سيسعى المجلس ليحدد بوضوح المؤهلات الفعالة من الكم الكبير المتوفر منها حاليا.

بنك المعرفة حول الأمن الإلكتروني (CyBOK) يُرشد ويدعم برامج التعليم والتدريب المهني لقطاع الأمن الإلكتروني.

[24] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة، فهم مجموعة التوظيف بمجال الأمن الإلكتروني (2021)

86. نعمل **لضمان أن يتمكن كل فرد من الانضمام لقوة العمل في القطاع الإلكتروني،** ومعالجة كل مسائل عدم المساواة في هذا القطاع والذي تشكل النساء فيه نسبة 16% فقط، بينما 3% فقط من المناصب القيادية تشغلها نساء وأشخاص من الأقليات العرقية.[25]

شارك في دورات CyberFirst وبرنامج Discovery قرابة 300,000 من الشباب الذين تتراوح أعمارهم بين 11-17 على مدى السنوات الخمس الماضية.

مؤسسة تعاون التجمعات الإلكترونية في المملكة المتحدة. UK Cyber Cluster Collaboration تؤسس شراكات بين القطاع والمدارس والكليات الجامعية لضمان أن تتوفر الفرص والخبرات في كافة مناطق المملكة المتحدة.

برنامج الخيارات الإلكترونية التابع للوكالة الوطنية لمكافحة الجريمة يقدم المساعدة للشباب لكي تكون خياراتهم مبينة على معلومات صحيحة، وليستخدموا مهاراتهم الإلكترونية بطريقة مشروعة. كما يرفع البرنامج من درجة الوعي ويقدم بدائل أفضل مثل دورات التدريب والتوظيف.

[25] الحكومة البريطانية، مهارات الأمن الإلكتروني في سوق العمل في المملكة المتحدة (2021)

الدعامة 2:
الصمود الإلكتروني

بناء تقنية رقمية قوية ومزدهرة في المملكة المتحدة

87. يُعتبر الأمن إلكتروني والقدرة على الصمود من أساسيات أهدافنا الاستراتيجية الأعم كقوة إلكترونية: فبدونهما لا يمكننا أن نتطلع لتحقيق الاستفادة القصوى من إمكانات التقنيات الرقمية للنهوض بشكل أفضل، وبحيث نكون أكثر عدلا وقوة، ولحماية المزايا الاستراتيجية للمملكة المتحدة في الفضاء الإلكتروني ومن خلاله. يتعين علينا الاستمرار في بناء دفاعات إلكترونية قوية، واتخاذ الخطوات اللازمة لحماية الشبكات الرقمية ومعلومات وموارد المملكة المتحدة على المستوى الوطني والمحلي والفردي، ولضمان أن تكون قادرة على الصمود حين وقوع الحوادث.

88. وبينما نركز في هذا الفصل على الصمود الإلكتروني، فإنه لكي يكون هذا المسعى فعالا بشكل كامل يجب أن يكون جزءا من جهد كلي يشمل المجتمع بأكمله من أجل تحسين قدرات الصمود في المملكة المتحدة. الاستراتيجية الوطنية للصمود التي ستصدر لاحقا، وهي أحد التعهدات الرئيسية الواردة في المراجعة المتكاملة، ستحدد المقاربة واسعة النطاق إزاء الصمود الوطني.

89. تم إحراز تقدم كبير في العقد الماضي من حيث تحسين قدرتنا على الصمود الإلكتروني، وذلك بإنشاء المركز الوطني لأمن المعلوماتية، وتوافر المزيد من النصح والإرشادات وغيرها من الأدوات، وتطبيق قوانين من بينها اللوائح بشأن الشبكات وأنظمة المعلومات، ولائحة حماية البيانات العامة، وقانون حماية البيانات لعام 2018. لكن لا يزال لدينا ثغرات خطيرة. فالانتهاكات الإلكترونية تُلحق الضرر بالحكومة والشركات والمؤسسات والأفراد، وما تزال مؤسسات عديدة تُبلغ عن تعرضها لانتهاكات أو اعتداءات.

90. سنبني على أسس الاستراتيجية السابقة، ونعمل على تغيير مقاربتنا وتعزيز قدرة المملكة المتحدة على الصمود - مع التركيز بشكل خاص على:

- الارتقاء بعملنا من أجل جعل الإنترنت أكثر أمنا بشكل تلقائي، ومنع الهجمات، وتوفير أساليب حماية أساسية لتستفيد منها كافة الشركات والمؤسسات والمواطنين في المملكة المتحدة، وزيادة الدعم المُتاح لأولئك الأقل قدرة على حماية أنفسهم على الإنترنت
- وضع هدف للحكومة لكي تكون مثالا يُحتذى في أفضل الممارسات في مجال الأمن الإلكتروني
- ترسيخ الأمن الإلكتروني كجزء أساسي من العمل الجيد عن طريق التطبيق الأفضل للوائح والمحفّزات، وتسخير قوة فهمنا العميق للتهديدات لبناء مجتمعات قادرة على الدفاع عن نفسها
- دعم كل ذلك بأدلة وبيانات ومعايير قابلة للقياس بشكل موضوعي، والانتقال من جمع البيانات إلى مرحلة التصرف بناء عليها

91. مفهوم الصمود الإلكتروني في هذه الاستراتيجية له ثلاثة أوجه. أولا، الحاجة إلى فهم طبيعة **الخطر**. وثانيا، ضرورة اتخاذ الخطوات **لحماية** الأنظمة ولمقاومة الهجمات الإلكترونية. وثالثا، انطلاقا من إدراكنا بأن بعض الهجمات ستحصل مهما كلف الأمر، علينا أن نستعد لها، وأن تكون لدينا القدرة على **الصمود** بما يكفي للإقلال من ضررها، وأن نتمكن من التعافي من أثرها.

92. ستكون مقاربتنا مصممة لكل فئة من المستخدمين، وتدعمها قدرات وطنية تمكننا من معالجة الأخطار العامة. الفئات التي نسعى لحمايتها والتأثير بها تشمل المواطنين والشركات والمؤسسات والحكومة والقطاع العام، وأولئك الذين يُشغّلون بنيتنا التحتية الوطنية الحيوية (الذين يوفرون لنا الخدمات الأساسية التي نعتمد عليها جميعا مثل مياه الشرب والكهرباء والخدمات المالية والنقل والاتصالات).

93. سنركز أولا على الخطوات اللازمة لحماية البيئة الرقمية لكل مستخدمي الإنترنت في المملكة المتحدة، ولمنع الهجمات، وبناء الأمن الأساسي في المنتجات والخدمات، ومساعدة الأفراد والشركات الصغيرة والمؤسسات في اتخاذ الخطوات الأساسية لتحسين أمنهم الإلكتروني. أما بالنسبة للجهات التي لديها مسؤوليات وقدرات أكبر تستدعي اتخاذ إجراءات إضافية لتعزيز الأمن والصمود بما ينسجم مع حجم الخطر المحتمل، فإن ذلك يبلغ أعلى مستوى من الحماية المتوقعة للخدمات العامة الرئيسية والهامة التي يعتمد عليها شعبنا واقتصادنا.

94. يجب أن يكون ذلك جهدا مشتركا بين الحكومة وكافة قطاعات الاقتصاد والمجتمع. حيث تقع على كاهل مجالس إدارات الشركات والمؤسسات مسؤولية إدارة المخاطر الإلكترونية الخاصة بها. وغايتنا هي أن نحدد توقعات واضحة يساندها الإطار المناسب من الحوافز والدعم واللوائح من أجل تمكين إدخال تحسينات، وإزاحة عبء مخاطر الأمن الإلكتروني عن كاهل المستخدمين وتوجيهه نحو أولئك الذين هم في الوضع الأمثل لإدارة المخاطر.

95. نطلب من وزارات الحكومة، والقطاع العام الأوسع نطاقا، ومشغلي البنية التحتية الوطنية الحيوية الخاضعين للتنظيم أن يبادروا إلى رفع معاييرهم وإدارة مخاطرهم بشكل استباقي. ونتوقع من الشركات والمؤسسات الكبرى، بما في ذلك مقدمي الخدمات والمنصات الرقمية، أن يتحملوا مسؤولية أكبر عن حماية أنظمتهم وخدماتهم وعملائهم كجزء رئيسي من إدارتهم لأعمالهم. وبدورها، ستزيد الحكومة من جهودها لتأمين الحماية للبيئة الرقمية، وللتصدي للأخطار العامة، وتوفير الدعم من خلال النصح والأدوات الأخرى، وضمان الاعتماد في الأسواق، وتطوير المهارات التي تمكّن من إدخال التحسينات.

96. ينبغي أن تكون جهودنا لتعزيز الصمود الإلكتروني في المملكة المتحدة جزءا كذلك من تواصلنا على الصعيد الدولي. حيث إن تزايد عولمة سلاسل التوريد، ومنصات تكنولوجيا المعلومات، والشركات متعددة الجنسيات، والإنترنت بحد ذاته، يعني أنه لا يمكننا رفع كفاءة الأمن الإلكتروني للمملكة المتحدة بمعزل عن الآخرين. وللاستجابة لهذا التحدي، سيكون علينا الاستمرار في بناء فهم أفضل للروابط بين الصمود الإلكتروني في المملكة المتحدة وعلى المستوى العالمي، ومعالجة المجالات عالية الخطورة، والعمل مع الشركاء الدوليين لبناء صمود يُسهّل التحول الرقمي والأمن والتجارة لتحقيق المنافع المتبادلة، كما هو مبين في الدعامة 4: القيادة الدولية.


خفض الأعباء على الجميع
العمل مع مقدمي الخدمات الإلكترونية من أجل توفير حماية أفضل لمستخدمي الإنترنت في المملكة المتحدة، وبناء أساليب حماية أساسية في الخدمات المتوفرة للمواطنين على الإنترنت
توسيع نطاق تعزيز الدفاعات الإلكترونية، ومنع وإحباط الجرائم الإلكترونية وعمليات الاحتيال
توعية المواطنين والممارسات الإلكترونية السليمة.
شركات ومؤسسات أكثر صمودا
رفع مستوى المعايير مثل أساسيات المجال الإلكتروني والمزيد من الشفافية
حوافز السوق والمزيد من الدعم المحلي
تنظيم أفضل في مجالات مُستهدفة بعينها، بما في ذلك الخدمات الرقمية والبيانات الشخصية
خدمات عامة أكثر صمودا
كافة مؤسسات الحكومة قادرة على الصمود في وجه أساليب الهجمات المعروفة بحلول 2030
مزيد من المساءلة والمعايير والضمانات المستقلة
الاستثمار في معالجة تكنولوجيا المعلومات القديمة
بنية تحتية وطنية حساسة وأكثر صمودا
الصمود بوجه أساليب الهجمات المألوفة، وحماية متقدمة وفقا لطبيعة الخطر
فهم ومعالجة المخاطر الناجمة عن الرقمنة ومجالات التكنولوجيا الجديدة

الهدف 1:
تحسين الفهم للمخاطر الإلكترونية من أجل التحفيز على اتخاذ خطوات أكثر فاعلية بشأن الأمن الإلكتروني والصمود

97. سنحقق شراكة أكثر قوة بين الحكومة والشركات والمؤسسات لتحفيز الفهم الجماعي للمخاطر، وتوجيه الأولويات، ووضع المُسوّغات للعمل. وسوف ندعم المواطنين من خلال العمل مع الشركات والمؤسسات التي تقدم الخدمات للمستهلكين، ونقوي قدرة الحكومة على تحديد المخاطر التي تصيب قطاعات واسعة. سوف نحقق النتائج التالية بحلول 2025:

98. سيكون لدى الحكومة فهم استراتيجي مُحدّث للمخاطر الإلكترونية التي تواجهها المملكة المتحدة، وستستخدم هذا الفهم لتحديد الأخطار العامة، وإبلاغ القطاعات المعنية بالأولويات، والمضي قدما بالاستراتيجية وبتطبيقها. سوف نجني ونحافظ على فوائد أكبر من استثماراتنا الكبيرة في مجال "فهم التهديدات" في الاستراتيجية الوطنية لأمن المعلوماتية التي نشرناها سابقا، وسنؤسس على الجهود الحالية لفهم المخاطر في عالم مترابط إلكترونيا بشكل متزايد. يشمل ذلك التعرف على المواقع التي تكون فيها سلاسل التوريد الرقمية متركزة بشكل كثيف، والعمل مع الشركاء الدوليين لإدارة المخاطر الجماعية. كما سوف نُحسّن من تسجيل المخالفات لقانون إساءة استخدام الكمبيوتر، وفهم الصلات بين اختراق البيانات والأعمال الإجرامية السائدة، وزيادة فهمنا لكيفية كون مخالفات قانون إساءة استخدام الكمبيوتر تسهل الأنواع الأخرى من النشاط الإجرامي.

99. ستكون الحكومة القدوة في فهمها للمخاطر الإلكترونية. سنتبنى إطار التقييم الإلكتروني الخاص بالمركز الوطني لأمن المعلوماتية كإطار ضمان لكافة وزارات الحكومة. وسيجري تحديد الأنظمة الحيوية والموردين المعروفين. سوف ننشئ مركزا حكوميا جديدا للتنسيق الإلكتروني وخدمة الإبلاغ عن نقاط الضعف في كافة مؤسسات الحكومة، لتمكين الحكومة من "الدفاع كوحدة واحدة" عند إدارة الحوادث ونقاط الضعف والتهديدات. ستسعى خدمة الإبلاغ عن نقاط الضعف لإقامة علاقات مهمة وموثوقة مع مجتمع الأبحاث الأمنية بما يؤدي إلى خفض نقاط الضعف في كافة المباني الحكومية. كما سنواصل تقديم الدعم والتنسيق بمبادرات مماثلة في الحكومات المفوضة، مثل مقترح إنشاء جهاز تنسيق مركزي للصمود الإلكتروني في اسكتلندا.

100. سيكون لدينا فهم أعمق للمخاطر الإلكترونية في كافة مجالات البنية التحتية الوطنية الحيوية. وسنزيد من تبنينا لإطار التقييم الإلكتروني أو ما يعادله في كافة قطاعات البنية التحتية الحيوية، وسنحسّن من تماثل ذلك الإطار مع أطر أخرى مستخدمة لتقييم الأمن الإلكتروني والإبلاغ عن نقاط الضعف. وسنكمل المراجعات المتعلقة بحساسية القطاعات، ونحدد التبعيات ضمن إطار البنية التحتية الوطنية الحيوية وسلاسل توريدها. وسنؤسس شراكات أقوى مع مالكي البنية التحتية الوطنية الحيوية ومشغليها من أجل تحسين فرص الحصول على المعلومات عن التهديدات والمخاطر، والاتفاق على الخطوات التي يجب اتخاذها إزاء المخاطر. وسنحاول فهم المخاطر الجديدة، أو أين ستبرز بنى تحتية حيوية نتيجة الرقمنة ومجالات التكنولوجيا الجديدة، وذلك كجزء من أولويات أشمل مثل التحول إلى خفض الانبعاثات إلى الصفر.

101. سيكون لدى الشركات والمؤسسات في المملكة المتحدة فهم أفضل للمخاطر الإلكترونية ولمسؤولياتها بشأن إدارة هذه المخاطر. سنساعد المؤسسات لبلورة فهم أفضل للمخاطر التي يتعرض لها عملاؤها، بما في ذلك كيفية إساءة استغلال البيانات التي لديها لتسهيل الجرائم، مثل الاحتيال وسرقة الشخصية أو الابتزاز. وسنتشارك مع المؤسسات المزيد من المعرفة المُستخلصة من الأبحاث والبيانات عن انتشار الهجمات الإلكترونية وتأثيرها، وعن التقدم النسبي الذي تحرزه القطاعات في تحسين الأمن الإلكتروني.

الهدف 2:
منع ومقاومة الهجمات الإلكترونية بشكل أكثر فاعلية عن طريق تحسين إدارة المخاطر الإلكترونية داخل مؤسسات المملكة المتحدة، وتوفير حماية أكبر للمواطنين

102. يعتمد أسلوبنا في منع ومقاومة الهجمات الإلكترونية على الافتراضات التالية: (أ) أن تتحمل المؤسسات مسؤولية اتخاذ الخطوات اللازمة لإدارة المخاطر التي تواجهها، لكن هناك حاجة لأطر مساءلة أقوى وإدارة جيدة على نطاق واسع لتحقيق هذه الأولوية؛ (ب) أن الحكومة لها دور في العمل مع القطاع من أجل اتخاذ الخطوات للإقلال من الخطر بشكل مباشر على نطاق واسع حيثما تكون الحكومة في مكانة مميزة تؤهلها لأن تفعل ذلك؛ (ج) أن علينا ضمان توفير الدعم والإرشاد لمساعدة الأفراد، والمشاريع الفردية، والشركات والمؤسسات الصغيرة على إدارة المخاطر الإلكترونية التي يتعرضون لها. سوف نحقق النتائج التالية بحلول 2025.

103. ستخفض الحكومة الكثير من الضرر الذي قد يصيب المملكة المتحدة، كما ستخفض من الأعباء على مواطنيها. سنعمل بجد أكبر في الحكومة لصالح مستخدمي الإنترنت في المملكة المتحدة، بحيث نتوسع في إجراءاتنا لتعزيز الدفاعات الإلكترونية من أجل دعم نطاق أوسع من القطاعات، بما في ذلك الجمعيات الخيرية والجامعات والشركات الصغيرة والمتوسطة والمواطنين. كما سنقوي أساليب الحماية للخدمات المقدمة على الإنترنت عن طريق التواصل بشكل أكبر مع القطاع وتبادل المعلومات معه.

104. يتمم هذا العمل أولويات الحكومة الأخرى التي تهدف لحماية مواطني المملكة المتحدة على الإنترنت، مثل مشروع قانون السلامة على الإنترنت، وسياسة التصدي للجرائم الإلكترونية مثل الاحتيال.

105. ذلك يعني العمل بشكل وثيق أكثر مع القطاعات المعنية، مثل مقدمي الخدمات على الإنترنت، والاتصالات اللاسلكية، والتكنولوجيا، والمصارف وقطاع التجزئة، من أجل توفير حماية أفضل لمستخدمي الإنترنت البريطانيين. من ضمن ذلك: جعل تسجيل المواقع الإلكترونية للأغراض غير المشروعة أكثر صعوبة، وزيادة حذف وحجب مواد المحتوى الضار على الإنترنت، وتحسين استرداد وإعادة الهويات المسروقة، وتعزيز أمن البنية التحتية للاتصالات في المملكة المتحدة. كما سوف نطوّر خيارات أخرى لتقديم دعم قانوني لأساليب حماية المواطنين في حال تبين أن الترتيبات الطوعية غير كافية.

106. كذلك ستشمل جهودنا لخفض الضرر على نطاق واسع التصدي للمخاطر العامة التي ترد من سلسلة التوريد الرقمية. وحيثما تدعو الحاجة، سنتدخل للتشجيع على تنويع سلاسل التوريد، مثلما نفعل الآن في قطاع الاتصالات؛ وسنقوي أمننا الاقتصادي الجماعي من خلال تبادل المعلومات بشكل أفضل، واتباع مقاربات متينة ومُجرّبة ومتناسبة إزاء التدقيق في الاستثمارات الخارجية المباشرة في القطاعات الحساسة، وفرض متطلبات واضحة على موردي المواد العامة والحساسة للحكومة.

107. تقوية الوظائف الحساسة التي تقوم بها الحكومة بشكل كبير في مواجهة الهجمات الإلكترونية، وستكون كافة مؤسسات الحكومة في القطاع العام أكثر صمودا أمام نقاط الضعف المعروفة وأساليب الهجمات بحلول 2030. هدفنا هو جعل القطاع العام في المملكة المتحدة قدوة في مجال أفضل الممارسات. ودعما لهذا الهدف، سننشر أول استراتيجية حكومية مخصصة لأمن المعلوماتية. تركز هذه الاستراتيجية على إجراءات أكثر فاعلية لإدارة المخاطر والحوكمة والمساءلة؛ والقدرات المطورة والمستخدمة مركزيا (بما فيها تعزيز الدفاعات الإلكترونية)؛ ومراقبة أكثر شمولا للأنظمة والشبكات والخدمات؛ واستجابة سريعة وواسعة للحوادث؛ والاستثمار في المهارات والمعرفة، وفي ثقافة تنمي التغير المستدام.

108. إدارة المخاطر الإلكترونية للبنية التحتية الوطنية الحيوية بفاعلية أكبر. فهذه الخدمات بطبيعتها هي أكثر ما تعتمد عليه الدولة. وسنستمر في العمل الوثيق مع مشغلي تلك الخدمات لتحقيق الصمود في مواجهة أساليب الهجمات الشائعة وبالسرعة الممكنة، ولتطبيق أساليب حماية متقدمة حيثما كان مناسبا. وبالنسبة لمشغلي الخدمات الضرورية المكلفين بموجب اللوائح بشأن الشبكات وأنظمة المعلومات، فإن ذلك يعني كحد أدنى استيفاء المعايير الأساسية التي تضعها الجهات المعنية لكل قطاع.

109. دعما لهذه الغاية، سنعيد النظر في قدرة الحكومة على مساءلة مشغلي البنية التحتية الوطنية الحيوية لضمان أنهم يستثمرون في الأمن الإلكتروني للأنظمة الحيوية ويديرون المخاطر بشكل فعال، بما في ذلك المخاطر التي تنشأ من سلاسل توريدهم. كما سنقوي الإطار التنظيمي لزيادة مجال تغطيته وصلاحياته وقدرته على التكيف بمرونة ضمن نطاق المخاطر الأمنية الأوسع نطاقا على المستوى الوطني، والتهديدات وأنواع التكنولوجيا سريعة التغير. وسنبدأ ذلك بالتشاور بشأن إدخال إصلاحات على اللوائح بشأن الشبكات وأنظمة المعلومات، بما يؤدي إلى تطبيق إطار أمني جديد لمقدمي خدمات الاتصالات اللاسلكية في المملكة المتحدة، ووضع إطار تنظيمي متناسب لضمان أن أنظمة الطاقة الذكية والمرنة التي تحتاجها المملكة المتحدة في المستقبل للوصول بانبعاثات الكربون إلى الصفر ستكون آمنة وقادرة على الصمود بوجه التهديدات الإلكترونية.

110. إلى جانب ذلك سوف: نعزز قدرات الجهات التنظيمية؛ ونستثمر في المهارات لتحسين قدرة مشغلي البنية التحتية الوطنية الحيوية على اجتذاب مهنيين بالمجال الإلكتروني وتطوير مهاراتهم والاحتفاظ بهم (انظر فصل البيئة الإلكترونية في المملكة المتحدة)؛ وسندعم المشغلين في طريقة إدارتهم لمخاطر سلاسل التوريد عن طريق رفع درجة تعاملنا مع الموردين الحيويين واستكشاف كامل الأدوات المساعدة، بدءا بالإرشادات ووصولا إلى التشريعات ومقترحات الشراء ذات الصلة.

111. البنية التحتية التي يعتمد عليها استخدامنا للبيانات ستكون آمنة وقادرة على الصمود. هذه البنية التحتية هي من الأصول الوطنية الحيوية - فهي تدعم اقتصادنا وتوفر الخدمات العامة وتحفز النمو. وسوف نلعب دورا أكبر في ضمان أن تكون البيانات محمية بشكل كاف أثناء معالجتها أو نقلها أو تخزينها بكميات ضخمة، كما في مراكز البيانات الخارجية على سبيل المثال. وسننشئ إطارا أقوى لإدارة المخاطر لضمان تطبيق أعلى معايير الأمن والصمود في كامل القطاع الإلكتروني، وتطبيق أحكام قانون الأمن القومي والاستثمار لعام 2021 من أجل تقوية التدقيق في الاستثمارات. وسنعزز عملنا مع الشركاء الدوليين لضمان أن الإمكانية المتزايدة للاطلاع على البيانات وتدفقها على المستوى العالمي لن تساهم في زيادة المخاطر الأمنية التي تتعرض لها المملكة المتحدة. كما سنعالج التحديات الأمنية التي تنجم عن جمع كميات ضخمة من البيانات.

112. سندرس أيضا الأهمية المتزايدة لخدمات البنية التحتية للبيانات في المملكة المتحدة في دعم الاقتصاد، ودورها في البنية التحتية الوطنية الحيوية. هذه الإجراءات منسجمة مع التعهدات التي نصت عليها الاستراتيجية الوطنية للبيانات والمراجعة المتكاملة.

113. هناك عدد أكبر من الشركات والمؤسسات البريطانية التي تبادر إلى إدارة مخاطرها الإلكترونية بشكل استباقي، وتتخذ الخطوات اللازمة لتحسين صمودها الإلكتروني. وسنقدم الدعم ونشجع على تغيير السلوك من خلال تطوير حوافز للسوق تشجع الأمن الإلكتروني الفعال. وعند الضرورة، سندعم ذلك بتشريعات موَجّهة لضمان أن تُدار المخاطر الإلكترونية بشكل فعال من قبل من تقع عليهم أكبر مسؤولية لفعل ذلك، وأن تظل التشريعات البريطانية المتعلقة بالأمن الإلكتروني فعالة على ضوء تطور الأخطار والتقنيات الإلكترونية.

114. لدعم هذه الغايات، سنرفع من وتيرة عملنا مع القوى المؤثرة في السوق (المشترين، والمؤسسات المالية، والمستثمرين، والمدققين، وشركات التأمين) من أجل تحفيز المؤسسات لتبني ممارسات جيدة بالنسبة للأمن الإلكتروني في مختلف القطاعات الاقتصادية. وسنقترح إدخال تحسينات على طريقة إبلاغ الشركات عن صمودها في وجه المخاطر، بما فيها المخاطر الإلكترونية. من شأن ذلك أن يوفر للمستثمرين وحَمَلة الأسهم رؤية أفضل للطريقة التي تدير بها الشركات المخاطر المادية التي تتعرض لها أعمالها، وكيفية الحد منها. وسوف نواصل التشجيع على تبني الاعتمادات والمعايير، مثل برنامج اعتماد الأساسيات الإلكترونية، وتطوير مشاركة واسعة في إدارة المخاطر الإلكترونية.

115. ستركز التشريعات الموَجّهة بصورة رئيسية على القطاعات التي يكون فيها للهجمات الإلكترونية أكبر تأثير محتمل، يشمل ذلك مقدمي خدمات أساسية محددة والخدمات الرقمية، وحماية البيانات على المستوى الأشمل في الاقتصاد، وفي الشركات الأكبر حجما. وستكون هذه التشريعات متممة لخطة التنظيم الرقمي، مع التركيز بداية على اللوائح التي تنظم أمن الشبكات وأنظمة المعلومات – كما هو مبين أعلاه وكذلك في الفصل عن التكنولوجيا، والخطوات التالية لإصلاح نظام المملكة المتحدة لحماية البيانات الشخصية.

116. ستتضمن لوائح تنظيم الأمن الإلكتروني ومراجعة الحوافز المزيد من التفاصيل التي توضح الخطوات التي سنتخذها لتحسين صمود الشركات والأمن الإلكتروني في كافة الشركات والمؤسسات البريطانية.

117. سيكون من السهل الحصول على النصائح الفنية، وأدوات المساعدة الذاتية، والمنتجات والخدمات المضمونة لتحسين الصمود الإلكتروني، وهي تتحسن باستمرار، مع التركيز بشكل خاص على مساعدة المواطنين والمشاريع الفردية والمؤسسات الصغيرة.
سنستمر في تطوير إرشادات وأدوات للمساعدة الذاتية تكون دقيقة من الناحية الفنية، وفورية، وقابلة للتطبيق من خلال المركز الوطني لأمن المعلوماتية. وسنضمن أن تكون النصائح الفنية متسقة وواضحة، وأن تُقدّم عن طريق أكثر القنوات فاعلية، سواء كان ذلك من خلال حملات التوعية الإلكترونية، أو الموقع الإلكتروني للمركز الوطني لأمن المعلوماتية، أو الحكومة، أو شبكات إنفاذ القانون، أو الشراكات مع القطاع، كما سنوفر المزيد من الدعم على المستوى المحلي. ومن خلال برنامج "التأهيل الرقمي" التابع لوزارة التعليم، سنستمر في تقديم التمويل الكامل للشهادات في المهارات الرقمية الأساسية للبالغين الذين يحتاجون إليها، بما يضمن أن يحصل الدارسون على المهارات الرقمية الأساسية التي يحتاجونها لكي يكونوا آمنين ومسؤولين على الإنترنت. كما سنساعد الشركات والمؤسسات في كيفية التصرف في سوق الأمن الإلكتروني المعقدة، ونوسّع من شبكاتنا للمنتجات والخدمات المضمونة، ونطور العروض التجارية المتعلقة بالأساسيات الإلكترونية، والتي ستسهّل على الشركات الصغيرة الحصول على الخدمات الأساسية.

إليس باور، مسؤول الحماية ومنع الجرائم الإلكترونية في وحدة تاريان الإقليمية لمكافحة الجرائم الإلكترونية

وحدة تاريان الإقليمية لمكافحة الجرائم الإلكترونية هي عبارة عن فريق متعدد التخصصات مكون من ضباط وعناصر شرطة مُعارين من قوات الشرطة في ويلز. مهمة الفريق المساهمة في توفير بيئة إلكترونية أكثر سلامة وأمنا في جنوب ويلز.

إليس باور هو مسؤول الحماية ومنع الجرائم الإلكترونية في هذا الفريق:

"لا يوجد يوم روتيني في هذه الوحدة، رغم أن ذلك القول قد يبدو عبارة مبتذلة. فقد أكون مسؤولا في أحد الأيام عن تقديم عروض إيضاحية توفر المشورة لإدارات الشرطة الداخلية، أو لمؤسسات خارجية، لضمان أن يكون لديها فهم جيد لكيفية حماية أنفسها وعامليها ضد التهديدات الإلكترونية. أو يمكن في يوم آخر أن أقدم لطلبة المدارس شرحا عن مواضيع تتراوح من السلامة على الإنترنت إلى قانون إساءة استخدام الكمبيوتر لعام 1990. كما أحضر بشكل دوري اجتماعات مع الوكالات والقوات الشريكة لمناقشة التهديدات الجديدة والإرشادات المتعلقة بها للمتلقين. وأتواصل أيضا مع المؤسسات التي تلقينا منها إشعارات بوجود نقاط ضعف، وأشارك في عمليات على المستوى الوطني، أو أكون ضيفا في فعاليات ومؤتمرات ذات صلة. وكذلك أجد متسعا من الوقت لتطوير مهاراتي وتوسيع قاعدة معلوماتي باستمرار".

الهدف 3:
تقوية الصمود على المستوى الوطني والمؤسساتي للاستعداد للهجمات الإلكترونية والاستجابة لدى وقوعها والتعافي منها

118. على الرغم من الجهود المبذولة لفهم المخاطر واتخاذ خطوات وقائية، ستقع لا محالة بعض الحوادث من حين لآخر. نحتاج إلى تقوية قدراتنا في إدارة الحوادث والاستجابة لدى وقوعها في جميع المؤسسات للإقلال من الضرر الذي تُحدثه، ولتوفير دعم أفضل للضحايا. سوف نحقق النتائج التالية بحلول 2025:

119. ستزداد فاعلية الإدارة والتنسيق الاستراتيجيين للمملكة المتحدة في الاستجابة للحوادث الإلكترونية الخطيرة على المستوى الوطني. وسوف نبني على أسس خبرة الحكومة في الاستجابة للحوادث الإلكترونية الكبيرة بما يضمن الاستفادة من الدروس المستقاة لتحسين سياساتنا وإجراءاتنا. وسنتشارك خبرتنا في إدارة الأزمات مع شركائنا الدوليين والقطاع، وبالتالي سنتعرف على أفضل الممارسات لدى الجهات الأخرى لتعزيز جاهزيتنا وإجراءاتنا. وسنعمل على ضمان أن يكون لدى فرق إدارة الحوادث في المركز الوطني لأمن المعلوماتية وأجهزة إنفاذ القانون الخبرات والأدوات المطلوبة للاستجابة لكافة أنواع الحوادث التي قد تطرأ، وتنسيق استجابة وطنية لمواجهة التهديدات ذات الأولوية.

120. سيصبح من الأسهل الإبلاغ عن الحوادث الإلكترونية، وأن يتلقى ضحايا الجرائم الإلكترونية دعما أفضل. وستُستخدم المعلومات الواردة في البلاغ للمساعدة في منع الحوادث في المستقبل، ودعم جهاز إنفاذ القانون في إجراء التحقيق، وإحباط خطط مرتكبي الجرائم الإلكترونية وجلبهم للعدالة. ودعما لذلك، سننشئ خدمة وطنية جديدة للإبلاغ عن الاحتيال والجرائم الإلكترونية وتحليلها لتحل محل مركز مكافحة الاحتيال بحلول 2025. وسوف نشجع على المزيد من الإبلاغ عن الجرائم الإلكترونية بطرق أخرى، ومنها عن طريق إنشاء آلية جديدة لدى شرطة حي المال بمدينة لندن للإبلاغ عن الحوادث في الشركات. وفي القطاعات الخاضعة للتنظيم، سوف نمكّن الجهات التنظيمية من طلب الإبلاغ عن مجموعة واسعة من الحوادث، بما ذلك الحوادث التي تم تفاديها قبل أن تتسبب بأضرار. إن بدء عمل الوحدة الوطنية لرعاية ضحايا الجرائم الاقتصادية سوف يحسّن دعم والإرشاد المتوفرين للضحايا في أعقاب ما يمكن أن تكون تجربة تسببت لهم بالضرر والشدة.

121. ستكون الحكومة والبنية التحتية الوطنية الحيوية أكثر استعدادا للاستجابة للحوادث والتعافي منها، بما في ذلك من خلال التخطيط الأفضل للحوادث والتدريب المنتظم على التعامل معها. سنساعد الحكومة البريطانية ومشغلي البنية التحتية الوطنية الحيوية للحصول على ما يحتاجون إليه من التدريب وخدمات إدارة الحوادث بالمجال الإلكتروني من السوق المحلية، وذلك عن طريق توسيع نطاق البرنامج المعتمد للاستجابة للحوادث الإلكترونية الذي أعده المركز الوطني لأمن المعلوماتية، وتقديم برنامج تدريبي جديد.

122. تحسين إمكانات مراقبة المخاطر وكشفها في وزارات الحكومة وفي مختلف المؤسسات الرقمية الحكومية. وسنعمل على ضمان تحديد الدروس المستقاة واستخدامها لتحسين سياساتنا وإجراءاتنا؛ ومشاركة خبرتنا في إدارة الأزمات مع شركائنا الدوليين والقطاع؛ وضمان أن يكون لدى فرقنا المعنية بإدارة الحوادث الخبرات والقدرات والإمكانات المطلوبة للاستجابة لشتى أنواع الحوادث المتغيرة.

123. في البنية التحتية الوطنية الحيوية، سنضع متطلبات واضحة بشأن إجراء التمارين والاختبارات، أو لمحاكاة هجمات الأعداء لدى كافة مشغلي البنية التحتية الوطنية الحيوية، وتحفيز الابتكار والتعاون في مجال الاستجابة للحوادث والتمرين، مع مراعاة الاقتداء بالنماذج الناجحة مثل مركز التعاون الإلكتروني للقطاع المالي. وكجزء من طموحاتنا بشأن التكنولوجيا (المبينة في الفصل التالي)، سننشئ مختبرا وطنيا لأمن التكنولوجيا العملية ليكون أحد مراكز التميز للاختبار والتمرين والتدريب على التقنيات الصناعية الحيوية من أجل بناء القدرات في هذا المجال، بالتعاون مع القطاع والجامعات والشركاء الدوليين.

124. سيكون لدى الشركات والمؤسسات البريطانية فهم أفضل لما يجب عمله في حال وقوع حادث، ومن يجب الاتصال به، ومن يمكنه أن يساعد، وكيفية التعافي من الحادث. سنزيد من فرص الحصول على التدريب والتمرين المدعوم بالخدمات المضمونة التي يوفرها القطاع، بما في ذلك برنامج جديد للاستجابة للحوادث الإلكترونية، وخدمة التدريب على الحوادث الإلكترونية. وسنعمل على ضمان الحصول على الدعم المستمر من مؤسسات إنفاذ القانون في جميع أنحاء البلاد لضحايا الجرائم الإلكترونية من الأفراد، وتشجيع الشركات والمؤسسات الصغيرة على الاستفادة من الدعم المحلي الذي تقدمه المراكز الإقليمية للصمود الإلكتروني في مناطقهم.

دانيال نج، المدير التنفيذي لشركة CyberOwl

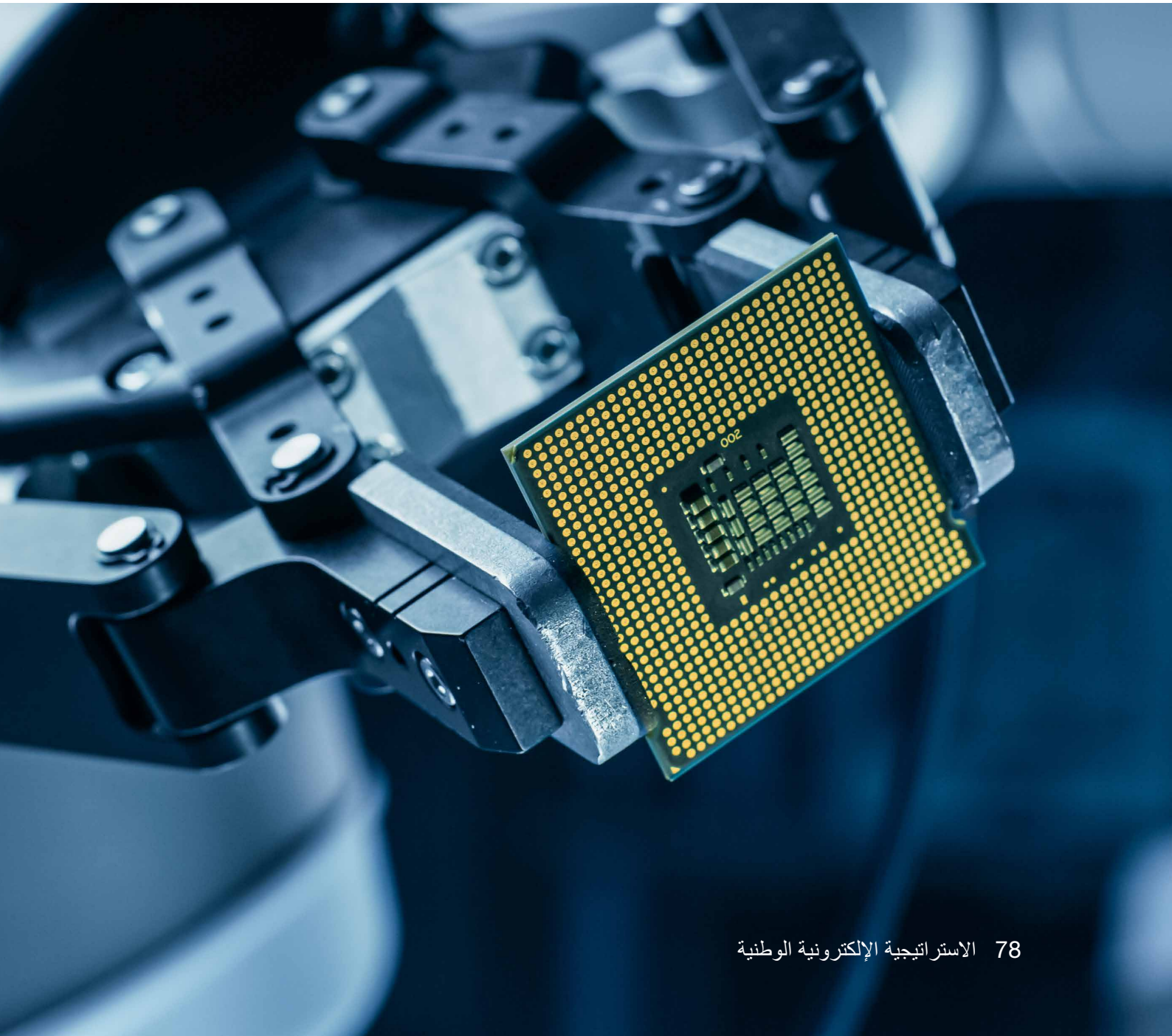
شركة CyberOwl هي أحد المستفيدين من البرنامج الحكومي للتطوير الإلكتروني. ونحن نقدم خدمات المراقبة والتحليل المتعلقة بالأمن الإلكتروني للموارد التشغيلية في قطاع الملاحة البحرية والبنية التحتية الوطنية الحيوية. إن التوجه لتحقيق الاستدامة يتطلب المزيد من الربط الإلكتروني ورقمنة الموارد الميدانية، وهذا ما يعرضها للمخاطر الإلكترونية. وبالتالي تساعد شركة CyberOwl المشغلين في تحديد مواردهم، واستلام إنذار مبكر بشأن المخاطر الإلكترونية، وفي أن يثبتوا لأنفسهم وللجهات التنظيمية أنهم قد حصّنوا أنفسهم ضد تلك الهجمات. نحن نعمل مع أكبر مشغلي موارد الملاحة البحرية في العالم في كافة مناطق أوروبا والشرق الأوسط وأفريقيا ومنطقة آسيا والمحيط الهادئ من أجل تحسين صمود سلسلة التوريد اللوجستي للشحن البحري العالمي. وفي عام 2021، ارتفع الطلب على خدماتنا 14 ضعفا، وازدادت عملياتنا في المملكة المتحدة وسنغافورة بمقدار الضعف.

جن إليس، نائب الرئيس لشؤون المجتمع والعلاقات العامة، شركة Rapid7

يتضمن عملي التحدث إلى خبراء الأمن والقياديين في القطاعات والمؤسسات من جميع الأحجام لفهم التحديات التي يواجهونها، ولمحاولة معرفة الحلول التي تساعدهم في تطوير أمنهم الإلكتروني. وكثيرا ما أسمع أن المؤسسات غارقة بالأعباء ولا تدري على ماذا تركز، ومن أين تبدأ، أو كيف تحقق التقدم. كما يمكن أن يصعب على الموظفين الفنيين الحصول على تأييد من القيادات. وبالتالي يمكن معالجة ذلك من خلال وجود استراتيجية إلكترونية حكومية واضحة وشفافة وثابتة. حيث توفر الاستراتيجية للموظفين الفنيين مرجعا يمكنهم الإشارة إليه في النقاشات مع قياداتهم. كما إنها تحدد المجالات الرئيسية الجديرة بالتركيز عليها، ومسارا محتملا للوصول إلى النضج في المجال الإلكتروني. لا يزال الأمن الإلكتروني شديد التعقيد ولا نهاية له. لكن مع الانتشار الواسع للاستراتيجية الإلكترونية، هناك فهم أكبر لأهميته، والإحساس أن لنا جميعا دور فيه.

الدعامة 3:

التفوق التكنولوجي



الريادة في مجال التكنولوجيا ضرورية لضمان القوة الإلكترونية

125. ستكون بعض التقنيات ضرورية لرسم معالم مستقبل الفضاء الإلكتروني. والدول القادرة على لعب دور ريادي في ذلك المجال ستكون في مكانة أفضل للتأثير على أساليب تصميمها واستخدامها، كما ستكون أكثر قدرة على حماية أمنها وتفوقها الاقتصادي، وأسرع في انتهاز الفرص لتحقيق السبق في القدرات الإلكترونية. ومع تحول التكنولوجيا إلى أداة ذات أهمية متزايدة للقوة الجيوسياسية، ستحتدم المنافسة في هذه الساحة.

126. بالنسبة للمملكة المتحدة، فإن السعي لتحقيق تفوق استراتيجي من خلال العلوم والتكنولوجيا، وتوفُّر البيانات التي تعتمد عليها، سيكون أحد المتطلبات الرئيسية لتحقيق أهدافنا الأشمل كقوة إلكترونية. وقد اتخذت الحكومة خطوات في الاستراتيجيات السابقة لتحفيز الأبحاث والابتكار في تقنيات الأمن الإلكتروني، مثلا عن طريق برامج التسريع في أبحاث الأمن الإلكتروني للشركات الناشئة والمراكز الأكاديمية للتميز، ولتشجيع تطوير أجهزة استهلاكية تكون "آمنة بأساس التصميم". لكننا نحتاج الآن لمقاربة استباقية أكثر طموحا للحفاظ على حصتنا في التقنيات الحيوية، ولتجنب أن نصبح معتمدين أكثر مما ينبغي على المنافسين والأعداء.

127. وضعت المراجعة المتكاملة الخطط لجعل المملكة المتحدة قوة عظمى في مجال العلوم والتكنولوجيا، وتستخدمهما لتحقيق تفوقنا الاستراتيجي والحفاظ عليه. هذه الاستراتيجية تدعم عمل المجلس الوطني للعلوم والتكنولوجيا، ومكتب استراتيجية العلوم والتكنولوجيا في السعي لتحقيق ذلك الهدف، إلى جانب كونها متممة لاستراتيجيات المملكة المتحدة الأخرى في مجالات مثل الذكاء الاصطناعي، والتقنيات الكمية، والبيانات.

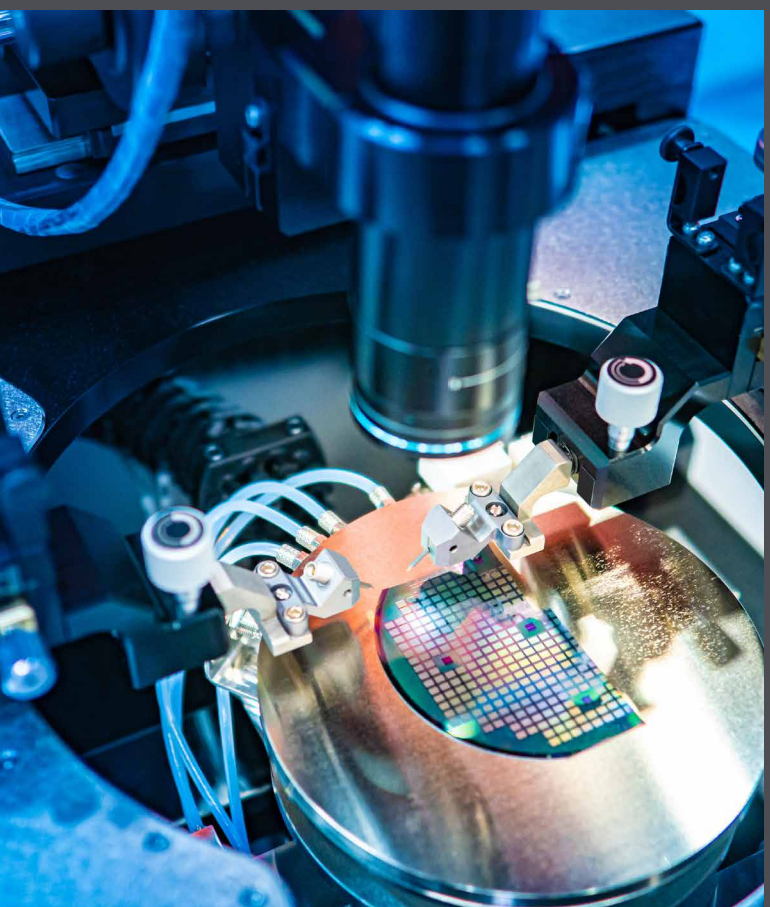
128. سنقوي قدرتنا في مختلف قطاعات الحكومة، تحت قيادة الخبرات الفنية لدى المركز الوطني لأمن المعلوماتية وغيره، من أجل تحديد مجالات التكنولوجيا الأكثر حيوية لقوتنا الإلكترونية. وسنتخذ قرارات استراتيجية على المستوى الوطني بشأن أولوياتنا، بالعمل ضمن مفهوم "التملك-التعاون-التوفر" المشار إليه في المراجعة المتكاملة. وفي بعض المجالات المُختارة، سنستثمر في مجالات الأبحاث والتطوير والشراكات الاستراتيجية التي نحتاجها لتطوير قدرات المملكة المتحدة المحلية. أما في المجالات التي نعتمد فيها على الأسواق العالمية، فسنعمل مع القطاع والجهات التنظيمية والشركاء الدوليين لتشجيع سلاسل التموين الموثوقة والمتنوعة، ولوضع المعايير لضمان أن تكون التقنيات أكثر أمنا وانفتاحا. كما سنعزز قدرة المملكة المتحدة على استغلال وحماية الكميات المتزايدة من البيانات والمعلومات التي تنتج عن الابتكار في مجالات التكنولوجيا الناشئة وتدفع عجلته، وذلك بالاعتماد على الإطار الذي حددته الاستراتيجية الوطنية للبيانات لتحقيق أكبر قدر من الفوائد لاقتصادنا ومجتمعنا.

التقنيات الحيوية للقوة الإلكترونية

ستكون مجموعة متنوعة من التقنيات القائمة والناشئة ذات أهمية حيوية للقوة الإلكترونية للمملكة المتحدة، وعلينا أن نكون قادرين على توقع وتقييم تلك التطورات والعمل على أساسها. نتوقع أن نرتب أولويات العديد من التقنيات والتطبيقات حين نطبق استراتيجيتنا، مثل التقنيات المبينة أدناه. القائمة التالية لن تكون شاملة أو ثابتة، حيث إن أولوياتنا ستستمر في التغير بالتشاور مع القطاع والجامعات والخبراء الفنيين:

- تكنولوجيا الجيل الخامس 5G والجيل السادس 6G، والأشكال الأخرى الناشئة لبث البيانات
- الذكاء الاصطناعي، ويشمل الحاجة لتأمين أنظمة الذكاء الاصطناعي، وإمكانية استخدامه لتعزيز الأمن الإلكتروني في عدد واسع من التطبيقات، مثل مراقبة الشبكات
- تقنية الكتل المتسلسلة وتطبيقاتها، مثل العملات الرقمية والخدمات المالية اللامركزية
- أشباه المحولات ورقائق المعالجات الصغيرة، وهندسة المعالجات الصغيرة، وسلسلة توريدها وتصميمها وعملية تصنيعها
- التحقق بالتشفير، بما في ذلك إدارة التحقق من الهوية والدخول إلى الإنترنت، ومنتجات التشفير عالية الضمان
- إنترنت الأشياء، والتقنيات المستخدمة في البيئات الاستهلاكية والتجارية والصناعية والمادية، مثل المجتمعات المرتبطة بالإنترنت
- التقنيات الكمية، بما في ذلك الحوسبة الكمية، والاستشعار الكمي، والتشفير ما بعد الكمي

هذا العمل سيدعم تحقيق عدد من الاستراتيجيات والمخرجات في مختلف قطاعات الحكومة ويتسق معها. مثال ذلك الاستراتيجية الوطنية للبيانات، والاستراتيجية الوطنية للذكاء الاصطناعي، والمراجعة المتكاملة، بالإضافة إلى المُخرجات التي تركز على التكنولوجيا ضمن هذه الدعامة.



الهدف 1:
تحسين قدرتنا على توقع وتقييم التطورات في مجال العلوم والتكنولوجيا الأكثر حيوية لقوتنا الإلكترونية والتصرف بموجبها

129. لبناء التفوق التنافسي والحفاظ عليه في مجال التقنيات الإلكترونية، علينا أن ننتهج مقاربة منسقة ومتينة وثابتة لتحديد وتحليل المجالات الحساسة من العلوم والتكنولوجيا، وأن نحدد أولويات جهودنا الوطنية. ذلك سيتطلب منا زيادة تطوير خبراتنا البحثية والفنية داخل إطار الحكومة والجامعات. وسوف ندمج ذلك مع الهياكل الحكومية الجديدة لمسح الأفق وجمع المعلومات في مجال العلوم والتكنولوجيا، مع الاعتماد على المعرفة لدى خبراء القطاع، واستغلال شبكتنا في الخارج لفهم الأولويات والأنظمة لشركائنا الدوليين ومنافسينا. سوف نحقق النتائج التالية بحلول 2025:

130. ستكون الحكومة أكثر قدرة على تحليل مجالات العلوم والتكنولوجيا الجديدة والآخذة في التطور، وفهم أثر ذلك بالنسبة للسياسة والاستراتيجية الإلكترونية للمملكة المتحدة. وسنوسع قدراتنا البحثية، بما في ذلك مركز الأبحاث التطبيقية الجديد في مانشستر التابع للمركز الوطني لأمن المعلوماتية، مع التركيز على التكنولوجيا الناشئة في مجالات مثل النقل والمجتمعات المرتبطة بالإنترنت، والعمل إلى جانب الخبراء في المكتب الحكومي للعلوم ومؤسسات أخرى. وسنستفيد من خبرات من خارج الحكومة لدعم المعاهد البحثية الأربعة المتخصصة في الأمن الإلكتروني، ومراكز التميز التسعة عشر المتخصصة في أبحاث الأمن الإلكتروني، وتمويل جوائز باثفايندر Pathfinder Awards للباحثين في المواضيع ذات الأولوية، بالإضافة إلى استغلال تواجدنا في الخارج وشركاتنا الدولية بفاعلية أكبر.

131. هذا الفهم الأفضل يساهم في جعل جهود الحكومة أسرع وأكثر فاعلية بالنسبة لمسح الأفق وترتيب الأولويات وآلية اتخاذ القرار . فهذا يتيح لنا اتباع مقاربة أكثر استباقية لاستغلال الفرص وتخفيف الخطر. وسننشئ آلية جديدة داخلية لمسح الأفق من أجل توقع التطورات في مجال العلوم والتكنولوجيا وتأثيراتها الإلكترونية. وسنتخذ قرارات مبنية على المزيد من المعلومات لترتيب أولويات التقنيات الإلكترونية الأساسية حسب أهميتها، وتوجيه أعمال البحوث والتطوير، ووضع السياسات بحيث تحقق المنفعة لأمن المملكة المتحدة. وحيثما أمكن، سيتيح ذلك مجالا أوسع لاتخاذ القرارات بشأن أولويات العلوم والتكنولوجيا من خلال مكتب استراتيجية العلوم والتكنولوجيا والمجلس الوطني للعلوم والتكنولوجيا.

الهدف 2:
تعزيز والحفاظ على تفوق الدولة وحلفائها في مجال التقنيات الإلكترونية الحيوية للفضاء الإلكتروني

132. سنسعى لتطوير قاعدتنا الصناعية المحلية حيثما كان لدى المملكة المتحدة الإمكانية لتبوّء مركز قيادي أو لتحقيق تفوق تنافسي في المجالات الرئيسية للتكنولوجيا الإلكترونية، أو حيثما يكون الاعتماد على مصادر توريد من غير الحلفاء يشكل أخطارا أمنية غير مقبولة. وستكون هناك بعض المجالات التي نحتاج فيها للاحتفاظ بقدرة سيادية حقة، ومجالات أخرى سنتعاون فيها مع الشركاء الدوليين أو نسعى لإحراز مركز قيادي في أحد جوانب السوق. ذلك سيتطلب مقاربة منسقة من أجل تحفيز الابتكار وأعمال البحوث والتطوير بالتعاون مع القطاع والجامعات. سوف نحقق النتائج التالية بحلول 2025:

133. ستحرز المملكة المتحدة نجاحا أكبر في ترجمة الجهد البحثي إلى ابتكارات وشركات جديدة في مجالات التكنولوجيا الأكثر حيوية لقوتنا الإلكترونية. سندعم الجامعات في كافة أنحاء المملكة المتحدة لتحويل أبحاثها إلى منتجات تجارية وعملية، وذلك من خلال تبني مقاربة تقوم على التحدي بالتعاون مع شركائنا في القطاع. من شأن ذلك أن يؤدي إلى التعرف على الأفكار التي لها أكبر الفرص للنجاح، وتحفيز الاستثمار من الجهات الممولة. وسوف نبني على أسس المقاربة الموضحة في استراتيجية الابتكار، والتي تدعم تطوير بيئات أكثر رسوخا بالنسبة لمجالات التكنولوجيا الأساسية، وبما يضمن أن يكون تفوق المملكة المتحدة أشد متانة ويصعب استنساخه.

مايري أونيل، كبير المحققين في مركز تقنيات المعلومات الآمنة

يعتبر مركز تقنيات المعلومات الآمنة (CSIT) أحد أكبر المراكز الجامعية في مجال بحوث تكنولوجيا الأمن الإلكتروني في المملكة المتحدة. هذا المركز ترأسه كبير المحققين البروفيسورة مايري أونيل، وكان قد اختير في 2009 كأحد المراكز الأولى في البلاد للابتكار والمعلومات. ومشاركة المركز الناجحة في مجال البحوث والابتكار والقطاع الإلكتروني قد ساهمت في تنمية سمعته محليا وعالميا خلال العقد الماضي. كان المركز عاملا حيويا في نجاح مركز الأمن الإلكتروني في إيرلندا الشمالية من خلال دعمه لأبحاث المركز، وتوسيع عمل الشركات المحلية، والاستثمارات الخارجية المباشرة في المنطقة. ومنذ انطلاقته في 2009، أصبح يعمل في القطاع الإلكتروني في إيرلندا الشمالية الآن 2,300 موظفا في 104 شركات ويتقاضون 110 مليون جنيه إسترليني من الرواتب كل عام.

134. ستكون المملكة المتحدة في مكانة أقوى كإحدى الدول الرائدة عالميا في مجال تصميم المعالجات الصغيرة الآمنة.[26]
وسوف نعتمد على برنامج "الأمن الرقمي بأساس التصميم" والذي طوّر تكنولوجيا جديدة أكثر أمنا لرقائق الكمبيوتر لحماية البرمجيات من نقاط الضعف. وسنستعين بهذه الخبرة في معالجات الذكاء الاصطناعي لمنح البائعين البريطانيين تفوقا على المستوى العالمي. كما سنعمل مع البرنامج الوطني للتقنيات الكمية لتصميم نموذج أمني للكمبيوترات الكمية، ولضمان أن تكون الشركات البريطانية رائدة عالميا في هذه التكنولوجيا.

135. سيُنظر للمملكة المتحدة على أنها رائدة عالمياً في أبحاث أمن التقنيات العملية وأنظمة التحكم الصناعي الحيوية، وفي قدرتنا على اختبار تلك التقنيات وتطبيقها في المملكة المتحدة . سننشئ مختبرا وطنيا لأمن التقنيات العملية بالشراكة مع القطاع والجامعات. وسيكون المختبر مقراً لبرامج بحثية رائدة عالمياً، ويوفر للحكومة والجيش والقطاع الإلكتروني والشركاء الدوليين المرافق المناسبة لاختبار وتطبيق تلك التقنيات هنا في المملكة المتحدة. وكما أكدته استراتيجية تنويع سلاسل توريد شبكات اتصالات الجيل الخامس 5G، سوف ننشئ المختبر البريطاني للاتصالات اللاسلكية، والذي سيضم الحكومة والجهات التنظيمية والقطاع لدعم الإطار الأمني الجديد للاتصالات اللاسلكية، والمساعدة في زيادة تنوع بائعي تجهيزات الاتصالات اللاسلكية ضمن سلسلة التوريد في المملكة المتحدة.[27]

136. ستكون الحكومة أفضل قدرة على حماية الابتكار والملكية الفكرية البريطانية في التقنيات الإلكترونية الحيوية ضد الأنشطة المعادية بما يحافظ على تفوقنا التنافسي.[28] وسنستثمر في الموارد والخبرات التي نحتاجها لتوفير القيادة الفنية بشأن أمن تلك التقنيات بينما تتطور، ومن ضمنها تقديم الاستشارات بشأن مخاطر الاستثمار الخارجي المباشر بما ينسجم مع أهداف قانون الأمن القومي والاستثمار لعام 2021. وسنواصل العمل مع الشركات والجامعات لخلق بيئة موثوقة في مجالات البحث والتطوير الرئيسية، ووضع تدابير حازمة لمنع سرقة البيانات والملكية الفكرية.

---

[26] المعالجات الصغيرة هي بمثابة الأدمغة بالنسبة للعديد من الأجهزة التي نستخدمها اليوم. وهي واسعة الانتشار، بما في ذلك في المجالات الحيوية مثل الاتصالات، والدفاع، والرعاية الصحية، وكذلك في الكثير من الصناعات الرئيسية. ما يعوق التقدم التكنولوجي في تصميم الأنظمة حاليا هو الهواجس المتعلقة بالأمن والسلامة والتي يفاقمها التعقيد المتزايد للأنظمة.

[27] وزارة الشؤون الرقمية والثقافة والإعلام والرياضة، استراتيجية تنويع سلسلة التوريد للجيل الخامس 5G (2020)

[28] سيكون التركيز بوجه خاص على القطاعات التي حددها قانون الأمن القومي والاستثمار لعام 2021: وهي الروبوتات المتقدمة، والذكاء الاصطناعي، والاتصالات، وأجهزة الحوسبة، والتحقق بالتشفير، والتقنيات الكمية.

الأمن الرقمي بأساس التصميم

سبعون بالمئة من نقاط الضعف الحالية في الأمن الإلكتروني تستغل خطأً في طريقة تصميم المعالجات الصغيرة معروفا منذ سبعينات القرن الماضي تقريبا. تتواجد هذه المعالجات الصغيرة في كل جهاز رقمي، من التلفزيونات وحتى أدوات الاتصالات. تعمل الحكومة العمل مع القطاع التكنولوجي لإصلاح ذلك الخلل. وبحلول عام 2025 سيتوفر تصميم جديد للمعالجات الصغيرة للهواتف الذكية وعدد متزايد من الأجهزة الأخرى.

يتطلب تغيير تصميم المعالجات الصغيرة شراكات واستثمارات عالمية. وبقيادة المملكة المتحدة، وبتوفير 70 مليون جنيه إسترليني من الاستثمارات الحكومية، يجري إدخال المزايا الأمنية في تصميم أجهزة المستقبل، وذلك سيقلل إلى حد كبير من خطر التعرض لهجوم إلكتروني ناجح.

هذه التكنولوجيا التي ستغير قواعد اللعبة قد جرى بحثها وتطويرها في المملكة المتحدة. وتستثمر كبرى شركات التكنولوجيا، مثل مايكروسوفت وغوغل وآخرين، حاليا لإدخال هذه المزايا الأمنية على منتجاتها. كما يعمل الباحثون اليوم في مختلف جامعات المملكة المتحدة على إيجاد طرق جديدة لاستخدام هذه التكنولوجيا الآمنة بشكل أفضل، فيما تدعم الحكومة الشركات البريطانية الصغيرة والمتوسطة لإيجاد أسواق جديدة للمنتجات التي تشتمل على تلك السمات الأمنية الجديدة.

فيل ويلسون، مدير البحوث والتطوير في مجموعة هَت The Hut Group

مجموعة هَت هي شركة تجارة إلكترونية تركز على المنتجات الاستهلاكية سريعة البيع. لدينا أكثر من 200 موقع إلكتروني يعمل على منصة عامة تعالج ما يصل إلى 3,000 طلب بالدقيقة، وبالتالي فإن أمن منصتنا وعملائنا يعتبر أولوية قصوى. ونحن نبذل كمّا هائلا من الجهود لضمان قدرتنا على احتواء أي هجوم إلكتروني. ولهذا السبب، نحن متشوقون جدا لاحتمال استخدام تكنولوجيا الأمن الرقمي بأساس التصميم في أنظمتنا. إن تشغيل أنظمتنا على هذه المعالجات الصغيرة الجديدة الآمنة، والتي يجرى تطويرها من خلال شراكة بين الحكومة والقطاع تبلغ تكلفتها 180 مليون جنيه إسترليني، ستجعل أنظمتنا أكثر صمودا. إلا أن إدارة هذا التحول ستكون معقدة، حيث لا نستطيع تبني تكنولوجيا جديدة ما لم تكن تلبي متطلباتنا بالنسبة للأداء. ولقد كان من دواعي الشرف لنا أن نكون أول مشروع لعرض برنامج الأمن الرقمي بأساس التصميم، ونأمل أن نستفيد من هذا الأمن الجديد في كافة أنظمتنا في المستقبل القريب.

الهدف 2(أ):
الحفاظ على قدرات وطنية قوية وصامدة بمجال مفتاح التشفير تلبي احتياجات عملاء الحكومة وشركائنا وحلفائنا، وتخفف بالشكل الملائم أكثر المخاطر ضررا التي نتعرض لها، بما في ذلك التهديدات من أكثر أعدائنا تمَكُّنا

137. تعبير "مفتاح التشفير" يصف استخدام المملكة المتحدة للتشفير لحماية المعلومات والخدمات الحيوية، والتي تعتمد عليها الحكومة والجيش والأمن القومي في المملكة المتحدة، بما في ذلك حمايتها من هجمات يشنها أكثر أعدائنا تمَكُّنا. التشفير يساند قدرتنا على اختيار كيفية استخدام قدراتنا في مجال الأمن القومي والدفاع. ولكي نكون دولة رائدة عالميا بمجال التشفير، نحتاج لأن تتوفر لدينا المهارات والتقنيات المناسبة في كل من الحكومة والقطاع الخاص.

138. سنواصل الاستثمار في قدراتنا في الحكومة ونعمل مع قطاع التشفير المحلي لضمان أن تظل المملكة المتحدة واحدة من الدول القليلة القادرة على تطوير مفتاح تشفير سيادي في المستقبل. كما سنستمر في لعب دور ريادي عالمي في مجال تقنية مفتاح التشفير، بما في ذلك تقديم الدعم لحلف الناتو كمُورّد للمواد الأساسية. وهذا الموقع القيادي سيعود علينا بالنفع من حيث الحفاظ على قطاع إلكتروني عالي المهارة في المملكة المتحدة، والحفاظ على قوتنا في قطاع هندسي عالي المتانة، مع إمكانية تمكين قدرات جديدة قوية لمجالات أخرى تتطلب ضمانات عالية، مثل البنية التحتية الوطنية الحيوية.

سوف نحقق النتائج التالية بحلول 2025:

139. سيكون لدينا قدرات تشفير أكثر قوة وأمنا، وقاعدة صناعية أكثر استدامة عالمية المستوى تدعم كامل الحلول التي تحتاجها المملكة المتحدة، وتُصدّر إلى بعض الشركاء والحلفاء المختارين. وسوف ندمج قدرات وخبرات الحكومة والقطاع الإلكتروني بفاعلية أكبر، ونتبع مقاربة وطنية أكثر دقة لإدارة القدرات. فذلك يضمن لنا أن ننمي المهارات التخصصية والمميزة التي نحتاجها.

140. سيكون لدى الحكومة البريطانية قدرات وخدمات قوية في مجال التشفير ، قادرة على تلبية الطلبات المتغيرة للمملكة المتحدة وحلفائها، إلى جانب ضمان أن نظل في طليعة أبحاث تطوير تقنية التشفير. وسنوفر قيادة فنية متمكنة لأجل فهم متطلبات المستخدمين وتحسين خدماتنا الأساسية، ومن ضمنها توفير المواد الأساسية وضمان جودة المنتجات والأنظمة. وسنطور خدمات التشفير بالاستفادة من التقنيات الجديدة لجعلها خفيّة وأكثر مرونة.

141. ستكون المملكة المتحدة قد طورت صدارتها العالمية في تقنية التشفير، وزادت من صادراتها للشركاء والحلفاء . وسنحافظ على دورنا الريادي في تحالف العيون الخمس وحلف الناتو والشراكات الدولية الأخرى، ونصيغ معايير دولية جديدة لكي تكون حلول التشفير البريطانية قادرة على العمل مع أنظمة أخرى. كما سنعمل مع القطاع الإلكتروني لزيادة فرص التصدير لأقصى حد.

الهدف 3:
حماية الجيل التالي من التقنيات المترابطة بما يخفف مخاطر الأمن الإلكتروني الناجمة عن الاعتماد على الأسواق العالمية، وضمان أن يتوفر للمستخدمين البريطانيين مصادر توريد متنوعة وجديرة بالثقة

142. سنستمر على مدى العقد القادم في أن نشهد إدخال قوة الحوسبة والاتصال بالإنترنت والأتمتة في المزيد من قطاعات بيئتنا، بما فيها الأجسام المادية والبنية التحتية، وحتى في البشر أنفسهم على المدى البعيد. سيوسع ذلك نطاق الفضاء الإلكتروني، ويزيد بشكل كبير من حجم البيانات المتولدة. وبالتالي ستصبح القدرة على إدارة البيانات بأمان أكثر أهمية من أجل إدارة اقتصادنا بشكل آمن.

143. علينا أن نضمن قدر المستطاع أن يكون الجيل التالي من التقنيات المرتبطة بالإنترنت قد جرى تصميمها وتطويرها واستخدامها بحيث يؤخذ الأمن والصمود بعين الاعتبار، وذلك كجزء من الجهود المنسقة لتبني مقاربة "آمن بأساس التصميم". وبحكم طبيعتها العالمية، فإن سلاسل توريد التكنولوجيا تعني أن علينا استخدام كل الأدوات المتاحة من أجل إدارة مخاطر الاعتماد على التكنولوجيا بفاعلية أكبر. وحيثما أمكن، سنسعى لضمان أن تكون السمات الأمنية مبنية ضمن تصميم الأنظمة. وحين لا نتمكن من ذلك، سنطبق إجراءات مشددة لتخفيف المخاطر، بما في ذلك في اللوائح المحلية، والتعاون الدولي بشأن المعايير. سوف نحقق النتائج التالية بحلول 2025:

144. المنتجات الاستهلاكية المتصلة بالإنترنت التي تُباع في مختلف أنحاء المملكة المتحدة ستكون مستوفية للمعايير الأساسية للأمن الإلكتروني . سوف نُصدر ونطبق قانون أمن المنتجات والبنية التحتية للاتصالات لإتاحة المجال لتوفير الحد الأدنى من معايير الأمن في كافة المنتجات الاستهلاكية الجديدة المتصلة بالإنترنت التي تُباع في المملكة المتحدة. وسندعم الانتقال الإلكتروني الآمن إلى أنظمة طاقة ذكية ومرنة، ومنها نقاط شحن المركبات الكهربائية الذكية وأجهزة الطاقة الذكية. وسنعمل مع الجهات المسؤولة عن وضع المعايير ومع القطاع الإلكتروني والشركاء الدوليين للتأثير على الإجماع العالمي بشأن المعايير الفنية. وسوف نساعد المؤسسات البريطانية في شراء واستخدام وإدارة الأجهزة المتصلة بالإنترنت بطريقة أكثر أمنا، بما في ذلك وضع إرشادات أمنية جديدة بشأن الأجهزة المتصلة بالإنترنت في الشركات.

145. سيُطلب من كبار مقدمي الخدمات الرقمية، كالخدمات السحابية والبرمجيات والخدمات المُدارة ومتاجر التطبيقات، أن تتبع أفضل معايير الأمن الإلكتروني ، بما يساعد في حماية المؤسسات والمستهلكين من التهديدات الإلكترونية. وسوف نقوّي ونوسع نطاق اللوائح القائمة حاليا بشأن مقدمي الخدمات الرقمية، ونعزز قدرة مكتب المفوض المعني بالحقوق المتعلقة بالمعلومات لضمان أن مقدمي الخدمات الرقمية يديرون مخاطر خدماتهم بشكل استباقي. وسنستمر في التواصل مع القطاع، بما في ذلك شركات التكنولوجيا الكبرى، لتسخير خبرات السوق، وضمان أن يؤدي الجميع أدوارهم في تأمين سلاسل التوريد الرقمية في المملكة المتحدة. كما سنكون في طليعة الجهود لتطوير حلول للسياسات الدولية تركز على مُقدمي الخدمات الرقمية.

146. ستكون المملكة المتحدة من أوائل من يتبنون تكنولوجيا المجتمعات المرتبطة بالإنترنت بشكل آمن ومُستدام لما هو لمصلحة المواطنين والشركات. هذه المجتمعات، والتي تُعرف أحيانا بالمدن الذكية، يمكنها توفير فوائد ملموسة للمجتمع: مثل إدارة حركة السير على الطرقات، وخفض التلوث، وتوفير المال والموارد. لكن الترابط البيني الذي يتيح لهذه المجتمعات بأن تؤدي عملها بكفاءة أكبر يخلق أيضا نقاط ضعف إلكترونية ويُفسح المجال للهجمات الإلكترونية. سوف نستند إلى مبادئ الأمن الخاصة بالمركز الوطني لأمن المعلوماتية في المجتمعات المرتبطة بالإنترنت لتقليل المخاطر التي تواجهها الشركات والبنية التحتية والقطاع العام والمواطنون.[29] وسنعزز قدرات السلطات المحلية والمؤسسات مثل المرافئ والجامعات والمستشفيات من أجل شراء واستخدام التكنولوجيا اللازمة في المجتمعات المرتبطة بالإنترنت بشكل آمن. كما سوف نحشد إجماعاً دولياً بشأن مقاربة ثابتة وفعالة إزاء أمن المجتمعات المرتبطة بالإنترنت.

147. سوف نُدخل اعتبارات الأمن الإلكتروني في تصميم أنماط التكنولوجيا الناشئة المستخدمة في المملكة المتحدة. وسنتعرف على التطبيقات الإلكترونية الجديدة والناشئة التي قد تخلق مخاطر أمن إلكتروني، ونضمن أن تكون المملكة المتحدة في طليعة تطوير هذه التقنيات بشكل آمن ومأمون. وفيما تدرس الحكومة الخيارات لقدرة المملكة المتحدة في مجال تكنولوجيا التوأمة الرقمية والبنية التحتية المادية الإلكترونية الأشمل، سنعمل على ضمان أن يكون الأمن الإلكتروني في صميم عملية اتخاذ القرار.[30] كما سنطبق برنامج ضمان للتأكد بأن المملكة المتحدة في موقع قوي بالنسبة لمجموعة واسعة من استخدامات المركبات المؤتمتة والمرتبطة بالإنترنت.[31]

[29] المركز الوطني لأمن المعلوماتية، مبادئ الأمن الإلكتروني للمجتمعات المرتبطة بالإنترنت (2021)
[30] جاء هذا الإعلان في تكنولوجيا الابتكار (2021)
[31] العملية المتعلقة بالمركبات المرتبطة بالإنترنت والمؤتمتة من أجل ضمان السلامة والأمن (CAVPASS)

شادي أ. رزاق، المدير الفني والمؤسس الشريك لشركة أنغوكا

إن نشر الحكومة للإرشادات الخاصة بأمن المجتمعات المرتبطة بالإنترنت، والاستخدام المتزايد للمركبات ذاتية القيادة يسلطان الضوء على أهمية الأمن في مجتمعنا. وتفخر شركة أنغوكا بأن تكون أحد خريجي برنامج المسرعات الإلكترونية الذي يديره المركز الوطني لأمن المعلوماتية. نحن نقدم الحلول لشريحة واسعة من التطبيقات، سواء كانت للبنية التحتية الوطنية الحيوية أو لوسائل النقل البري والجوي وغيرها، بما يوفر الصمود وضمان الأمن الشامل.

مهمة الشركة أن تضمن سلامة وصمود المدن الذكية ووسائل النقل. حيث أصبح هذان الجانبان أكثر تعقيدا واعتمادا على شبكات من الأجهزة المرتبطة بالإنترنت والاتصالات ما بين الأجهزة. الحلول التي نقدمها تتيح إنشاء مناطق موثوقة تشغّل نظاما أمنيا لا مركزيا مقاوما للهجمات التي قد تأتي من كمبيوترات كمية، ويجري تحديث ذلك النظام بشكل فعال لجعل الأهداف متغيرة دائما بالنسبة للمهاجمين. هذا يعني أن يكون لمالكي الأجهزة سيطرة تامة على أمنهم.

فريق شركة أنغوكا يعرض حلول الشركة

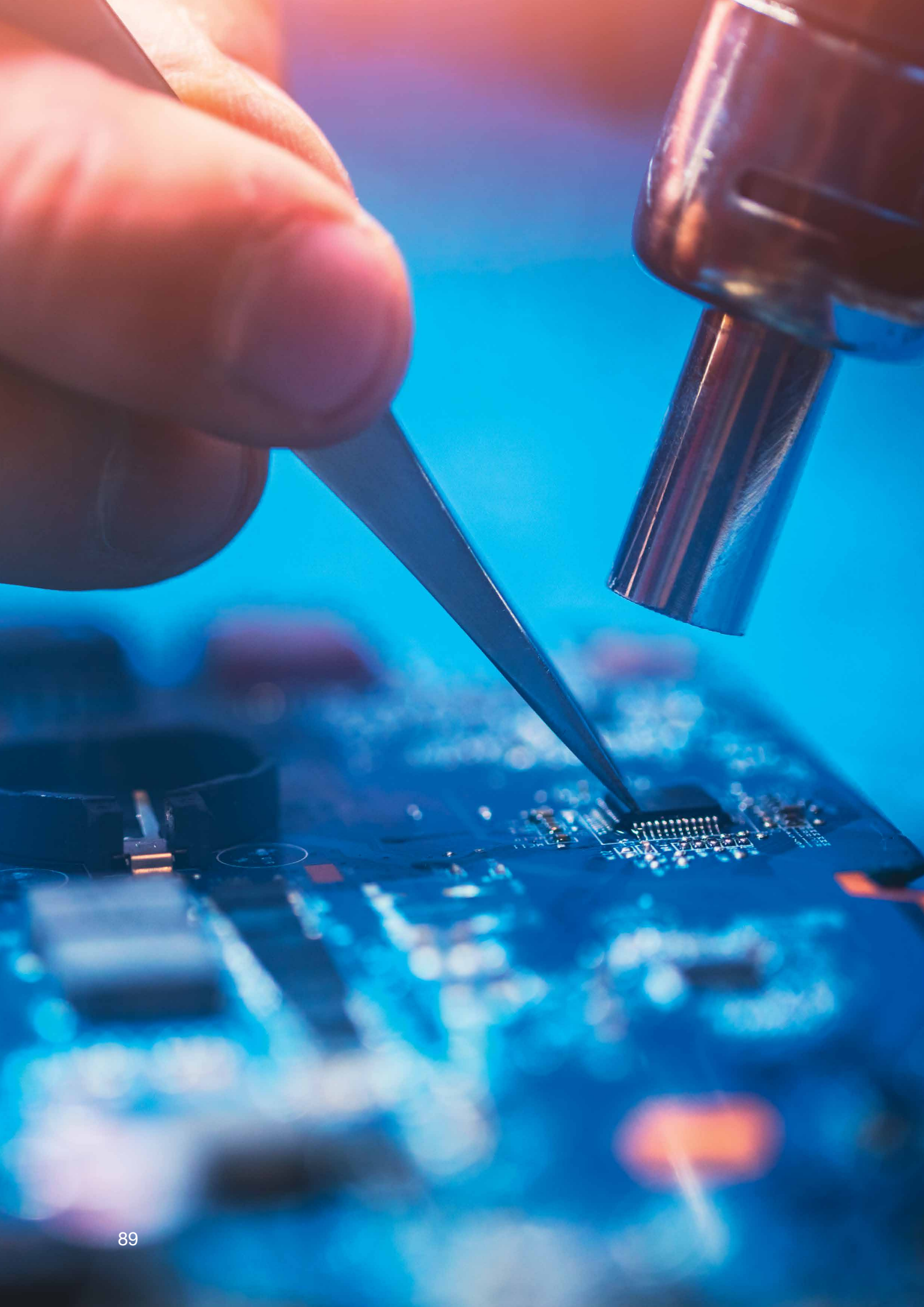
الهدف 4:
العمل مع جهات معنية متعددة لبلورة معايير عالمية رقمية فنية في المجالات ذات الأولوية والأكثر أهمية للحفاظ على قيمنا الديمقراطية، وضمان أمننا الإلكتروني، وتحقيق المصالح الاستراتيجية للمملكة المتحدة من خلال العلوم والتكنولوجيا

148. تعتبر المعايير الفنية الرقمية العالمية جزءا أساسيا من عمل الإنترنت وشبكات الاتصالات وأنواع التكنولوجيا الناشئة. ويمكن لطريقة تطوير تلك المعايير واستخدامها أن تؤثر على أهداف أمننا الإلكتروني، ورخائنا الاقتصادي، وعلى قوانيننا وقيمنا. في السابق، كانت صياغة تلك المعايير تتم من جانب الجهات التي تتمتع بأكبر قوة في السوق، وكانت هناك عوائق مادية تعرقل وتمنع مشاركة بعض الأطراف المعنية الهامة، مثل الشركات الصغيرة والمتوسطة، والأكاديميين، وغيرهم من الخبراء. سوف نحقق النتائج التالية بحلول 2025:

149. ستزداد مشاركة جهات معنية متعددة في بيئة المعايير الفنية الرقمية العالمية. سوف ندعم مشاركة جهات متعددة في المؤسسات الأساسية المعنية بتطوير المعايير، وسنكون القدوة بوفودنا إلى مؤتمرات الاتحاد الدولي للاتصالات. وسنشجع على النقاشات المفتوحة بشأن التوجهات والاعتبارات الأساسية بالنسبة لصانعي السياسات من خلال منتدى الأمم المتحدة لحوكمة الإنترنت وغيره من المنتديات. كما سنعزز التنسيق وتبادل المعلومات مع شركائنا الدوليين، بما في ذلك من خلال مجموعة نقاط الاتصال المعنية بالمعايير الرقمية، والتي تأسست خلال رئاسة المملكة المتحدة لمجموعة الدول السبع.

150. بلورة معايير فنية رقمية عالمية بفاعلية أكبر في المجالات ذات الأولوية بالنسبة للمملكة المتحدة، وذلك من خلال قيمنا الديمقراطية، واعتبارات الأمن الإلكتروني، والأبحاث، والبحوث والابتكارات البريطانية في أنواع التكنولوجيا الناشئة. سنعمل مع القطاع والجامعات والخبراء الفنيين والمجتمع المدني في مجالات مثل بروتوكولات الإنترنت، والشبكات المستقبلية، والذكاء الاصطناعي من أجل رفع درجة الوعي بالمضامين الهامة للسياسة العامة في تطوير المعايير الفنية. وسننشئ أول مركز لمعايير الذكاء الاصطناعي لدعم مشاركة المملكة المتحدة دوليا في مجال توحيد المعايير، كما هو مبين في الاستراتيجية الوطنية للذكاء الاصطناعي.

151. سندعم كل ذلك من خلال آليات تنسيق استراتيجي داخل المملكة المتحدة، مثل المبادرة المبينة في الاستراتيجية الوطنية للذكاء الاصطناعي بين الحكومة ومعهد المعايير البريطانية والمختبر الفيزيائي الوطني. من شأن تلك المشاركة أن تدعم ازدهار المملكة المتحدة من خلال الترويج للمعايير التي تُمكّن الابتكار وتسهّل النمو والارتقاء بالمناطق الأقل حظا.



الدعامة 4:
القيادة الدولية

تعزيز قيادة ونفوذ المملكة المتحدة في العالم من أجل نظام دولي آمن ومزدهر

152. يظل الفضاء الإلكتروني المنفتح والسلمي والآمن والمتاح للجميع عنصراً بالغ الحيوية لأمن ورخاء الجميع. وستظل المشاركة الدولية أمرا ضروريا لتحقيق كافة أهداف الاستراتيجية الإلكترونية للمملكة المتحدة. لكن لكي تستجيب المملكة المتحدة لحقبة من المنافسة العامة، سيكون عليها الآن أن تضطلع بدور قيادي عالمي ناشط من أجل الترويج لمصالحنا ونشر قيمنا في الفضاء الإلكتروني. كما سوف نضع كون نشاطات المملكة المتحدة في الفضاء الإلكتروني وخبراتنا الإلكترونية في صميم الجهود لتنفيذ أجندة الحكومة الأعم للسياسة الخارجية: سنبادر إلى استخدامها بشكل استباقي للمساعدة في تحقيق نظام عالمي منفتح وآمن ومزدهر.

153. سنسعى لتقوية تحالفاتنا الأساسية، فيما نعمل مع مجموعة أكبر من الشركاء - بما فيها القطاع والمؤسسات العالمية المعنية بالمعايير الفنية والمجتمع المدني والجامعات - كدولة تعمل على حل المشاكل وتقاسم الأعباء. وسنستثمر في توطيد العلاقات مع الشركاء في أفريقيا ومنطقة المحيط الهندي-الهادئ، ونغتنم الفرص لإنشاء تحالفات جديدة أكثر مرونة. كما سنواصل تعزيز أدواتنا الدبلوماسية، ونربط نفوذنا في الخارج بنقاط قوتنا المحلية، واستغلال خبراتنا العملية والاستراتيجية في مجال الاتصالات، وبرامجنا لتطوير المهارات، وشراكاتنا الاقتصادية كقوة عالمية من أجل الخير. مقاربتنا هذه هي لمصلحة الأمن والرخاء العالميين، وليس فقط لخدمة أمتنا.

الهدف 1:
تقوية الأمن والصمود الإلكتروني لشركائنا الدوليين ورفع وتيرة العمل الجماعي لعرقلة خطط الأعداء وردعهم

154. يعتبر العمل الجماعي والصمود المتبادل في غاية الأهمية للتصدي للتهديدات من أساسها، وفي نفس الوقت لخفض المغريات التي تحفز الأعداء لشن هجمات ضد المملكة المتحدة وشركائها. سوف نحقق النتائج التالية بحلول 2025:

155. سيكون لدى الشركاء الدوليين للمملكة المتحدة قدرات أكبر وإرادة سياسية وحوكمة وأنظمة من أجل التحري بشأن التهديدات الإلكترونية وإحباطها، وكذلك لبناء الصمود. ذلك سيؤدي إلى انخفاض التهديد الخارجي لمواطني المملكة المتحدة. وسوف نعطي الأولوية للمساعدة في بناء القدرات الإلكترونية في أوروبا الشرقية وأفريقيا ومنطقة المحيط الهندي-الهادئ، كما سنواصل العمل مع الحلفاء الأساسيين في الشرق الأوسط والأمريكيتين. وسنطور أيضا مساعدة فنية أكثر تكاملا تشمل الحكومة بأكملها، والاستثمار بقدر أكبر في مؤسسات إنفاذ القانون وخبرات الدفاع، اعتمادا على القطاع والجامعات في المملكة المتحدة. وسينصب تركيزنا على حماية سلاسل التوريد الحيوية الدولية والبنية التحتية، مع التشجيع على الاستخدام الآمن للتقنيات الرقمية، والعمل مع شركائنا في القطاع لفعل ذلك على نطاق واسع.

156. سنبذل المزيد من الجهد أيضا من أجل بناء قدرات المجتمع المدني والمؤسسات بما يتيح المجال لحوار مبني على القيم بشأن التكنولوجيا والمجتمع، وبناء آليات محلية للمساءلة. وسنواصل العمل مع شراكات ومؤسسات فعالة متعددة الأطراف، ومنها الأمم المتحدة، وتحالف العيون الخمس، وحلف الناتو، ومجموعة الدول السبع، والاتحاد الأوروبي، والكومنويلث، ومنظمة التعاون الاقتصادي والتنمية، والمنتدى العالمي للخبرات الإلكترونية، ورابطة دول جنوب شرق آسيا (آسيان)، والاتحاد الأفريقي، والبنك الدولي.

157. لرفع كفاءة حمايتنا للمصالح البريطانية ومواطني المملكة المتحدة في الخارج، سنعمل أيضا لتصميم وتنفيذ حملة دولية للممارسات الإلكترونية السليمة لبعثاتنا الدبلوماسية في الخارج، وهذه الحملة سوف يجري تصميمها وتطبيقها محليا. والغرض منها جعل الأنشطة الضارة، مثل القرصنة وسرقة البيانات والملكية الفكرية وبرمجيات انتزاع الفدية، باهظة التكلفة على مرتكبيها. وسيتولى تنفيذ هذه الحملة الدبلوماسيون والموظفون المحليون في بعثاتنا بالخارج، ومجتمع الشركات البريطانية المحلية، والجهات التي تنفذ برامج التنمية البريطانية.

158. سنشكل تحالفا دوليا أوسع يكون مستعدا وقادرا على فرض عواقب أكثر تأثيرا على أعداء المملكة المتحدة . سنعزز العزم والقدرات على الصعيد الدولي من خلال تواصل دبلوماسي أوسع، وتعاون عملي، وتبادل المعلومات، وتمارين مشتركة. وعن طريق العمل من خلال قنوات السياسات وجهاز إنفاذ القانون والقنوات العملية، سنزيد من مفعول الإجراءات مثل العقوبات الإلكترونية الموجّهة، كما سنستحدث أدوات جديدة لجعل التهديدات الإلكترونية المعادية أكثر تكلفة على مرتكبيها. وسنتوصل إلى المزيد من الفهم المشترك مع القوى الإلكترونية في الدول الحليفة والشريكة الأساسية، إلى جانب تحقيق تكامل أفضل بين عملياتنا الإلكترونية وعمليات الحلفاء في كافة المجالات: البر، والبحر، والجو، والفضاء، والفضاء الإلكتروني.

159. كما سنستمر في دعم تطوير قدرات الأمن الإلكتروني لحلف الناتو من أجل ضمان عمل جماعي أفضل، بما في ذلك دعم الإجراءات التي تقدمها المملكة المتحدة وحلفاء آخرون طواعية من أجل دمج التأثيرات الإلكترونية السيادية في عمليات ومهام الناتو.

الهدف 2:
بلورة حوكمة عالمية لتطوير فضاء إلكتروني منفتح وآمن ومحمي ومتاح للجميع

160. الدول التي لا تشارك المملكة المتحدة نفس القيم تستغل التحديات التي يمثلها الإنترنت المنفتح والمتاح للجميع من أجل نشر تصوراتها الاستبدادية بشأن الفضاء الإلكتروني تحت ذريعة الأمن. ستنتهج المملكة المتحدة مقاربة استباقية، وستعمل مع حلفائنا وشركائنا لضمان تطوير القواعد والأطر الدولية بما ينسجم مع قيمنا الديمقراطية. وسنسعى لدعم النمو الاقتصادي الوطني والعالمي، وتعزيز الأمن الجماعي، وتشجيع الاستخدام المسؤول للأدوات الإلكترونية الهجومية، وتمكين فرض عواقب مؤلمة على مرتكبي الأنشطة الضارة غير المسؤولة. سوف نحقق النتائج التالية بحلول 2025:

161. ستحمي الحوكمة العالمية للفضاء الإلكتروني والإنترنت مصالح وقيم المملكة المتحدة، وسيكون للمملكة وشركائها نفوذ أكبر في تطوير وتطبيق أطر الحوكمة والمعايير الدولية. كما سنتبع مقاربة تقدمية واستباقية لوضع الأطر التي تحكم الفضاء الإلكتروني من أجل تعزيز النمو الاقتصادي والأمن العالميين. وسنصمم ونطبق خطوات عملية لإطلاق حوار دولي بشأن تطبيق القواعد والأعراف والمبادئ في مجال الفضاء الإلكتروني، ودفع ذلك الحوار باتجاه تحقيق إجماع حول القيود الفعالة على الأنشطة الهدامة والمخلة بالاستقرار. وسنفعل ذلك من خلال منظمات أساسية ومتخصصة، ومنها منظمة الأمن والتعاون الأوروبي، ورابطة دول جنوب شرق آسيا (آسيان)، والمنتدى العالمي للخبرات الإلكترونية. كما سنعمل بشكل بنّاء مع عمليات الأمم المتحدة لوضع معاهدة دولية جديدة بشأن الجرائم الإلكترونية لتكون أداة أخرى إلى جانب اتفاقية بودابست، بما يكفل تقوية التعاون الدولي وحماية حقوق الانسان.

162. كما سنستمر في التشجيع على اتباع اتفاقية بودابست بشأن الجرائم الإلكترونية بالعمل مع الشركاء الدوليين لتقديم حجة قوية للحفاظ على أن تظل هي الاتفاقية الدولية الأولى للتعاون. وسنستمر في تشجيع وتعزيز إجراءات الجهات المعنية متعددة الأطراف من أجل حوكمة الإنترنت، مثل شركة الإنترنت للأسماء والأرقام المخصصة (آيكان)، وأيضا من خلال منتدى حوكمة الإنترنت. وهذه الجهود يتممها سعينا لوضع معايير فنية رقمية دولية (شُرحت في فصل التكنولوجيا) وجهودنا لزيادة صادرات المملكة المتحدة في مجال الأمن الإلكتروني (انظر أدناه)، وهو ما سيساعد أيضا في ترسيخ معايير المملكة المتحدة في البيئات الإلكترونية للدول الأخرى.

163. معظم دول "الأرضية الوسط" ستدعم وتروّج رؤية المملكة المتحدة للفضاء الإلكتروني ومستقبل الإنترنت، بما يؤدي للتصدي بنجاح لتأثير الدول ذات الأنظمة الاستبدادية على نظام الجهات المعنية متعددة الأطراف. سنبين كيف أنه بالإمكان معالجة الصعوبات في الفضاء الإلكتروني دون تبني مواقف استبدادية، وبنفس الوقت تمكين الابتكار والتنمية والنمو. وسوف نساعد الدول التي تجد صعوبة بمجال الرقمنة على بناء كامل نطاق الخبرات القانونية والاستراتيجية في مجال الاتصالات التي تحتاجها لكي تشارك في الحوار الدولي، ولتنفيذ الأطر المتفق عليها. وسنستمر في فضح الاستخدام غير المسؤول للقدرات الإلكترونية، وفي بناء الثقة على المستوى الدولي. وكذلك سنواصل إبداء مقاربة منفتحة وشفافة في استخدامنا للقدرات الهجومية الإلكترونية كلما استطعنا ذلك، بما يقوي سمعة المملكة المتحدة كقوة للخير.

الهدف 3:
الاستعانة بالقدرات والخبرات الإلكترونية البريطانية وتصديرها لتعزيز تفوقنا الاستراتيجي، والترويج لسياستنا الخارجية الأعم ومصالحنا في الازدهار الاقتصادي.

164. استجابة للمنافسة العامة والتغيرات التكنولوجية المتسارعة، سوف يُنظر في أمر الاستعانة بأنشطة وقدرات المملكة المتحدة الإلكترونية ومصادر القوة الوطنية الأخرى لتعزيز تفوقنا الاستراتيجي، والترويج لسياستنا الخارجية وأهدافنا في تحقيق الازدهار. غايتنا هي إنشاء نظام عالمي يتيح ازدهار المجتمعات والاقتصادات المنفتحة، وحماية حقوق الانسان، فيما نواصل العمل على تحقيق الازدهار في بلادنا. سوف نحقق النتائج التالية بحلول 2025:

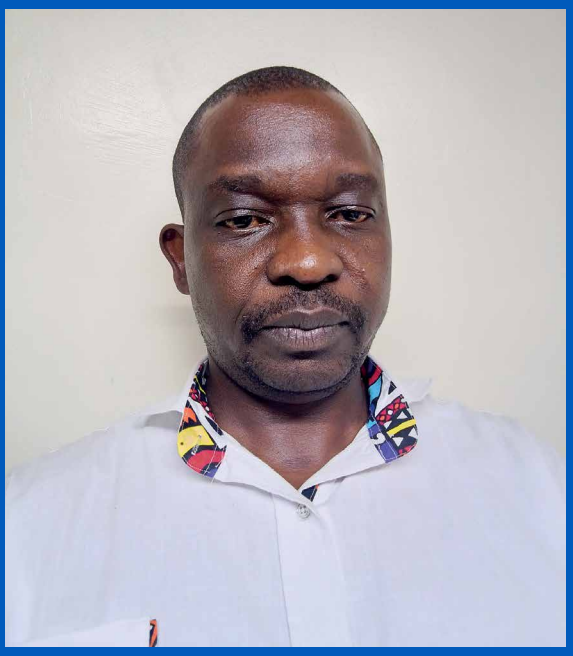
165. نشاطنا في الفضاء الإلكتروني وما يتصل به سيعزز الاستقرار العالمي، ويحمي النظام الدولي القائم على قواعد القانون، والمجتمعات المنفتحة، والأنظمة الديمقراطية حين تتعرض لمحاولات تقويضها. سوف نطلق حملة مبنية على قيمنا لمؤازرة حقوق الانسان، والتنوع، والمساواة بين الجنسين في مجالات تصميم وتطوير واستخدام الفضاء الإلكتروني. وسيشمل ذلك، على سبيل المثال لا الحصر، التصدي لحجب خدمة الإنترنت، والتحيز في خوارزميات الذكاء الاصطناعي، وزيادة درجة الأمان على الإنترنت. وسننافس بفاعلية أكبر لحماية القيم والأنظمة والإجراءات الديمقراطية، ونقوي النظام الدولي القائم على قواعد القانون (بما في ذلك الأمم المتحدة، ومنظمة الصحة العالمية، ونظام التجارة العالمي) من خلال ضخ المزيد من الاستثمارات في شبكة العاملين في القطاع الإلكتروني التي تمتد لتشمل ست قارات. وسندعم استخدامنا للاتصالات الاستراتيجية لتطوير تعاوننا مع الأخرين في مجال البحوث، وبرامج التبادل الأكاديمي، والمساهمة في ضمان ترجمة الأفكار البريطانية إلى تطبيقات عملية.

166. ستصبح المملكة المتحدة أحد أكبر ثلاثة مصدرين للحلول والخبرات الإلكترونية. وسيكون القطاع الإلكتروني البريطاني هو الجهة التي تلجأ إليها الحكومات الأخرى وكبار العملاء التجاريين للحصول على حلول لمشاكل الأمن الإلكتروني. وسوف نعرض أفضل ما لدى المملكة المتحدة في مجال الأمن الإلكتروني من خلال تواصل دولي أكثر نشاطا بين الحكومات، وتحت مظلة برنامج سفير الأمن الإلكتروني البريطاني وشبكتنا الدولية. وسنقدم الدعم للشركات في كافة أنحاء المملكة في كل مرحلة من مراحل الابتكار وحتى التصدير لكي تصبح من المصدّرين المؤهلين، ولاستقطاب الاستثمارات الأجنبية، ومساندة الشركات الصغيرة والمتوسطة، بما في ذلك من خلال كلية التصدير الجديدة.[32][33] وإلى جانب عملنا ضمن إطار شراكة النمو الإلكتروني والجهود الأخرى المبينة في فصل البيئة الإلكترونية في المملكة المتحدة من هذه الاستراتيجية، سننشئ أيضا مكتبا جديدا لحملات ترويج القدرات الإلكترونية لكي يقدم دعما أفضل تصميما وتنسيقا لحملات التصدير الكبرى.

[32] مبينة في الاستراتيجية البريطانية للابتكار (2021)

[33] كلية صادرات الدفاع والأمن البريطانية هي كلية للتعلم والتطوير على الإنترنت مصممة لخدمة الشركات الصغيرة والمتوسطة العاملة في مجال الدفاع والأمن، وتقدم مواد تدريب لشركات الأمن الإلكتروني. التسجيل في كلية التصدير يتيح توفير برنامج من مساقات التعلم المبنية على منهج دراسي، وكذلك معلومات قيمة عن الفعاليات والمعارض القادمة المتعلقة بصادرات الدفاع والأمن البريطانية.

تشارلز جوما، البرنامج البريطاني لتوفير الخدمات الرقمية في نيروبي



اسمي تشارلز ويسونغا جوما، وأنا مسؤول عن تصميم وتنفيذ الأمن الإلكتروني، والتطوير والشمول وريادة الأعمال بالمجال الرقمي كجزء من البرنامج البريطاني العالمي والحكومي لتوفير الخدمات الرقمية في كينيا. كما أقدّم الدعم لمشاريع مُكمِلة ضمن إطار المحفظة الإلكترونية لصندوق معالجة الصراع وإحلال الاستقرار والأمن. لا يمكن المبالغة بالتشديد على أهمية السلامة والأمن وحفظ البيانات على الإنترنت والاستخدام المسؤول للفضاء الإلكتروني. وكما تعلمنا من تجربة جائحة كوفيد-19، فإن السلامة والممارسات السليمة على الإنترنت لا تقل أهمية عن صحة الأفراد ونظافتهم. وأنا حريص على حماية الجميع من التهديدات والأذى على الإنترنت ضمن إطار القوة الإلكترونية الكلية للحكومة البريطانية.

سارا ميرتشانت، مسؤولة الأنظمة الإلكترونية في السفارة البريطانية في تبليسي، جورجيا

اسمي سارا، وأنا معيّنة في السفارة البريطانية في تبليسي كمسؤولة الأنظمة الإلكترونية. أعمل بشكل وثيق مع الحكومة الجورجية والمركز الوطني لأمن المعلوماتية في المملكة المتحدة. يتراوح عملي اليومي بين المهام السياسية، والمساعدة في تطبيق الاستراتيجية الإلكترونية الجديدة، وحتى الاستعانة بخبراء بريطانيين لرفع القدرات الفنية لجورجيا. ويشرفني أن أكون في طليعة الجهود الرامية لعرض الخبرات البريطانية ودعم جورجيا لبناء القدرة على الصمود ضد التهديدات الإلكترونية. ولكون جورجيا، لسوء الحظ، دولة مرت بتجربة واسعة في التعرض لأنشطة إلكترونية معادية صادرة عن دول أجنبية، يمكننا أن نتعلم الكثير منها. وعملنا معا يجعلنا أكثر قوة وصمودا ودراية.

الدعامة 5:
مكافحة التهديدات

كشف أعدائنا وعرقلتهم وردعهم لتعزيز أمن المملكة المتحدة في الفضاء الإلكتروني ومن خلاله

167. التهديدات التي تواجهنا طبيعتها معقدة. وتقلقنا التهديدات في الفضاء الإلكتروني (التي تستهدف نشاطنا على الإنترنت مثلا)، وتلك الموجهة ضد المملكة المتحدة وشركائها من خلال الفضاء الإلكتروني (مثل التهديدات لشبكات البنية التحتية الوطنية الحيوية في المملكة المتحدة)، وتلك الموجهة ضد وظائف البنية التحتية الإلكترونية الدولية التي ترتكز عليها. يمكن لكل هذه التهديدات أن تؤثر على توفُّر الخدمات التي يعتمد عليها الناس، وعلى سرية وسلامة البيانات والمعلومات التي تمر عبر تلك الأنظمة الإلكترونية. الأسس التي تقوم عليها مقاربتنا في التصدي للتهديدات تتمثل في تقوية الصمود الإلكتروني كما سبق شرحه في هذه الوثيقة. وهذا الفصل يركز على كيفية زيادتنا للتكلفة والمخاطر التي يتكبدها كل من يفكر بمهاجمة المملكة المتحدة في الفضاء الإلكتروني، وضمان تحقيق كامل إمكاناتنا كقوة إلكترونية.

168. منذ إطلاقنا للاستراتيجية الوطنية لأمن المعلوماتية 2016 - 2021، غيّرنا مقاربتنا بشأن تخفيف حدة التهديدات. حيث أسسنا قدرات عالمية المستوى بمجال كشف التهديدات الإلكترونية وتحليلها ضمن المركز الوطني لأمن المعلوماتية. يعمل هذا المركز مع شركاء في القطاعين العام والخاص، وفي الداخل والخارج، لكشف التهديدات والحوادث والاستجابة لها. وكجزء من مجتمع الاستخبارات الأعم، تمكن المركز أيضا من تزويد صانعي السياسات بمعلومات بشأن منفذي الهجمات والتهديدات ضد مصالح المملكة المتحدة، وهذا بحد ذاته جزء حيوي في مقاربتنا لردع التهديدات الإلكترونية. كما استثمرنا بشكل كبير في قدراتنا الإلكترونية الهجومية من خلال برنامجنا الوطني للهجوم الإلكتروني، ونفعل ذلك الآن أيضا من خلال القوة الإلكترونية الوطنية. كما طورنا آلية استجابة وطنية لمؤسسات إنفاذ القانون تحت قيادة الوكالة الوطنية لمكافحة الجريمة، وسعينا إلى عرقلة ورفع تكلفة الأعمال العدائية والإجرامية في الفضاء الإلكتروني. كما أنشأنا قدرات عالمية المستوى لكشف التهديدات وتقييمها، مع وجود الوسائل لترجمة المعلومات المكتسبة إلى أساليب مؤثرة للحد من ضرر التهديدات على القطاعين العام والخاص. وقد وضعنا نظاما مستقلا للعقوبات بشأن الجرائم الإلكترونية كعنصر آخر لفرض تكلفة عالية على الفاعلين المعادين. والجهود الإجمالية لتواصلنا الدبلوماسي، والمركز الوطني لأمن المعلوماتية، والوكالة الوطنية لمكافحة الجريمة، ووكالاتنا الأمنية والاستخباراتية، وجهاز إنفاذ القانون عموما، والقوة الإلكترونية الوطنية، قد ساهمت في تقليل الأضرار التي تسببها هذه التهديدات في العالم المادي، عن طريق اتخاذ الخطوات اللازمة للتصدي للأعداء مباشرة، ومنع وقوع الهجمات، والإقلال من ضررها.

169. لكن التهديدات قد ازدادت تطورا وتعقيدا وشدة؛ ولم تفلح جهودنا بعد بشكل جوهري في جعل المهاجمين يعيدون حساباتهم بالنسبة لمخاطر هجماتهم، وهم يواصلون بنجاح استهداف المملكة المتحدة ومصالحها. والدافع وراء الهجمات على المملكة المتحدة هو إما التجسس، أو تحقيق مكاسب إجرامية وتجارية ومالية وسياسية، بالإضافة إلى التخريب والتضليل الإعلامي. كما يواصل المهاجمون تطوير قدرات تستطيع أن تتجنب أساليب تخفيف حدة الهجمات، وذلك باستخدام أدوات إلكترونية معقدة وأدوات أخرى أصبحت تُباع تجاريا في القطاع الإلكتروني المتنامي، وهذا ما يحد من مفعول الموانع التي تعوق دخول مختلف أنواع المهاجمين المعادين. كما أن الفوائد التي يجنيها هؤلاء المهاجمون تزداد مع ازدياد قدرتهم على سرقة وتشفير بيانات ثمينة، وابتزاز الأموال عن طريق برامج انتزاع الفدية، ما يؤدي إلى عرقلة الأعمال والخدمات العامة الأساسية. والنتيجة هي أن المهاجمين يستفيدون ماديا بشكل متزايد، ويستغلون الخصوصية وحرية التعبير، ويحاولون التلاعب بالأحداث عن طريق المعلومات المضللة.

170. بالتالي فإن مقاربة المملكة المتحدة ستتحول إلى حملة أكثر تكاملا واستمرارية تنطوي على الاستخدام المنتظم والمتكامل والمبتكر لمجموعة واسعة من كافة الإمكانات والقدرات المتوفرة لفرض تكلفة عالية على أعدائنا، وملاحقة منفذي الهجمات وإحباط خططهم، وردع الهجمات في المستقبل. وستكون العناصر الأساسية المساندة لهذه المقاربة هي:

- التطوير المتواصل للقوة الإلكترونية الوطنية ليكون بمثابة الخطوة التالية في تعزيز قدرات المملكة المتحدة على تنفيذ هجمات إلكترونية ضد أعدائها
- حملات مصممة خصيصا تشمل كامل قطاعات الحكومة للتصدي للتهديدات الموجّهة ضد المملكة المتحدة – بالاستعانة بأدواتنا الدبلوماسية والعسكرية والاستخباراتية والاقتصادية والقانونية، بالإضافة إلى مؤسسات إنفاذ القانون، والاتصالات الاستراتيجية
- استثمارات جديدة لتمكين مؤسسات إنفاذ القانون من متابعة التحقيقات على نطاق واسع وبوتيرة سريعة، والحفاظ على تفوقنا التقني على الأعداء من أجل منع وقوع الهجمات وكشف المجرمين الخطرين والخدمات المساندة التي يعتمدون عليها
- زيادة تبادل البيانات بشكل كبير بين مختلف مؤسسات الحكومة والقطاع، كما هو مبين في الفصل المتعلق بالصمود

171. يوفر الفضاء الإلكتروني الفرص للمملكة المتحدة، ويخلق سبلا جديدة في السعي الحثيث لتحقيق مصالحنا الوطنية. فمثلا، توفر لنا العمليات الإلكترونية الهجومية مجموعة من الإجراءات المرنة والقابلة للتوسع والتي تخفف من حدة التهديدات المعادية، والتي تساعد المملكة المتحدة في الحفاظ على تفوقها الاستراتيجي، وتحقيق أولوياتها الوطنية. وغالبا ما يكون ذلك بطرق تتجنب تعريض الأفراد للخطر أو للأذى الجسدي.

172. سنستمر في تطوير قدراتنا الإلكترونية الهجومية والاستثمار فيها من خلال القوة الإلكترونية الوطنية. هذه القوة تُحدِث تحولا في قدرة المملكة المتحدة على تحدي الأعداء في الفضاء الإلكتروني والعالم المادي لحماية بلادنا وشعبنا وأسلوب حياتنا. وسنستخدم تلك القدرات بشكل مسؤول كقوة للخير إلى جانب عناصر أدوات القوة الأخرى الدبلوماسية والاقتصادية والعسكرية وكذلك العدل الجنائي. وسنوظف تلك الأدوات لدعم وتحقيق مجموعة واسعة من أولويات الحكومة المتعلقة بالأمن القومي، ومتانة الاقتصاد، ولمساندة جهود كشف الجرائم الخطرة ومنع وقوعها.

الهدف 1:
كشف التهديدات الإلكترونية من الفاعلين من الدول والمجرمين وغيرهم من الفاعلين الخبيثين في الفضاء الإلكتروني، والتحقيق بأفعالهم وتبادل المعلومات بشأنهم من أجل حماية المملكة المتحدة ومصالحها ومواطنيها.

173. سوف نحقق النتائج التالية بحلول 2025:

174. سيكون لدى الحكومة فهم شامل للقدرات الإلكترونية للفاعلين من الدول والمجرمين وغيرهم من الفاعلين الخبيثين ونواياهم الاستراتيجية تجاه المملكة المتحدة. وسنحافظ على الاستثمارات الكبيرة المعلن عنها في استراتيجية 2016 وننميها للإنفاق على وكالات الاستخبارات وجهاز إنفاذ القانون من أجل فهم طبيعة التهديدات الإلكترونية. وبوجه خاص، سنرفع من قدرات جهاز إنفاذ القانون لأجل فهم تهديدات الجرائم الإلكترونية والتصدي لها. ذلك يشمل معرفة الصلة بين تلك التهديدات والدول، وغيرها من التهديدات المحلية والدولية، والوسائل التكنولوجية المُستخدمة فيها، حيث سيساعدنا ذلك على تطوير سياسة استجابة فعالة. كما سوف نُحسّن تنسيق كشف التهديدات في كافة قطاعات الحكومة من خلال استراتيجية تتعلق بالاطلاع على البيانات واستغلالها تشترك بها كافة الوكالات الاستخباراتية وجهاز إنفاذ القانون. وسنركز بشكل أكبر على فهم نوايا أعدائنا والمعايير التي يطبقونها في اتخاذ القرارات، وتأثير نشاطاتنا عليهم، بما في ذلك كيفية تحول الأفراد إلى مرتكبي جرائم إلكترونية، وما ينبغي علينا فعله لمنع وقوع ذلك.

175. عملنا في تسهيل الإبلاغ عن الحوادث والجرائم بشكل أسرع، كما هو مبين في فصل الصمود من هذه الاستراتيجية، سوف يساعد كذلك في تحقيق ذلك.

176. سيجري التحقيق بشكل منتظم وشامل في التهديدات الخطيرة التي يقف وراءها فاعلون تابعون لدول ومجرمون آخرون. وسنعتمد في ذلك على كافة مصادر المعلومات، وجمع الخبرات من كافة قطاعات الحكومة، وجهاز إنفاذ القانون، والقطاع الخاص. وسنقوي من القدرات الاستخباراتية والعملية والفنية للشبكة الإلكترونية لمؤسسات إنفاذ القانون. كما سنستثمر في القدرات الاستخباراتية الإلكترونية للوكالة الوطنية لمكافحة الجريمة التي تُستخدم لاستهداف مجموعات الجريمة المنظمة؛ وفي مبادرة جمع الاستخبارات الإقليمية، والتي من شأنها أن تعزز الاطلاع على المعلومات الاستخباراتية ونقلها في أنحاء المملكة المتحدة؛ وفي تقوية المهارات والقدرات التي يحتاجها جهاز إنفاذ القانون للتحقيق في الجرائم الإلكترونية والرقمية ومنع وقوعها.

177. التحقيقات سوف تساندها معلومات استخباراتية من كافة المصادر، وستستفيد من مهارات وخبرة القطاع الخاص، بما في ذلك عن طريق مساعدة الشركات على تبادل البيانات بسهولة أكبر مع مؤسسات إنفاذ القانون. وسوف نستمر في تطبيق توصيات هيئة التفتيش على أجهزة الشرطة وخدمات الإطفاء والإنقاذ بشأن استجابة الشرطة للجرائم الإلكترونية، وذلك من أجل ضمان استمرار أمن وسلامة شبكة الجريمة الإلكترونية على المستوى الوطني والإقليمي والمحلي.[34]

[34] هيئة التفتيش على أجهزة الشرطة وخدمات الإطفاء والإنقاذ

178. تبادل البيانات والمعلومات عن التهديدات بشكل منتظم وعلى نطاق واسع وبوتيرة سريعة، وستكون الجهات التي تتلقاها أكثر قدرة على التصرف. وقد جرّب المركز الوطني لأمن المعلوماتية عددا من المبادرات لتشكيل مجموعات فعالة من المدافعين عن الشبكات الإلكترونية في قطاعات مختلفة عديدة باستطاعتها ليس فقط تلقي المعلومات عن التهديدات وتبادلها، بل أيضا استخدامها على نحو متزايد لتحقيق المصلحة الجماعية. سوف نتوسع في هذه الجهود، مع التركيز مبدئيا على مساعدة الحكومة في الدفاع عن نفسها بشكل أفضل، بدعم من مركز التنسيق الإلكتروني الحكومي (المشار إليه في فصل الصمود). ومركز التعاون الإلكتروني للقطاع المالي يحتل صدارة تلك الجهود بالفعل في القطاع الخاص.[35]

179. يبحث المركز الوطني لأمن المعلوماتية أيضا في سبل تعقب التهديدات التي تطرأ، ويواصل العمل مع معهد آلان تورينغ لمعرفة إن كان بالإمكان الاستعانة بتعلم الآلات لكشف أنماط معينة من الهجمات الإلكترونية. هذه الأبحاث سوف تستمر في تحسين فهمنا لكيفية استطاعتنا استخدام الذكاء الاصطناعي لكشف الأنشطة الخبيثة.

[35] المركز الوطني لأمن المعلوماتية، مركز التعاون الإلكتروني للقطاع المالي (FSCCC) (2021)

منع الجرائم الإلكترونية يعني أيضا التصدي لأنواع أخرى من النشاط الإجرامي

تقع الجرائم الإلكترونية (المُعرّفة بأنها المخالفات لقانون إساءة استخدام الكمبيوتر) عند الدخول غير المصرح به إلى أجهزة الكمبيوتر والشبكات والبيانات والأجهزة الرقمية الأخرى، أو الأفعال المرتبطة بذلك والتي تسبب الضرر، أو صناعة أو توفير الأدوات لارتكاب مثل هذه المخالفات. ذلك يتيح لمرتكبي الجرائم الإلكترونية ارتكاب أفعال إلكترونية خبيثة أخرى، مثل الهجمات لانتزاع الفدية، أو الدخول غير المصرح به إلى الحسابات، أو سرقة الملكية الفكرية، أو هجمات حجب الخدمة، أو سرقة بيانات شخصية ضخمة - وهذه كلها جرائم كبيرة آخذة في الازدياد.

بالنسبة للمواطنين، غالبا ما تتمثل الجرائم الإلكترونية فيما تسببه من جرائم أخرى يُسهّلون هم وقوعها. فالدخول غير المصرح به إلى أجهزة الكمبيوتر يمكن أن يؤدي إلى مجموعة واسعة من عمليات الاحتيال والسرقة والابتزاز الجنسي، كما قد يُسهّل في بعض الحالات مطاردة الأفراد والعنف المنزلي والتحرش. وكل هذه الجرائم تسبب ضررا بالغا للمواطنين البريطانيين بشكل يومي، وتدمر الشركات وتهدم حياة الأفراد. لذلك فإن الجرائم الإلكترونية تختلف عن غيرها من المسائل العديدة المتعلقة بالسلامة على الإنترنت، مثل التنمر والتحرش وخطاب الكراهية والتضليل الإعلامي، والترويج لثقافة العصابات والعنف، أو زيارة القاصرين للمواقع الإباحية. تعالج الحكومة هذه القضايا من خلال الورقة البيضاء حول الأضرار على الإنترنت، ومشروع القانون المتعلق بالسلامة على الإنترنت.

الهدف 2:
ردع الفاعلين من الدول والمجرمين وغيرهم من الفاعلين في العمليات الإلكترونية الخبيثة، وعرقلة خططهم وأفعالهم الموجهة ضد المملكة المتحدة ومصالحها ومواطنيها.

180. سوف نحقق النتائج التالية بحلول 2025:

181. سنجعل الفاعلين من الدول والمجرمين وغيرهم من الفاعلين الخبيثين يدفعون ثمنا غاليا ويتعرضون لخطر أكبر إذا حاولوا استهداف المملكة المتحدة. وسننفذ حملات متواصلة ومصممة خصيصا لردع المجرمين، والتي ستستفيد من كامل قدرات المملكة المتحدة (ومنها القدرات الدبلوماسية والاقتصادية وغيرها من الأدوات العلنية والمستترة) من أجل التأثير على سلوك مرتكبي الجرائم الإلكترونية. وسنعمل بوجه خاص على تحسين أسلوبنا في إظهار قدراتنا لأعدائنا واستعدادنا لجعلهم يدفعون ثمنا باهظا، بما في ذلك من خلال العقوبات، وكذلك من خلال عمليات مؤسسات إنفاذ القانون والقوة الإلكترونية الوطنية. ومن خلال برنامج الخيارات للوكالة الوطنية لمكافحة الجريمة، سوف نُبعد الأفراد عن الانخراط في الجرائم الإلكترونية، وذلك بالعمل مع القطاع والجامعات لتقديم بدائل أفضل لمن يُحتمل تحولهم للإجرام، مثل فرص التدريب والتوظيف.

182. كذلك سوف نوفر الأدوات والصلاحيات التي تحتاجها مؤسسات إنفاذ القانون ووكالات المخابرات من خلال مشروع قانون التصدي للتهديدات من الدول، وذلك بتحديث القانون المعمول به حاليا، وإدراج جرائم جديدة تعكس كيفية تغير التهديدات من الدول الأخرى. كما سنعدّل قانون العوائد من الجريمة لعام 2002 لرفع قدرة جهاز إنفاذ القانون في التعرف على عائدات الجرائم الإلكترونية ومصادرتها واستعادتها. وسنفعل ذلك تحديدا بإعطاء صلاحيات مدنية لمصادرة العائدات للإقلال من المخاطر التي يتسبب بها الأفراد الذين لا يمكن إخضاعهم للمحاكمة.

183. سيصبح الفاعلون من الدول والمجرمون وغيرهم من الفاعلين في العمليات الإلكترونية أقل قدرة على استهداف المملكة المتحدة نتيجة لجهودنا في عرقلة خططهم وإبطال مفعول جرائمهم وقدراتهم. وسوف نراجع سياسات الحكومة ومقاربتها العملية بالنسبة للتصدي لبرامج انتزاع الفدية، حيث سيكون ذلك من أولويات حملاتنا وبالتعاون مع القطاع الإلكتروني وشركائنا الدوليين. كما سنعزز الشراكة بين القوة الإلكترونية الوطنية، والمجلس الوطني لأمن المعلوماتية، والوكالة الوطنية لمكافحة الجريمة، وجهاز إنفاذ القانون عموما، والسلك الدبلوماسي، ووكالات المخابرات من أجل التصدي للتهديدات التي تهدد سرية وسلامة وتوافر الفضاء الإلكتروني أو البيانات والخدمات في الفضاء الإلكتروني. وسنستثمر بشكل خاص في القدرات التي تمكننا من استهداف البنية التحتية لمرتكبي الجرائم الإلكترونية، وسنستعين بمؤسسات إنفاذ القانون وقدراتنا الإلكترونية الهجومية لعرقلة الأنشطة الإلكترونية الخبيثة. وفيما يطور أعداؤنا قدراتهم الإلكترونية ويستخدمونها بشكل متزايد في الأعمال الضارة، سوف نسخّر كامل طاقات القوة الإلكترونية الوطنية، حيثما لزم الأمر، لعرقلة خطط أعدائنا والدفاع عن المملكة المتحدة وحمايتها.

184. سوف نتصدى أيضا لانتشار القدرات الإلكترونية المتطورة في بعض الدول ولدى جماعات الجريمة المنظمة، والمتوفرة لهم من خلال الأسواق التجارية وأسواق المجرمين، وسنقف في وجه المنتديات التي تتيح أو تسهّل أو تمجّد الإجرام الإلكتروني.

185. **سنزيد من تطبيق العدالة الجنائية وغيرها من الأدوات التي تعرقل الجرائم الإلكترونية**، واستخدام قدرات العدالة الجنائية المطورة لملاحقة مرتكبي الجرائم الإلكترونية في المملكة المتحدة. وسنُجري مراجعة لقانون إساءة استخدام الكمبيوتر والصلاحيات الأخرى ذات الصلة لضمان أن يكون لدى مؤسسات إنفاذ القانون القدرة على التحري عن التهديدات الجديدة والناشئة الصادرة عن المجرمين، كما سنستعين بممثلي ادعاء متخصصين وأفضل تأهيلا للتعامل مع العدد المتزايد من قضايا الجرائم الإلكترونية. وسوف نحسّن أيضا المهارات المتخصصة لمؤسسات إنفاذ القانون وتدريبها وتوسيع قدراتها لضمان توفر عدد كاف من عناصر الأمن الذين لديهم المعرفة التخصصية بمجال الأمن الإلكتروني. وسيكون ذلك من خلال منهج المهارات الإلكترونية في المجلس الوطني لرؤساء الشرطة، والمسار المهني بالمجال الرقمي الإلكتروني في كلية الشرطة.

سوزان مودي، مسؤولة منع الحوادث في هيئة شرطة إيرلندا الشمالية

من اليسار إلى اليمين: سوزان مودي (هيئة شرطة إيرلندا الشمالية)، ومقدمة التلفزيون سارة ترافرس، ومدير مركز الأمن الإلكتروني في إيرلندا الشمالية جو دولان.

أصبح الكمبيوتر والهاتف النقال جزءا من الحياة اليومية لجيل الشباب. وهما يوفران فرصا كبيرة، لكنهما يمثلان أيضا مصدر خطر إذا أُسيء استخدامهما. وإدارة منع الجرائم في شرطة إيرلندا الشمالية توفر التدخل المبكر المطلوب للتعامل مع الشباب ومساعدتهم على فهم القانون بشأن استخدام وإساءة استخدام الكمبيوتر. وهذا ما يؤدي إلى تسليط الضوء على دلائل احتمال ارتكاب نشاط إجرامي وكذلك، من ناحية أخرى، يسلط الضوء على الفرص الكبيرة المتاحة من خلال مبادرات مثل CyberFirst، وامتهان العمل في المجال الإلكتروني. من شأن ذلك أن يوفر البديل عن الإجرام لمن لديهم الفضول أو الموهبة، وأن يمنع استغلالهم من قبل الآخرين لغايات إجرامية. وقد عملت سوزان دون كلل لتطوير برنامج مدرسي عن المعلومات الإلكترونية، وجعلِه متاحا لطلاب المرحلة الثانوية. كما تعاونت بشكل مباشر مع أكثر من 40 مدرسة ابتدائية، والعديد من المدارس الثانوية، والمنظمات الشبابية، والمجموعات الكشفية. حيث يمكن لهؤلاء الشباب أن يصبحوا سفراءنا في المجال الإلكتروني والمدافعين عنا في المستقبل.

الهدف 3:
العمل في الفضاء الإلكتروني ومن خلاله لدعم أمننا القومي ومنع وكشف الجرائم الخطيرة

186. سوف نحقق النتائج التالية بحلول 2025:

187. سيكون للقدرات الإلكترونية للمملكة المتحدة تأثير أكبر في ردع وعرقلة التهديدات غير الإلكترونية. وسنرفع من كفاءة القوة الإلكترونية الوطنية ونطورها لتطبيق رؤيتنا بعيدة المدى لهذه القوة الرئيسية، إلى جانب ضمان أن تكون متكاملة تماما مع القيادة المركزية الحكومية للاتصالات، ووزارة الدفاع، وجهاز المخابرات الخارجية، ومختبر العلوم والتكنولوجيا الدفاعية، وأن تعمل بشكل وثيق مع مؤسسات إنفاذ القانون والحكومة عموما. وسوف ننفذ عمليات إلكترونية هجومية قانونية ومتناسبة عن طريق القوة الإلكترونية الوطنية، ونتصرف بشكل مسؤول في الفضاء الإلكتروني، ونكون قدوة في ذلك المجال. وستواصل العمليات الإلكترونية الهجومية دعم الأمن القومي للمملكة المتحدة، بما في ذلك سياستنا الدفاعية والخارجية، ومنع الجرائم الخطيرة.

188. كما سوف نوسع القدرات الفنية لمؤسسات إنفاذ القانون ونطورها ضد البنية التحتية للجهات المعادية والعملات الرقمية، ويمكن استخدام تلك القدرات أيضا ضد أنواع أخرى من التهديدات.

189. ستكون القدرات الإلكترونية للمملكة المتحدة متكاملة مع كامل نطاق عمليات الدفاع بما ينسجم مع مفهوم العمل المتكامل لعام 2025.[36] من شأن ذلك أن يحافظ على تفوقنا التنافسي القتالي على أعدائنا، ويتيح لنا التعاون بشكل أكبر مع حلفائنا وشركائنا. وسنستمر في تطوير برنامج تغيير التكامل بين مختلف القوات المتعددة التابع لوزارة الدفاع، والذي سيجمع قدرات كافة القوات، ويحقق تكاملا أكبر مع العناصر الأخرى لقوتنا الوطنية، وبالتالي يعزز تفوقنا العسكري على أعدائنا. سيكون المجال الإلكتروني جزءا أساسيا من العمل الدفاعي، ويدعمه متخصصون ماهرون في المجال الإلكتروني، ووعي إلكتروني شامل في كافة قوات الدفاع، وقدرات إلكترونية متطورة وقادرة على الصمود.

[36] وزارة الدفاع،مفهوم العمل المتكامل (2020)

تحقيقات واسعة في جرائم إلكترونية أجرتها أجهزة إنفاذ القانون

عملية إمبريل : كانت عملية إمبريل عبارة عن تحقيقات أجرتها وحدة الجريمة المنظمة المشتركة في جنوب شرق إنجلترا بالتعاون مع المكتب الفيدرالي للتحقيقات (الشرطة الأمريكية) بشأن موقع إلكتروني يبيع معلومات شخصية ومصرفية مسروقة من ضحايا هجمات إلكترونية. ذلك مكّن أشخاصا آخرين من شراء البيانات الشخصية لارتكاب أعمال احتيال وجرائم أخرى تتعلق بإساءة استخدام الكمبيوتر. وقد أدت التحقيقات الموسّعة إلى التعرف على الحسابات المصرفية والدفعات المالية التي استُخدمت لشراء البنية التحتية الفنية، وكشفت أن صاحب الموقع الإلكتروني يُقيم في باكستان. أتاحت تلك التحقيقات للشرطة الأمريكية مصادرة الموقع الإلكتروني سرا وإغلاقه لاحقا. وقد ألقت وحدة الجريمة المنظّمة في جنوب شرق إنجلترا القبض على المشتبه به الرئيسي البريطاني، والذي تبين أنه فتح حسابا مصرفيا أمريكيا لصالح مالك الموقع الإلكتروني من أجل غسيل الأموال المكتسبة من أعمال إجرامية. وارتكب المشتبه به البريطاني عمليات احتيال كبيرة باستخدام بعض البيانات المسروقة من الضحايا، حيث فتح حسابات مصرفية بأسماء أخرى، واستخدم حسابات مصرفية مسروقة لدفع تكاليف عطلات باذخة، ولتقديم مطالبات زائفة لوزارة العمل والتقاعد للحصول على معونات اجتماعية، ما تسبب بخسائر للدولة تزيد عن 90,000 جنيه إسترليني. وُجهت للمشتبه به تسع تهم، وحُكم عليه بالسجن لأربع سنوات، لكن تم تخفيف الحكم نظرا لأنه اعترف بالذنب في وقت مبكّر. وقد أثنى القاضي على فريق التحقيق في هذه العملية. وقت نشر هذه الاستراتيجية، كان جاري العمل على تقديم طلب لمصادرة عوائد الجريمة من المتهم.

عملية نيبيغون : تلك كانت عملية تحقيق أجرتها شرطة لندن بشأن مواطن بلغاري يُشتبه بأنه أنشأ صفحات مخصصة للتصيّد، والتي يُقدّر أنها كلفت المملكة المتحدة خسائر تفوق 40 مليون جنيه إسترليني. تعرفت الشرطة على المشتبه به بعد تحقيق بشأن مرتكب جرائم إلكترونية آخر معروف جيدا وسبق أن حُكم عليه بالسجن 10 سنوات عام 2018، والذي كان يستخدم صفحات التصيد التي أنشأها المواطن البلغاري لينفذ أعماله الإجرامية الخاصة به. وقد بوشر بالتحقيق بعد التعرف على عنوان بريد إلكتروني مهم يتصل بالمشتبه به. وبعد سلسلة من الاستفسارات الطويلة والمعقدة، أدى التحقيق إلى التواصل مع السلطات البلغارية التي اعتقلت المشتبه به وسلمته إلى المملكة المتحدة. وبعد كشف الأدلة بشكل شامل، اعترف المتهم بذنبه في كل الاتهامات الجنائية الموجهة إليه، وحُكم عليه بالسجن لمدة تسع سنوات ونصف السنة.

عملية ليسينغ: في عام 2020، ترأست الوكالة الوطنية لمكافحة الجريمة التحقيقات في تهديد إرهابي بالهجوم بالقنابل يستهدف الهيئة الوطنية للخدمات الصحية، وذلك وقت ذروة تفشي جائحة كوفيد-19. وكان المهاجم قد طالب بمبالغ تُدفع له بعملة البيتكوين. وبالعمل مع السلطات الألمانية، كشفت الوكالة الوطنية لمكافحة الجريمة المشتبه به واعتقلته، وأُدين فيما بعد من قبل محكمة ألمانية.

في 12 إبريل 2020 أرسل مواطن إيطالي يعيش في ألمانيا رسالة إلكترونية عبر شبكة "تور" المشفرة يُعلن فيها عن عزمه تفجير قنبلة في مستشفى تابع للهيئة الوطنية للخدمات الصحية البريطانية ما لم يستلم مبلغ 10 ملايين جنيه إسترليني بعملة البيتكوين.

وقد سارعت الوكالة الوطنية لمكافحة الجريمة إلى تصنيف هذا التهديد على أنه أولوية قصوى، وكلفت ضباط متخصصين بالجريمة الإلكترونية لمعرفة مُرسل التهديد ومنع أي هجوم محتمل.

كما أرسل المهاجم رسائل إلكترونية يهدد فيها بمهاجمة نواب في البرلمان، وبتفجير قنبلة بالمسيرات التي تنظمها في لندن مجموعة "حياة السود مهمة". ورغم أنه كان كتب الرسائل الإلكترونية باللغة الإنجليزية، إلا أن المحققين التابعين للوكالة الوطنية لمكافحة الجريمة استخدموا تقنيات إلكترونية متخصصة وأجروا تحليلا سلوكيا ولغويا للرسائل، واستنتجوا أن كاتبها على الأرجح من الناطقين باللغة الألمانية.

وبالتعاون مع السلطات الألمانية، اكتشف ضباط الوكالة الوطنية لمكافحة الجريمة أن الرسائل الإلكترونية قد أُرسلت من كمبيوتر في عنوان في برلين. وبفضل العمل المشترك الدولي، وعلى الرغم من جهود كبيرة بذلها المشتبه به لإخفاء هويته وموقعه، تم التعرف عليه ووضعته أجهزة الأمن الألمانية تحت المراقبة. وفي 15 يونيو 2020، أُلقي القبض على المشتبه به ووُجهت إليه تهمة محاولة الابتزاز وتم احتجازه. وقد أُدين بتاريخ 26 فبراير 2021 وحُكم عليه بالسجن لثلاث سنوات.

العمل من خلال الفضاء الإلكتروني لمكافحة للإرهاب

حملة التصدي لداعش: العمل الذي تقوم به وزارة الدفاع والقيادة الحكومية المركزية للاتصالات ضد داعش هو مثال على الخطوات الفعالة التي اتخذناها للتصدي للتهديدات من جانب أولئك الذين يُسيئون استخدام قوة الإنترنت ووسائل الاتصالات الحديثة.

فقد خصص تنظيم داعش الكثير من الوقت والجهد للتكنولوجيا من أجل إعداد المحتوى الإعلامي المستخدم في نشر التطرف وجذب المنتسبين الجدد، ولإلهام الإرهابيين في تنفيذ هجمات إرهابية حول العالم. وفي السنوات الأخيرة، رأينا تأثير طريقته هذه في مختلف أنحاء أوروبا، بما في ذلك الهجمات التي وقعت في لندن ومانشستر. كما استخدم تنظيم داعش أنظمة الاتصالات الحديثة في القيادة والسيطرة في عملياته في ساحات القتال. ذلك أتاح لداعش العمل بمرونة على نطاق واسع وبوتيرة سريعة، وأن يُشكّل خطرا أكبر على المجموعات السكانية التي كان يسعى للسيطرة عليها، ولتوسيع رقعة انتشاره في مناطق ما يُطلق عليه "الخلافة الإسلامية".

وخلال معركة الموصل، وهي المدينة التي أعلنها التنظيم عاصمة له، استخدمنا أدوات وتقنيات إلكترونية إلى جانب العمليات العسكرية دعما للتحالف الدولي، وكجزء من حملة واسعة وشاملة. وقد كانت نتائج تلك العمليات واسعة النطاق. حيث أمكن إضعاف فعالية عمليات داعش من خلال عرقلة اتصالاته، وإفشال حملته الدعائية، وزعزعة الثقة ضمن أعضاء التنظيم، وحرمانه من الأجهزة والشبكات المستخدمة كجزء من عملياته. كما تمكنا من استخدام تقنيات إلكترونية لنشر رسائل الحكومة البريطانية إلى الأهداف، أو لتسليط الضوء على أنشطة داعش لمن كانوا يزودونه بالمساعدة دون أن يشكّوا بنواياه. وقد أسهمت تلك العمليات في جهود التحالف الكبيرة لكبح الحملات الدعائية لداعش، وإعاقة قدرته على تنسيق الهجمات، وحماية قوات التحالف في ساحات القتال.

آندرو، من أعضاء القوة الإلكترونية الوطنية

لطالما أثارت إعجابي التكنولوجيا المتطورة. وقبل عملي في جهاز المخابرات، كنت قد التحقت بالشرطة وارتقيت بالعمل من شرطي متجول إلى متخصص بالتحليل الجنائي الرقمي - حيث كان عملي هو فحص الأجهزة الإلكترونية للمتهمين بحثا عن أدلة. أحببت هذا العمل، لكنني أردت اكتشاف فرص أخرى خارج هذا المجال.

أنا لم ألتحق بالجامعة بعد تخرجي من المدرسة، بل كان الفضول الطبيعي هو الذي يوجه مهنتي آنذاك. وهذا ينطبق أيضا على جميع زملائي الذين انضموا إلى القوة الإلكترونية الوطنية. فهم ينحدرون من خلفيات اجتماعية مختلفة. فمنهم من هم خبراء متعمقون في التقنيات، إلى جانب من كان مديرا لفرع سوق مركزي، وآخر كان معلما في مدرسة ابتدائية، وآخر كان رجل إطفاء. والشيء الوحيد المشترك بيننا هو الذهن المنفتح، والشغف للتعلم، وهدفنا المشترك بحفظ وطننا سالما - وذلك بمعرفة ما تخلقه التكنولوجيا الناشئة من فرص وتهديدات بالنسبة لأمننا القومي.

كعنصر شرطة، كنت شديد الفخر بمساعدة الناس على المستوى الشخصي. أما اليوم، وكعضو في فريق مميز في القوة الإلكترونية الوطنية، فأنا جزء من قوة لأجل الخير تعمل على المستوى العالمي.

تحقيق طموحنا

190. لن يكون لهذه الاستراتيجية أي معنى دون اتباع مقاربة حازمة في تنفيذ أهدافها، ورصد وتقييم التقدم الحاصل بناء على تلك الأهداف، ووجود الآليات لتعديل المسار إذا اقتضت الضرورة. يوضح هذا الفصل مقاربتنا تجاه التنفيذ.

الأدوار والمسؤوليات في جميع إدارات الحكومة

191. ستكون الاستراتيجية الإلكترونية الوطنية إحدى الاستراتيجيات الفرعية التي تحقق مجتمعة تطلعات المراجعة المتكاملة. سيمارس مجلس الأمن القومي الاشراف الوزاري على تلك الاستراتيجيات، بحيث يرصد تنفيذها مع مراعاة التوازن الإجمالي للاستراتيجية وتوجهها. كما سيَجري تقييم التقدم بناء على أهداف الاستراتيجية من خلال الإطار الحكومي للتخطيط والأداء، وخطط تحقيق النتائج.

192. لكافة الوزراء دور في ضمان تعزيز موقف المملكة المتحدة كقوة إلكترونية مسؤولة وديمقراطية، وقادرة على حماية وتطوير مصالحها في الفضاء الإلكتروني ومن خلاله. تتضمن هذه القائمة مجموعات محددة من المسؤوليات للوزراء الذين يتولون أدوارا قيادية، إما لتنفيذ أو لتنسيق واحدة أو أكثر من الدعامات الخمس لاستراتيجيتنا الإلكترونية الوطنية، أو للإشراف على أهم قدراتنا الإلكترونية والقرارات المتعلقة بها.

- **مستشار دوقية لانكستر**، بمساندة من **المحاسب العام للحكومة**، يلعب الدور القيادي العام في كل الوزارات لضمان استجابة الحكومة بفعالية للتهديدات الإلكترونية، ولتحقيق طموحاتنا كقوة إلكترونية. ذلك يشمل وضع وتنفيذ الاستراتيجية الإلكترونية الوطنية، والبرنامج الذي يساندها المتعلق بالاستثمارات وتنسيق جهود الحكومة بشأن الصمود الإلكتروني. كما تقع على عاتقهما معا مسؤولية وضع وتنسيق سياسة عامة لكافة القطاعات من أجل ضمان الأمن الإلكتروني للمملكة المتحدة وصمود بنيتها التحتية الحيوية. مستشار دوقية لانكستر هو الرئيس المفترض لاجتماعات اللجنة المركزية الوزارية للاستجابة للأزمات إذا ما دعت الضرورة لانعقادها في حال وقوع حوادث إلكترونية.

- **وزير الداخلية** لديه دور مهم في تنفيذ الاستراتيجية الإلكترونية الوطنية ككل، وفي الاستجابة للحوادث الإلكترونية بما ينسجم مع مسؤولياته تجاه أمن البلاد. وهو الذي يترأس جهود الحكومة في كشف الأعداء وعرقلة خططهم وردعهم، إلى جانب وزير الخارجية والكومنولث والتنمية ووزير الدفاع، ويتولى التنسيق الإجمالي لتلك الجهود. كما إنه مسؤول بشكل خاص عن التصدي للجرائم الإلكترونية.

- **وزير الخارجية وشؤون الكومنولث والتنمية** لديه مسؤولية قانونية تجاه القيادة الحكومية المركزية للاتصالات، وبالتالي تجاه المركز الوطني لأمن المعلوماتية. وهو يترأس عمل الحكومة لتطوير قيادة المملكة المتحدة العالمية في مجال الفضاء الإلكتروني، ولديه مسؤولية محددة في عملية التعرف على مرتكبي الجرائم الإلكترونية، ونظام العقوبات الإلكترونية، والتواصل على الصعيد الدولي بما يخص الحوادث الإلكترونية الكبرى. كما إنه يترأس عمل الحكومة لكشف الأعداء وعرقلة خططهم وردعهم بالتشارك مع وزير الداخلية ووزير الدفاع.

- **وزير الدفاع** يقود العمل الحكومي لكشف الأعداء وإحباط خططهم وردعهم بالتشارك مع وزير الخارجية والكومنولث والتنمية ووزير الداخلية.

- **وزير الخارجية وشؤون الكومنولث والتنمية ووزير الدفاع** مسؤولان عن القوة الإلكترونية الوطنية، والتي هي جهد مشترك بين الدفاع والمخابرات.

- **وزير الشؤون الرقمية والثقافة والإعلام والرياضة** مسؤول عن الأمن الإلكتروني للمؤسسات في مجمل القطاع الاقتصادي نظرا لارتباطه بالسياسة الرقمية والجوانب ذات الصلة بالنمو والابتكار والمواهب ضمن الاستراتيجية الإلكترونية الوطنية. كما إنه مسؤول عن عمل الحكومة من أجل تقوية البيئة الإلكترونية في المملكة المتحدة، وعن مجالات التكنولوجيا الحيوية للقوة الإلكترونية.

- **وزراء كافة الوزارات الحكومية الأساسية بالنسبة للبنية التحتية الحيوية** مسؤولون عن الأمن الإلكتروني وسياسات الصمود، كل ضمن نطاق قطاعه.

- **جميع الوزراء** ملزمون بالإشراف على الأمن الإلكتروني في وزاراتهم، وتطبيق التدابير المناسبة للوقاية من الحوادث الإلكترونية. وحين تكون وزارة ما مسؤولة عن الإشراف على أحد جوانب القطاع الخاص أو العام (مثلا وزارة شؤون الارتقاء بالمناطق وشؤون الإسكان والمجتمعات مسؤولة عن الحكومات المحلية، ووزارة البيئة والغذاء والشؤون الريفية مسؤولة عن شركات المياه)، فإنها تكون مسؤولة أيضا عن السياسة الإلكترونية وإجراءات الضمان المتعلقة بذلك القطاع.

193. نائب مستشار الأمن القومي لشؤون المخابرات والأمن والصمود هو المسؤول الأول عن الاستراتيجية والمكلّف بها، وهو المسؤول عن التنفيذ في كافة قطاعات الحكومة على المستوى الرسمي، يدعمه في ذلك مسؤولون كبار من مختلف الوزارات.

المسؤوليات الوزارية

رئيس الوزراء

وزير الشؤون الرقمية	مستشار دوقية لانكستر*	وزير الخارجية	وزير الدفاع	وزير الداخلية	جميع وزراء الحكومة

تنسيق وقيادة الدعامات الاستراتيجية

البيئة الإلكترونية					الإشراف على المخاطر ودعم إصلاح السياسات
	الصمود				
التكنولوجيا					
		القيادة العالمية			
			التصدي للتهديدات		

العمليات ودعم التنفيذ في كافة جوانب الاستراتيجية

		المركز الوطني لأمن المعلوماتية			
				الوكالة الوطنية لمكافحة الجريمة	
			القوة الوطنية الإلكترونية		

* مسؤول عن القيادة العامة في كافة الوزارات لضمان استجابة الحكومة بفعالية للتهديدات الإلكترونية، وتحقيق طموحاتنا كقوة إلكترونية.

الاستثمار في قوتنا الإلكترونية

194. ستستثمر الحكومة 2.6 مليار جنيه إسترليني في القطاع الإلكتروني وتكنولوجيا المعلومات القديمة على مدى السنوات الثلاث القادمة. وسيكون ذلك بالإضافة إلى استثمارات ضخمة في القوة الإلكترونية الوطنية. سيشمل الاستثمار زيادة قدرها 114 مليون جنيه إسترليني في البرنامج الوطني لأمن المعلوماتية، مع نقل الانفاق السنوي على بناء القدرات بموجب استراتيجية 2016 ليكون تحت إدارة وزارية وبشكل دائم. أما البرامج الدولية، فستُنفّذ من خلال صندوق معالجة الصراع وإحلال الاستقرار والأمن من أجل مساعدة الدول الشريكة في بناء قدرتها على الصمود الإلكتروني والتصدي للتهديدات الإلكترونية. هذا إلى جانب الزيادات المُعلنة في الاستثمار في مجالات البحث والتطوير، والاستخبارات، والدفاع، والابتكار، والبنية التحتية، والمهارات - وجميعها تساهم جزئيا في القوة الإلكترونية للمملكة المتحدة.[37]

قياس النجاح

195. الاستراتيجية يحكمها إطار أداء يجري تطويره بشكل متواصل، ويتضمن رفع تقارير إلى كبار المسؤولين ومجلس الأمن القومي. وسيُستخدم الإطار للاسترشاد به في النقاشات مع الجهات البرلمانية وغيرها التي تشرف على عمل أجهزة الأمن القومي. وبما ينسجم مع مقاربة الاستراتيجية الوطنية لأمن المعلوماتية 2016 - 2021، لن يكون هذا الإطار وثيقة للتداول العام نظرا لحساسية المعلومات التي يحتويها. إلا أن الحكومة ستنشر تقارير سنوية عن التقدم الحاصل.

196. إطار الأداء المذكور سوف:

- يوفر مسارا واضحا للطريقة التي سيؤدي بها عملنا إلى تحقيق الغايات المختلفة المبينة في هذه الاستراتيجية
- يضمن المساءلة عن تنفيذ الاستراتيجية
- يوفر الشفافية بشأن التقدم الذي تحرزه الدولة نحو تحقيق الأهداف المبينة في هذه الاستراتيجية
- يوضح كيف يجب تعديل عملنا لينسجم مع الاستراتيجية
- يساعد في فهم النشاطات التي تسهم بفاعلية في تحقيق طموحات الاستراتيجية، بحيث يمكن تطبيق الدروس المستفادة في المستقبل
- يقدم نظرة إجمالية عن الفعاليات في الدعامات الخمس للاستراتيجية، بما يقلل من ازدواجية العمل، ويحدد نقاط القوة والضعف في القوة الإلكترونية للدولة
- يضمن أن توفر الاستراتيجية الدعم الإلكتروني لكافة قطاعات المجتمع

[37] وزارة الخزانة، الميزانية ومراجعة الانفاق لخريف 2021 (2021)

الخطوات التالية

197. يُقصد من هذه الاستراتيجية أن تكون دليلا إرشاديا للعمل، ليس فقط للمسؤولين في الحكومة عن المجال الإلكتروني ومجموعة السياسات المتعلقة به (انظر الملحق أ)، بل أيضا لكل شخص ومؤسسة في كافة قطاعات المجتمع ممن لديهم مصلحة في، ومسؤولية عن، جهودنا الوطنية في القطاع الإلكتروني. كما تُعتبر الاستراتيجية بداية لحوار نريد له أن يستمر لضمان أن تبقى أهدافنا وأولوياتنا مفيدة على مدى السنوات الخمس أو العشر القادمة. وسوف نستخدم نشر هذه الاستراتيجية كمنصة تفسح المجال لمزيد من التفاعل مع القطاعين العام والخاص، وكذلك القطاعات الأخرى، في مختلف أنحاء المملكة المتحدة. ونحن ندعو لإبداء الملاحظات مباشرة بالبريد الإلكتروني ukcyberstrategy@cabinetoffice.gov.uk. وسوف نرفع تقارير سنوية عن التقدم الذي نحرزه في تطبيق هذه الاستراتيجية.

الملحق(أ) القطاع الإلكتروني كجزء من أجندة الحكومة الأوسع نطاقا

يُقصد من الاستراتيجية الإلكترونية الوطنية أن تدعم وتوسّع أولويات الحكومة الأخرى في قطاعات الأمن، والدفاع، والسياسة الخارجية، وأجندتنا الاقتصادية. وتعتمد هذه الاستراتيجية بدورها على القدرات الأوسع التي جرى تطويرها من خلال برامجنا للتعليم وتنمية المهارات، ومقاربتنا الوطنية للسياسة التكنولوجية والرقمية، والأبحاث، ونمو قطاع الأعمال. فيما يلي الاستراتيجيات والخطط الأساسية ذات الصلة:

- **المراجعة المتكاملة**، بما فيها الجهود الوطنية لرفع كفاءة الصمود، والتصدي للتهديدات من الدول ومن مجموعات الجريمة الخطيرة المنظمة والإرهاب، والحفاظ على تفوقنا الاستراتيجي من خلال العلوم والتكنولوجيا، وبلورة النظام العالمي

- **الاستراتيجية الوطنية للبيانات**، والتي تطرح رؤيتنا لتسخير قوة الاستخدام المسؤول للبيانات من أجل تعزيز الإنتاجية، وإنشاء شركات ووظائف جديدة، وتحسين الخدمات العامة، ودعم مجتمع أكثر عدلا، وتشجيع الاكتشافات العلمية، وبالتالي وضع المملكة المتحدة في صدارة الموجة التالية من الابتكار. ذلك يشمل تغيير أسلوب استخدام الحكومة للبيانات من أجل زيادة الكفاءة وتحسين الخدمات العامة من خلال معالجة العوائق التي تعترض تبادل المعلومات بين الوزارات، وتحسين جودة البيانات التي بحوزتها. سيكون ذلك ضروريا لدعم أجندتنا الإلكترونية، ومنها ضمان أن نتمكن من جمع واستخدام بيانات عالية الجودة فيما يخص الحوادث الإلكترونية

- **خطة النمو** ، وهي تساعدنا على **النهوض بشكل أفضل** من خلال مزيد من الدعم والاستثمار في البنية التحتية والمهارات والابتكار، **واستراتيجية الابتكار** التي تحدد طموحاتنا في اقتصاد يحركه الابتكار

- **التخطيط للتنظيم الرقمي**، وهو يحدد مقاربتنا الداعمة للتطوير بشأن تنظيم التقنيات الرقمية بطريقة تحفّز الازدهار، وتنمي الثقة باستخدام تلك التقنيات

- **الاستراتيجية الوطنية للذكاء الاصطناعي**، وهي تهيئ المملكة المتحدة للعقد القادم من التحولات في الذكاء الاصطناعي عن طريق الاستثمار في الاحتياجات طويلة الأمد لبيئة الذكاء الاصطناعي، ودعم الانتقال إلى اقتصاد يقوم على الذكاء الاصطناعي، وضمان حصول المملكة المتحدة على حق حوكمة تقنيات الذكاء الاصطناعي على المستويين الوطني والدولي. ويتضمن ذلك أيضا التدابير اللازمة لدعم الابتكارات الآمنة إلكترونيا في أنظمة قائمة على الذكاء الاصطناعي، مع حماية المواطنين وبناء الثقة بشأن استخدام تلك الابتكارات

- **الاستراتيجية الوطنية للصمود** التي ستُنشر لاحقا، والتي ستركز في بعض جوانبها على كيفية إبقاء المملكة المتحدة قادرة على التعامل بنجاح مع التهديدات التكنولوجية، والمحافظة على صمودها في الفضاء الإلكتروني

- **الاستراتيجية الرقمية** التي ستُنشر لاحقا، والتي ستطرح رؤية واضحة لطموحات الحكومة في تسخير الإقبال الجديد على التحول الرقمي، وتسريع النمو، ومواصلة بناء اقتصاد رقمي أكثر تنافسية وشمولا وابتكارا للمستقبل، والذي سيرتكز على الأولويات التقنية العشر لوزارة الشؤون الرقمية والثقافة والإعلام والرياضة لوضع المزيد من الطموحات الحكومية في القطاع الرقمي

- **استراتيجية خفض الانبعاثات إلى الصفر** وهي ستضمن أن يكون اقتصادنا المزدهر والقائم على الابتكار اقتصادا منخفض الانبعاثات الكربونية

- **خطة القضاء على الجريمة**، وهي تطرح تصورنا لكيفية استعادة الثقة بنظام العدالة الجنائية، وتحقق رؤيتنا المشتركة بأن تكون بريطانيا أكثر أمنا وفيها عدد أقل من الجرائم ومن الضحايا أيضا[38]

[38] وزارة الداخلية، خطة التغلب على الجريمة (2021)

الاستراتيجية الإلكترونية الوطنية تدعمها بشكل مباشر وثيقتان أخريان متوقعتان تبينان كيفية تنفيذ بعض الأجزاء المنفردة من الاستراتيجية، وهما:

- **الاستراتيجية الحكومية لأمن المعلوماتية** التي ستُنشر لاحقا، وهي تضع خططا أكثر تفصيلا لرفع كفاءة أمن الحكومة والقطاع العام دعما لهذه الاستراتيجية الوطنية
- **مراجعة الحوافز واللوائح 2021** التي ستُنشر لاحقا، والتي تستعرض ما توصلنا إليه بشأن مقدار فاعلية عملنا في تحفيز التحسينات في الأمن الإلكتروني ضمن إطار الاقتصاد الأوسع، وما نقترحه لتطبيق الجوانب المتعلقة بالأعمال والمؤسسات في الدعامة المتعلقة بالصمود في هذه الاستراتيجية

الملحق (ب): اللوائح بشأن الشبكات وأنظمة المعلومات - الاستراتيجية الوطنية

مقدمة

الاستراتيجية الوطنية للوائح بشأن الشبكات وأنظمة المعلومات

1. تُعتبر الاستراتيجية الإلكترونية الوطنية بمثابة الاستراتيجية الوطنية للمملكة المتحدة لأغراض اللائحة رقم 2 من اللوائح بشأن الشبكات وأنظمة المعلومات البريطانية لعام 2018.

2. يقدم هذا الملحق معلومات إضافية وتشمل:

- أدوار ومسؤوليات الهيئات الرئيسية المسؤولة عن تطبيق اللوائح بشأن الشبكات وأنظمة المعلومات في المملكة المتحدة؛
- وقائمة بالهيئات الرئيسية المعنية.

اللوائح بشأن الشبكات وأنظمة المعلومات في المملكة المتحدة

3. في 2016، وافقت المفوضية الأوروبية على توجيهات تهدف لزيادة أمن الشبكات وأنظمة المعلومات في الاتحاد الأوروبي، وقد أيدت الحكومة البريطانية تلك التوجيهات.

4. في 20 إبريل 2018، قدمت الحكومة إلى البرلمان اللوائح بشأن الشبكات وأنظمة المعلومات لعام 2018، وقد دخلت هذه اللوائح حيز التنفيذ بتاريخ 10 مايو 2018.

5. أرست اللوائح بشأن الشبكات وأنظمة المعلومات أسلوبا تنظيميا جديدا في المملكة المتحدة يتطلب من المشغّلين المعينين للخدمات الضرورية ومن مقدمي الخدمات الرقمية ذات الصلة وضع تدابير فنية وتنظيمية من أجل حماية شبكاتهم وأنظمة معلوماتهم.

6. ينطبق ذلك على القطاعات الحيوية لاقتصادنا ولمجتمعنا، والتي تعتمد اعتمادا كبيرا على الشبكات وأنظمة المعلومات، مثل الطاقة، والنقل، ومياه الشرب، والرعاية الصحية، والبنية التحتية الرقمية.

7. كما يشمل ذلك مقدمي الخدمات الرقمية الأساسية (محركات البحث، وخدمات الحوسبة السحابية، والأسواق على الإنترنت).

8. تؤسس اللوائح بشأن الشبكات وأنظمة المعلومات ما يلي:

- **إطارا وطنيا** لدعم التنفيذ، بما في ذلك استراتيجية وطنية بهذا الشأن؛
- سلطات معنية **بالقطاع** لتكون بمثابة جهات تنظيمية؛
- المركز الوطني لأمن المعلوماتية باعتباره **نقطة اتصال وحيدة**، وأيضا **فريق الاستجابة لحوادث أمن الكمبيوتر**.

9. يجري تقييم التقدم الحاصل عن طريق إجراء مراجعات ما بعد التنفيذ كل سنتين إلى خمس سنوات.

الأدوار والمسؤوليات الرئيسية

الإطار الوطني

10. وزارة شؤون مجلس الوزراء مسؤولة عن الاستراتيجية الإلكترونية الوطنية، والتي تتضمن الاستراتيجية الوطنية للوائح بشأن الشبكات وأنظمة المعلومات. كما إن الوزارة مسؤولة أيضا عموما عن تحسين أمن وصمود البنية التحتية الحيوية الوطنية.

11. وزارة الشؤون الرقمية والثقافة والإعلام والرياضة مسؤولة عن التنفيذ عموما للوائح بشأن الشبكات وأنظمة المعلومات. ويشمل ذلك تنسيق العمل مع الهيئات المعنية والمركز الوطني لأمن المعلوماتية. تُصدر الوزارة توجيهات للهيئات المعنية لدعم تطبيق اللوائح بشأن الشبكات وأنظمة المعلومات عموما في مختلف أنحاء المملكة المتحدة.

نقطة الاتصال الوحيدة

12. هي نقطة الاتصال الوطنية للتعامل مع الشركاء الدوليين (الاتحاد الأوروبي) بشأن الشبكات وأنظمة المعلومات، وتنسيق الطلبات لاتخاذ إجراءات أو لتوفير معلومات، ولتقديم إحصاءات سنوية عن الحوادث. المركز الوطني لأمن المعلوماتية هو نقطة الاتصال الوحيدة بالنسبة للمملكة المتحدة.

فريق الاستجابة لحوادث أمن الكمبيوتر

13. فريق الاستجابة لحوادث أمن الكمبيوتر في المملكة المتحدة متمثل في المركز الوطني لأمن المعلوماتية. وهو مسؤول عن مراقبة حوادث الأمن الإلكتروني على المستوى الوطني؛ ويقدم تحليلات آنية للتهديدات، والحماية ضد الهجمات الإلكترونية على المستوى الوطني، والمشورة الفنية، والاستجابة للحوادث الإلكترونية الكبيرة من أجل تخفيف ضررها.

14. يدير المركز الوطني لأمن المعلوماتية إطارا للتقييم الإلكتروني يستند إلى النتائج المحققة، ويقدم توجيهات إرشادية موسّعة فيما يتعلق بالأمن الإلكتروني بصفته هيئة فنية وطنية.

الهيئات المعنية

15. هي الجهات المسؤولة عن الإشراف على اللوائح بشأن الشبكات وأنظمة المعلومات وتطبيقها في القطاعات الخاصة بها، وهي تحدد مشغلي الخدمات الضرورية ومقدمي الخدمات الرقمية ذات الصلة، وتقيّم درجة امتثالهم لمتطلبات اللوائح بشأن الشبكات وأنظمة المعلومات. وهذه الهيئات مدرجة في الجدول 1 من اللوائح بشأن الشبكات وأنظمة المعلومات، وتوجد قائمة بها في القسم 3.

مشغلو الخدمات الضرورية ومقدمو الخدمات الرقمية ذات الصلة

16. مشغلو الخدمات الضرورية ومقدمو الخدمات الرقمية ذات الصلة، والذين يستوفون معايير الأهمية الحيوية في ذلك القطاع، أو الذين تتحدد أهميتهم الحيوية من قبل الهيئات ذات الصلة بموجب اللائحة 8(3) من اللوائح بشأن الشبكات وأنظمة المعلومات، عليهم أن يلتزموا بمتطلبات اللوائح بشأن الشبكات وأنظمة المعلومات.

17. هذه المتطلبات تشمل كلا مما يلي:

- اتخاذ خطوات فنية وتنظيمية ملائمة ومتناسبة من أجل إدارة المخاطر التي يتعرض لها أمن الشبكات وأنظمة المعلومات؛
- اتخاذ خطوات ملائمة ومتناسبة لمنع وقوع الحوادث وتخفيف أثرها على أمن الشبكات وأنظمة المعلومات؛
- إبلاغ الهيئات المسؤولة ذات الصلة عن أي حادث له أثر بالغ على خدماتها؛
- تلبية متطلبات التفتيش بموجب اللوائح بشأن الشبكات وأنظمة المعلومات؛
- الالتزام بالمعلومات والتطبيق والإشعارات بالغرامات.
- يُطلب أيضا من مقدمي الخدمات الرقمية ذات الصلة التسجيل لدى مكتب المفوض المعني بالحقوق المتعلقة بالمعلومات.

هيئات أخرى ذات صلة:

18. تعمل الحكومة البريطانية بشكل وثيق مع الحكومات المفوّضة وغيرها من السلطات ذات الصلة، بما في ذلك الوزارات الحكومية الرئيسية، بشأن تطبيق اللوائح بشأن الشبكات وأنظمة المعلومات.

19. مركز حماية البنية التحتية الوطنية يوفر المشورة بشأن الأمن المادي وأمن العاملين.

قائمة بالهيئات الرئيسية المعنية بتطبيق اللوائح بشأن الشبكات وأنظمة المعلومات

الهيئات الوطنية	
اللوائح بشأن الشبكات وأنظمة المعلومات في المملكة المتحدة	وزارة الشؤون الرقمية والثقافة والإعلام والرياضة
الاستراتيجية الإلكترونية الوطنية في المملكة المتحدة	وزارة شؤون مجلس الوزراء
نقطة الاتصال الوحيدة في المملكة المتحدة	المركز الوطني لأمن المعلوماتية
فريق الاستجابة لحوادث أمن الكمبيوتر في المملكة المتحدة	المركز الوطني لأمن المعلوماتية

الهيئات ذات الصلة					
القطاع	**القطاع الفرعي**	**إنجلترا**	**ويلز**	**اسكتلندا**	**إيرلندا الشمالية**
الطاقة	الكهرباء	مشتركة: وزارة الأعمال والطاقة والاستراتيجية الصناعية، وهيئة أسواق الغاز والكهرباء			وزارة المالية
	النفط	وزارة الأعمال والطاقة والاستراتيجية الصناعية			وزارة المالية
	الغاز	مشتركة: وزارة الأعمال والطاقة والاستراتيجية الصناعية، وهيئة أسواق الغاز والكهرباء[39]			وزارة المالية
النقل	الجوي	مشتركة: وزارة النقل وهيئة الطيران المدني			
	السكة الحديدية	وزارة النقل			وزارة المالية
	البحري	وزارة النقل			
	البري	وزارة النقل		وزراء من اسكتلندا	وزارة المالية
الرعاية الصحية	أنظمة الرعاية الصحية	وزارة الصحة والرعاية الاجتماعية	وزراء من ويلز	وزراء من اسكتلندا	وزارة المالية
مياه الشرب	مياه الشرب	وزارة البيئة والأغذية والشؤون الريفية	وزراء من ويلز	الجهة التنظيمية لجودة مياه الشرب في اسكتلندا	وزارة المالية
البنية التحتية الرقمية	البنية التحتية الرقمية	مكتب الاتصالات			

[39] بالنسبة لاستثناءات معينة، تُعتبر وزارة الأعمال والطاقة والاستراتيجية الصناعية هي الهيئة المسؤولة الوحيدة. لمزيد من التفاصيل انظر الجدول 1 و2 من اللوائح بشأن الشبكات وأنظمة المعلومات لعام 2018.

الملحق (ج) المصطلحات

إدارة الحادث Incident Management -
إدارة وتنسيق الجهد للتحقيق في، وتخفيف أثر، حادث إلكتروني عدائي وقع أو محتمل وقوعه وقد يؤدي لتقويض نظام أو شبكة والتسبب بأضرار.

الاستجابة لدى وقوع حادث Incident Response - جهود معالجة الآثار المباشرة قصيرة المدى نتيجة حادث ما، كما يمكن أن تساعد في التعافي على الأجل القصير.

إطار التقييم الإلكتروني Cyber Assessment Framework (CAF) –
يوفر طريقة منهجية وشاملة لتقييم إلى أي مدى تعمل المؤسسة المعنية على إدارة المخاطر الإلكترونية للمهام الحيوية.

الأمن الإلكتروني Cyber Security -
حماية الأنظمة المتصلة بالإنترنت (ذلك يشمل الأجهزة والبرمجيات 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.

آمن بأساس التصميم Secure by design - برامج إلكترونية وأجهزة وأنظمة مصممة أصلا بمجملها لتكون آمنة.

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 وبرمجيات ومجسات يمكنها إيصال وتبادل المعلومات عبر الإنترنت.

برمجيات انتزاع الفدية Ransomeware -
برنامج خبيث يحرم المستخدم من إمكانية الاطلاع على ملفاته أو تشغيل كمبيوتره أو جهازه إلا بعد دفع فدية.

بنك المعرفة حول الأمن الإلكتروني Cyber Security Body of Knowledge (CyBOK) – مورد فريد يوفر، ولأول مرة، قدرا كبيرا من المعرفة حول الأمن الإلكتروني على اتساعه وعمقه، ويتبين منه بأن الأمن الإلكتروني يشمل نطاقا واسعا من التخصصات.

البنية التحتية الوطنية الحيوية Critical National Infrastructure –
هي عناصر البنية التحتية (وتحديدا الموارد والمرافق والأنظمة والشبكات والعمليات، والعاملين الأساسيين الذين يشغلونها ويُسهلون عملها)، والتي يمكن أن تؤدي خسارتها أو تقويضها إلى:

أ. ضرر كبير يؤثر على توفر أو سلامة أو تقديم خدمات أساسية – بما فيها الخدمات التي يمكن أن تؤدي، في حال تقويض سلامتها، إلى خسائر كبيرة في الأرواح أو وقوع إصابات – وتؤخذ في عين الاعتبار الأضرار الاقتصادية أو الاجتماعية الكبيرة الناجمة عن ذلك،

ب. و/أو آثار كبيرة على الأمن القومي أو الدفاع الوطني أو قدرة الدولة على أداء مهامها.

البيئة الإلكترونية Cyber Ecosystem -
إجمالي البنية التحتية المترابطة والأشخاص والعمليات والبيانات والمعلومات وتقنيات الاتصال، إلى جانب البيئة والعوامل التي تؤثر في هذه التعاملات.

التحقق Authentication – عملية التحقق من هوية مُستخدِم أو عملية أو جهاز ما أو بيانات أخرى ذات صلة تتعلق بأي منهم.

التخطيط للتنظيم الرقمي Plan for Digital Regulation – تحديد مقاربة الحكومة بشكل عام لإدارة التقنيات الرقمية لأجل دفع النمو والابتكار.

تعزيز الدفاعات الإلكترونية Active Cyber Defence (ACD) – برنامج يساعد المؤسسات لإيجاد نقاط الضعف ومعالجتها، أو إدارة الحوادث الإلكترونية، أو أتمتة عرقلة الهجمات الإلكترونية. بعض الخدمات متوفرة أساسا للمؤسسات الحكومية، بينما بعضها الآخر متاح على نطاق أوسع للقطاع الخاص أو المواطنين، بناء على مدى انطباقها وصلاحيتها.

التقنيات العملية Operational Technologies – تجمع البرمجيات والأجهزة لمراقبة العمليات المادية وضبطها وأتمتتها، وخاصة في القطاعات الصناعية مثل الطاقة والتصنيع والمياه والنقل.

التقنيات الكمية Quantum Technologies – تعتمد التقنيات الكمية على مبادئ الفيزياء الكمية. وتطوير وفهم وضبط ما يُعرف بمصطلح «الآثار الكمية»، كالانطباق والاشتباك، سوف يؤدي إلى موجة جديدة من التطور الذي يعزز اقتصادنا وينمي مجتمعنا: الإدراك، ونقل البيانات والتشفير، والتوقيت، والحوسبة.

تقنية الكتل المتسلسلة Blockchain Technology – طريقة معينة لتخزين البيانات. الكتل المتسلسلة هي مثال على مجموعة البيانات المنسقة والموزعة – نوع من تقنية التخزين التي يمكن فقط إرفاق محتواها ولا يمكن التلاعب بها.

تكنولوجيا المعلومات القديمة Legacy IT - تشير إلى الأنظمة الإلكترونية وبرمجياتها وأجهزتها التي لم تعد مشمولة بدعم فني من الجهة البائعة، أو أنها مشمولة في ترتيبات ممددة للدعم الفني أو بترتيبات خاصة للدعم الفني.

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

التوأم الرقمي Digital Twin – هو تقليد أو تمثيل افتراضي لموارد أو عمليات أو أنظمة أو مؤسسات في بيئات عمرانية أو مجتمعية أو طبيعية، ويتيح تكوين فكرة معمّقة حول كيفية تصرف الموارد المادية المعقدة والمواطنين، وذلك يساعد المؤسسات في تحسين اتخاذ القرار وتحقيق أكبر كفاءة من العمليات. التغييرات في العالم الواقعي تظهر أيضا في توأمها، والتغييرات في التوأم يمكن محاكاتها في العالم الواقعي.

توليد الطاقة على نطاق مصغّر Microgeneration – توليد الطاقة على نطاق مصغّر في البيوت والشركات الصغيرة والمجتمعات.

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).

حادث إلكتروني Cyber Incident - حادث يهدد فعليا، أو يمكن أن يهدد، جهاز كمبيوتر أو جهاز متصل بالإنترنت أو شبكة متصلة بالإنترنت – أو بيانات تجري معالجتها أو تخزينها أو بثها عبر هذه الأنظمة – وقد يتطلب اتخاذ إجراء لتخفيف آثاره.

الحكومة المفوضة أو الإدارة المفوضة Devolved government or administration –
هي الحكومات التشريعية والتنفيذية المنفصلة في اسكتلندا وويلز وإيرلندا الشمالية، وهي مسؤولة عن الكثير من مسائل السياسات المحلية في بلدانها، ولديها صلاحية إصدار قوانين في هذه المجالات.

خدمة الإبلاغ عن نقطة ضعف Vulnerability reporting service – آلية يمكن للمؤسسة من خلالها التنبيه لوجود ثغرات أمنية قبل أن يستغلها مخترقو الشبكات.

الخطر الإلكتروني Cyber Risk – إمكانية أن يستغل تهديد إلكتروني معين نقاط الضعف في نظام معلومات ما ويتسبب بالضرر.

الذكاء الاصطناعي Artificial Intelligence –
هي تقنية لترميز نظام حوسبة «ليفكر بنفسه»، بحيث يتكيف ويعمل تلقائيا. يستخدم الذكاء الاصطناعي بشكل متزايد في مهام أكثر تعقيدا، كالتشخيص الطبي، واكتشاف المخدرات، والصيانة الوقائية.

سلامة المعلومات Integrity - في أمن المعلومات، سلامة المعلومات تعني بأن المعلومات لم تتعرض للتغيير عن قصد، أو عن غير قصد، وهي معلومات دقيقة وتامة.

السلطات المختصة Competent Authorities –
الجهات التنظيمية وفق ما هي موصوفة في التوجيهات بشأن الشبكات وأنظمة المعلومات لسنة 2018. توجد سلطات مختصة عديدة مسؤولة عن قطاعات مختلفة تنطوي تحت الشبكات وأنظمة المعلومات.

شركة الإنترنت للأسماء والأرقام المخصصة (آيكان) ICANN – معنية بتنسيق أسماء المواقع الإلكترونية وعنوان بروتوكول الإنترنت.

الصمود الإلكتروني Cyber Resilience - القدرة العامة للأنظمة والمؤسسات على الصمود في مواجهة حوادث إلكترونية، والتعافي منها في حال وقوع ضرر.

علم التشفير Cryptography - علم أو دراسة تحليل وفك تشفير الرموز والشيفرات؛ تحليل الشيفرات.

العملة الرقمية Cryptocurrency – هي عملة رقمية ونظام الدفع بها، مثل عملة بيتكوين.

العيون الخمس Five Eyes – هو اسم التحالف الاستخباراتي الذي يضم الولايات المتحدة والمملكة المتحدة وكندا وأستراليا ونيوزيلندا، ويساعد في تبادل المعلومات للحفاظ بأكبر قدر ممكن على حماية المواطنين من التهديدات.

القيادة الحكومية المركزية للاتصالات GCHQ -
المركز المعني باستخبارات الإشارات في الحكومة والهيئة الفنية الوطنية للمعلوماتية.

كشف المعلومات Data Breach -
نقل أو كشف معلومات متوفرة على شبكة ما إلى طرف لا يحق له استلام أو الاطلاع على هذه المعلومات.

اللجنة المركزية للاستجابة للأزمات COBR –
هي لجنة مركزية في الحكومة البريطانية تجتمع عادة في مقر الحكومة في ويستمنستر، ومن خلالها يجري تفعيل الاستجابة المركزية ورصدها وتنسيقها، وهي تمثل النقطة المحورية للاستجابة الحكومية، ومصدرا موثوقا للمشورة المقدمة للأجهزة الأمنية المحلية المستجيبة.

اللوائح بشأن الشبكات وأنظمة المعلومات لسنة 2018 Network and Information Systems Regulations – هي اللوائح البريطانية التي تعطي التدابير القانونية لتعزيز مستوى الأمن (سواء الصمود الإلكتروني أو المادي) للشبكات وأنظمة المعلومات لتوفير الخدمات الضرورية والخدمات الرقمية.

المجتمعات المرتبطة بالإنترنت Connected Places – عبارة عن مجتمع يدمج المعلومات وتقنيات الاتصالات وأجهزة إنترنت الأشياء لجمع وتحليل البيانات بهدف تقديم خدمات جديدة في المدن، وتحسين جودة حياة المواطنين.

المراجعة المتكاملة Integrated Review – «بريطانيا العالمية في عصر التنافس، المراجعة المتكاملة للأمن والدفاع والتنمية والسياسة الخارجية» تصف رؤية الحكومة البريطانية لدور المملكة المتحدة في العالم على مدى العقد القادم، والإجراء الذي ستتخذه الحكومة حتى سنة 2025.

المركز الحكومي للتنسيق الإلكتروني GCCC – مشروع مشترك بين المجموعة الأمنية الحكومية، والمكتب الوطني للشؤون الرقمية والبيانات، والمركز الوطني لأمن المعلوماتية، حيث تجتمع مهام كل منهم ومجالات خبراتهم لتحسين تنسيق الجهود العملياتية للأمن الإلكتروني في جميع الإدارات الحكومية، وإحداث تحوّل في كيفية الاستفادة من المعلومات المتوفرة حول البيانات والتهديدات المتعلقة بالأمن الإلكتروني في جميع أنحاء الحكومة، وتعزيز قدرة الحكومة حقا على «الدفاع كجهاز واحد».

المركز الوطني لأمن المعلوماتية National Cyber Security Centre – هي الجهة الفنية في المملكة المتحدة المعنية بالتصدي للتهديدات، وبلورة استجابة وطنية موحدة لتقليل ضررها، والمساعدة في التعافي منها، والاستفادة من الدروس للمستقبل.

مركز مكافحة الاحتيال Action Fraud – المركز المعني بعمليات الاحتيال والجرائم الإلكترونية، والذي يجب أن يلجأ إليه المواطنون والمؤسسات للإبلاغ عن عمليات الاحتيال إن كانوا قد تعرضوا للخداع أو الاحتيال أو لجريمة إلكترونية في إنجلترا وويلز وإيرلندا الشمالية. أما في اسكتلندا، فتُقدَّم البلاغات للشرطة الإسكتلندية.

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.

مشغلو الخدمات الضرورية Operators of Essential Services – هي المؤسسات ضمن القطاعات الحيوية التي تعتمد اعتمادا كبيرا على شبكات المعلومات، كقطاعات المرافق والرعاية الصحية والنقل والبنية التحتية الرقمية وفق ما تحدده المعايير في اللوائح بشأن الشبكات وأنظمة المعلومات لسنة 2018.

مفتاح التشفير Crypt-Key – هذا المصطلح يصف استخدام المملكة المتحدة للتشفير لحماية معلومات وخدمات حيوية تعتمد عليها الحكومة البريطانية والجيش والأجهزة المعنية بالأمن القومي، بما في ذلك الحماية من اعتداء من أعدائنا الأكثر تمكّنا.

مقدمو الخدمات المدارة Managed Service Providers – أطراف ثالثة تقدم مجموعة من الخدمات المعينة للعميل وتتولى مسؤولية إدارة تلك الخدمات والاستمرار بها وتوفيرها.

المنتدى العالمي للخبرات الإلكترونية GFCE

منظمة التعاون الاقتصادي والتنمية OECD – هي منظمة اقتصادية حكومية.

الناتو NATO – منظمة حلف شمال الأطلسي

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

نظام التحكم الصناعي Industrial Control System - نظام معلومات يُستخدم للتحكم بالعمليات الصناعية، كالتصنيع والتعامل مع المنتجات والإنتاج والتوزيع، أو للتحكم بموارد البنية التحتية.

النظام المستقل Autonomous System – مجموعة من شبكات بروتوكولات الإنترنت (IP) التي يكون التحويل إليها من خلال كيان أو نطاق محدد.

نقطة ضعف Vulnerability - أخطاء في برمجيات يمكن للقراصنة استغلالها.

الهجوم الإلكتروني Offensive Cyber – إضافة أو حذف أو التلاعب بالبيانات على أنظمة أو شبكات للتسبب بأثر مادي أو افتراضي أو إدراكي. عمليات الهجوم الإلكتروني عادة ما تستغل نقاط الضعف الفنية أو الأنظمة أو الشبكات بطرق تتنافى مع استغلالها، أو الموافقة على استغلالها، من جانب أصحابها أو مشغليها، وقد تعتمد على الخداع أو التحايل.

هجوم إلكتروني Cyber Attack – استغلال متعمد لأنظمة الكمبيوتر، والمؤسسات والشبكات التي تعتمد على النظام الرقمي، وذلك بهدف التسبب بالضرر.

الوكالة الوطنية لمكافحة الجريمة
National Crime Agency