مؤشر الجاهزية الإلكترونية 2.0

خطة للجاهزية الإلكترونية: خط قاعدي ومؤشر

الباحث الرئيس: ميليسا هاثاواي

كريس دمتشاك، جيسون كيربن، جينيفر مكأردل، فرانشسكا سبيداليري

نوفمبر 2015

POTOMAC INSTITUTE FOR POLICY STUDIES

تم النشر بواسطة: معهد بوتوماك للدراسات السياسية

معهد بوتوماك للدراسات السياسية
901 N. Stuart St, Suite 1200
Arlington, VA, 22203
www.potomacinstitute.org
هاتف: 703 525 0770؛ فاكس: 703 525 0299

بريد إلكتروني: *CyberReadinessIndex2.0@potomacinstitute.org*

تابعونا على موقع تويتر:
@CyberReadyIndex

شكر وتقدير

يتقدم معهد بوتوماك للدراسات السياسية بالشكر والتقدير لقسم تطبيقات تقنيات المعلومات والاتصالات والأمن الإلكتروني في الاتحاد الدولي للاتصالات، وللجنة البلدان الأمريكية لمحاربة الإرهاب التابعة لمنظمة الدول الأمريكيةعلى الدعم المستمر. كما يتقدم المؤلفون بالشكر إلى شيري لوفليس وألكس تاليسن لإنجازهما لأعمال التحرير والتصميم.

مؤشر الجاهزية الإلكترونية 2.0

خطة للجاهزية الإلكترونية: خط قاعدي ومؤشر

قائمة المحتويات

مؤشر الجاهزية الإلكترونية 2.0

خطة للجاهزية الإلكترونية: خط قاعدي ومؤشر

الباحث الرئيس: ميليسا هاثاواي
كريس دمتشاك، جيسون كيربن،
جينيفر مكأردل، فرانشسكا سبيداليري

مؤشر الجاهزية الإلكترونية 2.0 هو نُسخة مُوسعة من مؤشر الجاهزية الإلكترونية 1.0 الذي تم نشره في نوفمبر 2013.

المُقدمة

في يومنا هذا، تفتقر جميع الدول للجاهزية الإلكترونية.

من المعلوم أن النمو الاقتصادي العالمي أصبح يعتمد بشكل متزايد على الاستعمال السريع لتكنولوجيا المعلومات والاتصالات (ICT) وعلى ربط المجتمع بالإنترنت.في الواقع، تعد الأجندات الرقمية لجميع الدول بتنشيط النمو الاقتصادي وبزيادة الفعالية وتحسين تقديم الخدمات وكفاءتها ودفع الابتكار والمكاسب الإنتاجية وتعزيز الحوكمة الجيدة. ولكن توفر هذه البنية التحتية المهمة وسلامتها ومرونتها عُرضة للأذى. إن حجم ونطاق وسرعة وتعقيد التهديدات التي تواجه أنظمة شبكاتنا وبنانا التحتية حقيقية ومتنامية. فخروقات البيانات والنشاطات الإجرامية وتعطيل الخدمات وتدمير الممتلكات أصبحت من الأمور الشائعة وهي تهدد اقتصاد الإنترنت.

يُدرك قادة العالم أن الربط المتزايد بالإنترنت لا يؤدي إلى النمو الاقتصادي إلا في حال كانت البنية التحتية الأساسية والأدوات المُتصلة آمنة ومُؤمنّة. بالتالي، ينبغي على الدول تنظيم نظراتها الاقتصادية الوطنية لتتماشى مع أولوياتها الأمنية الوطنية.

ولكن، ولغاية الآن، لم يتم وضع منهجية شاملة وتجريبية ومبنية على المُقارنة لتقييم مستوى نضج الدول والتزامها بتأمين بنيتها التحتية الإلكترونية التي يعتمد عليها نموها ومستقبلها الرقمي. مؤشر الجاهزية الإلكترونية (CRI) 1.0[1] مثّل طريقة جديدة لبحث المشكلة وتم تصميمه ليثير نقاشاً دولياً وليُلهم الدول على اتخاذ إجراءات عالمية لعلاج التآكل الاقتصادي الذي تسبب به *انعدام الأمن الإلكتروني*.

تم إعداد مؤشر الجاهزية الإلكترونية 2.0 بناءً على مؤشر الجاهزية الإلكترونية 1.0، وهو يختبر مئة وخمسة وعشرين دولة من الدول التي تبنت، أو بدأت بتبني، تكنولوجيا المعلومات والاتصالات والإنترنت ومن ثم تُطبّق منهجية موضوعية لتقييم مستوى نضج كل دولة والتزامها بالأمن الإلكتروني بالنسبة لسبعة عناصر أساسية. من خلال تطبيق هذه المنهجية، تستطيع الدولة فهم المشاكل التي تعاني منها البنية التحتية للإنترنت لديها بالإضافة إلى التبعيات ونقاط الضعف الناتجة عنها.[2] على وجه التحديد، يُقيّم مؤشر الجاهزية الإلكترونية 2.0 مستويات جاهزية الدول لبعض المخاطر الإلكترونية المُحددة ويُحدد المجالات التي يُمكن فيها للقادة تعديل أو تحسين الوضع الحالي لدولهم من خلال زيادة فعالية القوانين والسياسات والمعايير والعوامل الرافعة للسوق (مثل الحوافز والأنظمة) أو تغييرها للحفاظ على أمن اتصال الدول ولحماية قيمة اقتصادها.

معلومات عامة

لقد تبنت معظم الدول إستراتيجيات اقتصادية تدعم تكنولوجيا المعلومات والاتصالات وهي تعمل على توفير الاتصالات السريعة والموثوقة وميسورة التكلفة لجميع المنازل والشركات لنقل مجتمعاتها المعلوماتية إلى العصر الرقمي.[3] مبادرات التحديث مثل الحكومة الإلكترونية والصيرفة الإلكترونية والصحة الإلكترونية والتعلم الإلكتروني وشبكات الطاقة من الجيل المقبل وأتمتة عناصر البنية التحتية للنقل والخدمات الأساسية الأخرى أصبحت على قمة الأجندة الاقتصادية لمعظم الدول. فعلى سبيل المثال، تسعى إستراتيجية "Internet Plus" في الصين إلى تشجيع التطور السليم للتجارة الإلكترونية والشبكات الصناعية والصيرفة على الإنترنت بالإضافة إلى تسهيل نمو صناعات جديدة وتوسيع بصمة الإنترنت الدولية لشركاتها.[4] وكحال العديد من الدول الأخرى، تعتبر الصين الإنترنت عنصراً أساسياً لنموها المستقبلي ولفرصها التطويرية. وعلى نحو مماثل، وضع رئيس وزراء الهند مودي نظرته لتحويل دولته إلى "اقتصاد قائم على المعرفة الرقمية" من أجل استغلال كفاءة الهند في مجال تكنولوجيا المعلومات (IT) التي تحظى بشهرة عالمية من أجل خلق فرص عمل في أسواق تكنولوجيا المعلومات، والاتصالات، والأجهزة الإلكترونية. إضافة إلى ذلك، تسعى الهند إلى أن تصبح دولة مبتكرة في مجال حلول تكنولوجيا المعلومات والاتصالات (ICT) في أسواق الصحة وإدارة المعرفة والأسواق المالية.[5] أخيراً، تعمل المفوضية الأوروبية على إنشاء سوق واحد وهادف للخدمات الرقمية قادر على ضمان حرية حركة البضائع والخدمات ورؤوس الأموال والأعمال التجارية. ومن المتوقع أن يؤدي التنفيذ الناجح "لإستراتيجية السوق الرقمي الواحد" هذه إلى نمو إجمالي الناتج المحلي في أنحاء أوروبا بمقدار 415 مليار يورو في السنة.[6]

ينبغي على الدول تنظيم نظراتها الاقتصادية الوطنية لتتماشى مع أولويات أمنها الوطني.

أما الحكومات، في الدول النامية بشكل خاص، فهي تسعى لتبني سياسات أعنف في مجال تكنولوجيا المعلومات والاتصالات لتوفير خدمات إضافية للملايين من مواطنيها من أجل دفع عجلة التقدم الاقتصادي بشكل أسرع.[7] في الواقع، تشير تقديرات البنك الدولي إلى أن إجمالي الناتج المحلي ينمو بمقدار 1 إلى 2 بالمئة لكل 10% من السكان المتصلين بالإنترنت.[8] علاوة على ذلك، أشارت إحدى الأبحاث الأخيرة إلى أن الاعتراف المتنامي للحكومات والأعمال التجارية بتبني حلول الإنترنت وتكنولوجيا المعلومات والاتصالات سيحسن من تنافسيتها على المدى الطويل ومن رفاهيتها الاجتماعية

بنسبة قد تصل إلى 8 بالمئة من إجمالي الناتج المحلي للدولة.[9] كما أن بعض التقارير تذهب إلى ما هو أبعد من ذلك وتشير إلى أن تحديث الأنظمة الصناعية (مثل شبكات الطاقة الكهربائية، وأنابيب النفط والغاز، والتصنيع إلخ.) يُمثّل حصة مقدارها 46% من الاقتصاد العالمي، وقد تنمو لتصل لغاية 50% بالمئة في السنوات العشر القادمة.[10]

لا يمكن للدول أن تتجاهل هذه الفرصة الاقتصادية. ولكن بعضاً منها يدرس التكاليف الاقتصادية وأثر الخدمات الحساسة الأقل مرونة، وكشف/انتهاك خصوصية المواطن، وسرقة بيانات الشركات ذات الملكية الخاصة وأسرار الدولة، وأثر الاحتيال الإلكتروني والجريمة الإلكترونية – التي تؤدي جميعها إلى انعدام الاستقرار الاقتصادي والوطني. ببساطة، يُشكل *انعدام الأمن* الإلكتروني عبئاً ثقيلاً على كاهل النمو.[11]

فعلى سبيل المثال، تشير التقديرات إلى أن اقتصادات مجموعة العشرين (G20) قد خسرت 2.5 مليون وظيفة بسبب التزوير والقرصنة، وأن الحكومات والمستهلكين يخسرون ما يصل إلى 125 مليار دولار بسبب الجريمة الإلكترونية سنوياً، بما في ذلك الخسائر في أرباح الضرائب.[12] حسب تقديرات الولايات المتحدة يبلغ الأثر السنوي لسرقة الملكية الفكرية (IP) على الاقتصاد الأمريكي 300 مليار دولار. أي ما يُعادل 1 بالمئة من ناتجها المحلي الإجمالي.[13] وتُقدر دراسات أخرى أجرتها هولندا والمملكة المتحدة وألمانيا خسائر مماثلة في الناتج المحلي الإجمالي. لا تستطيع أي دولة تحمل خسارة حتى 1 بالمئة من ناتجها المحلي الإجمالي بسبب النشاطات الإلكترونية غير المشروعة. مع استمرار الدول في تبني تكنولوجيا المعلومات والاتصالات والاتصال بالإنترنت ستزداد

يُشكل انعدام الأمن الإلكتروني عبئاً ثقيلاً على كاهل النمو.

ينبغي على المجتمعات المرنة والمتصلة أن تقود عملية التحديث بحيث يكون الأمن في صميم هذه العملية.

نسبة تعرضها للمخاطر ذات الصلة وستزداد التكاليف الاقتصادية بشكل تصاعدي إذا لم تعتمد إستراتيجياتها الخاصة بالتحديث على الأمن والتمكين.

قياس مثل هذه الخسائر التي يتعرض لها الاقتصاد سيجبر قادة الدول على تنظيم أجندات دولهم للأمن الوطني لتتماشى مع أجنداتهم الاقتصادية والاستثمار في القيمة المشتقة لكليهما.[14] التعامل بشفافية مع الخسائر الاقتصادية الناتجة عن انعدام الأمن الإلكتروني قد يجذب الاهتمام الوطني والعالمي لمعالجة هذا التآكل الاقتصادي. يضع مؤشر الجاهزية الإلكترونية 2.0 إطار عمل لإرشاد الدول حول كيفية السعي لتحقيق النمو الاقتصادي لمجتمعاتها المرنة والمُعززة بتكنولوجيا المعلومات والاتصالات والمتصلة بالإنترنت.

مؤشر الجاهزية الإلكترونية 2.0 - المنهجية

يتكون مؤشر الجاهزية الإلكترونية 2.0 من عنصرين أساسيين: الأول، صُمم لُيطلع قادة الدول على الخطوات التي ينبغي عليهم أخذها بعين الاعتبار لحماية دولهم التي يزداد اتصالها بالإنترنت بشكل متزايد ولحماية النمو المحتمل لناتجها الإجمالي المحلي من خلال التقييم الموضوعي لمستوى نضج كل دولة والتزامها بالأمن والمرونة الإلكترونية. ثانياً، يُحدد مؤشر الجاهزية الإلكترونية معنى تمتع الدولة بـ "الجاهزية الإلكترونية" ويضع العناصر الرئيسة للجاهزية الإلكترونية على شكل خطة قابلة للتنفيذ لتتبعها الدول. تُمثل منهجية مؤشر الجاهزية الإلكترونية 2.0 أداة مفيدة وفريدة وسهلة الاستخدام لتقييم الفجوة بين الوضع الحالي للدولة بالنسبة للأمن الإلكتروني وبين

قدرات الدولة الإلكترونية اللازمة لتحقيق نظرتها الاقتصادية. يشمل المخطط الذي تم تطويره وتوظيفه لهذا التحليل أكثر من سبعين مؤشر فريد للبيانات موزعين على العناصر السبعة التالية:

1. الإستراتيجية الوطنية؛
2. التعامل مع الحوادث؛
3. الجريمة الإلكترونية وتطبيق القانون؛
4. مشاركة المعلومات؛
5. الاستثمار في البحث والتطوير (R&D)؛
6. الدبلوماسية والتجارة؛
7. الدفاع والتعامل مع الأزمات.

تعتمد التقييمات القائمة على الحقائق لكل دولة على المصادر الأولية، وكل نقطة بيانات فريدة مبنية على أبحاث ووثائق تجريبية. يتم تقييم الدول بالنسبة لكل مؤشر على ثلاثة مستويات من الجاهزية الإلكترونية هي: الأدلة غير الكافية، الجاهزية الجزئية للعمل، الجاهزية التامة للعمل.

تُستخدم منهجية مؤشر الجاهزية الإلكترونية 2.0 لتقييم الجاهزية الإلكترونية لدى مائة وخمسة وعشرين دولة؛ حيث تعمل على تقييم مستوى النضج لدى كل دولة والتزامها بالأمن الإلكتروني والبنى التحتية والخدمات المرنة (الشكل 1 والجدول 1).

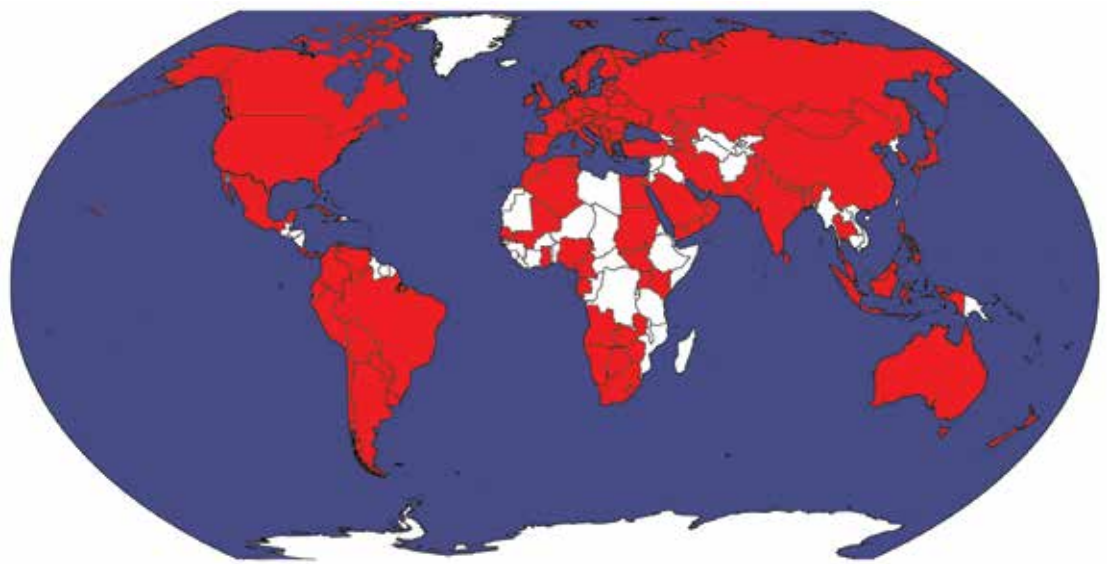
وتشمل مجموعة الدول المختارة الدول الخمس وسبعين الأولى من مؤشر تطور تكنولوجيا المعلومات والاتصالات (IDI) الخاص بالاتحاد الدولي للاتصالات (ITU) للتشديد على أهمية الربط. وتمت إضافة أعضاء اقتصادات مجموعة العشرين (G20) لأنها تمثل ما نسبته 90 بالمئة من الناتج المحلي الإجمالي العالمي، و80 بالمئة من التجارة العالمية، و64 بالمئة من عدد سكان العالم، و84 بالمئة من جميع انبعاثات الوقود الأحفوري.

ومن أجل أن يكون المؤشر ممثلاً لجميع الأقاليم وليشمل دولاً من جميع أنحاء العالم، تم اختيار دول إضافية من: منظمة التعاون الاقتصادي والتنمية (OECD)، والمجموعة الاقتصادية

الأدلة غير كافية: الأدلة غير كافية أو لم يتم إيجادها بعد. ولكن من المحتمل أن تكون البيانات موجودة ولكن غير متاحة بشكل عام أو أنها سريّة..

الجاهزية الجزئية للعمل: هناك أدلة على وجود سياسات ونشاطات و/أو تمويل، ولكن قد يكون النشاط غير ناضج، أو غير مكتمل، أو لا يزال في مراحله الأولى من التطوير. بالرغم من ملاحظة هذه المبادرات إلا أنه قد يكون من الصعب قياس أداءها الوظيفي.

الجاهزية التامة للعمل: هناك دليل كافٍ لمراقبة وقياس النشاطات الناضجة والفعّالة.[15]



الشكل 1: مجموعة دول مؤشر الجاهزية الإلكترونية 2.0

الجزائر	كولومبيا	إسرائيل	هولندا	سريلانكا
أندورا	كوستاريكا	إيطاليا	نيوزيلندا	سانت كيتس ونيفيس
أنغولا	كرواتيا	اليابان	نيجيريا	سانت فنسنت والجرينادين
أنتيغوا وبربادوس	كوبا	كازاخستان	النرويج	السودان
أرمينيا	قبرص	كينيا	عُمان	سوازيلاند
الأرجنتين	جمهورية التشيك	الجمهورية القيرغستانية	باكستان	السويد
أستراليا	الدنمارك	لاتفيا	باراغواي	سويسرا
النمسا	جيبوتي	لبنان	بنما	تايوان
أذربيجان	إكوادور	ليسوتو	بيرو	جمهورية مقدونيا
البحرين	مصر	ليتوانيا	الفلبين	تايلاند
بنغلادش	استونيا	لكسمبورغ	بولندا	ترينيداد وتوباغو
باربادوس	فنلندا	ماكاو، الصين	البرتغال	تونس
بيلاروسيا	فرنسا	ماليزيا	قطر	تركيا
بلجيكا	الجابون	المالديف	رومانيا	أوغندا
بوتان	جامبيا	مالي	روسيا	أوكرانيا
بوليفيا	ألمانيا	مالطا	السعودية	الإمارات العربية المتحدة
البوسنة والهرسك	غانا	موريشيوس	السنغال	المملكة المتحدة
بوتسوانا	اليونان	المكسيك	صربيا	الولايات المتحدة الأمريكية
البرازيل	هونج كونج	مولدوفا	سيشل	أوروغواي
بروناي دار السلام	هنجاريا	منغوليا	سنغافورة	أوزبكستان
بلغاريا	أيسلندا	موناكو	سلوفاكيا	فنزويلا
الكاميرون	الهند	مونتينيغرو	سلوفينيا	فيتنام
كندا	إندونيسيا	المغرب	جنوب أفريقيا	اليمن
تشيلي	إيران	ناميبيا	كوريا الجنوبية	زامبيا
الصين	ايرلندا	نيبال	إسبانيا	زمبابوي

الجدول 1: مجموعة دول مؤشر الجاهزية الإلكترونية 2.0

الأفريقية (AEC)، ومنظمة التكامل الاقتصادي لدول أمريكا اللاتينية (LAIA)، والتعاون الاقتصادي لدول آسيا والمحيط الهادي (APEC)، والتعاون الاقتصادي الإقليمي لآسيا الوسطى (CAREC)، ومجلس التعاون الخليجي (GCC)، واتحاد جنوب آسيا للتعاون الإقليمي (SAARC) والاتحاد التجاري لدول أمريكا الشمالية. الدول من هذه المجموعات الاقتصادية الإقليمية مُمثلة في مؤشر التطور (IDI)، كما أنها مشمولة في العادة في مؤشر جاهزية الشبكات الخاص بالمنتدى الاقتصادي العالمي (WEF). ويضمن هذا تبني كل دولة من الدول المختارة تكنولوجيا المعلومات والاتصالات واستثمارها في خدمات الإنترنت المُتاحة وذات التكلفة الميسورة لتعزيز النمو الاقتصادي.

بما أن مجلس دول التعاون الخليجي لا يمثل الشرق الأوسط، تمت أيضاً إضافة الدول الثلاث التي تتمتع بأعلى تصنيفات للناتج الإجمالي المحلي خارج دول مجلس التعاون الخليجي وهي: إيران، اليمن ولبنان.[16]

هذا المقطع العرضي المكون من مئة وخمسة وعشرين دولة يُمثل جزءاً كبيراً من العالم ويوضح الطبيعة المتنوعة والممثلة لمعايير اختيار دول مؤشر الجاهزية الإلكترونية 2.0.

يوفر تركيز مؤشر الجاهزية الإلكترونية 2.0 على الترابط بين علم الاقتصاد والأمن (أو انعدامه) قاعدة متينة لكل دولة لتقييم مستوى نضجها فيما يتعلق بالأمن الإلكتروني، ويخدم كإطار عمل لوضع السياسات والإستراتيجيات والمبادرات التشغيلية والمؤسساتية، ومتطلبات الموارد، وصياغة الأنظمة والتشريعات، والتنفيذ المتنوع للعناصر الرافعة السوق. سيؤدي تطبيق مؤشر الجاهزية الإلكترونية 2.0 إلى رفع مستوى الوعي حول الرابط بين الفضاء الإلكتروني المُستدام وبين نمو إجمالي الناتج المحلي لكل دولة بما أنه من الأرجح أن يزداد اعتماد مستقبل إجمالي الناتج المحلي للدول على التكنولوجيا والإنترنت. علاوة على ذلك، فهو يخلق أساس لفهم التآكل الاقتصادي الذي يتسبب به انعدام الأمن الإلكتروني ومستوى اعتبار المخاوف الأمنية الوطنية من عناصر الأجندة الاقتصادية والرقمية للدولة. بإمكان هذه المنهجية أن تؤدي إلى قرارات قائمة على التحاليل حول كيفية الاستجابة للمشاكل واستباق حدوثها.

أخيراً، يقدم مؤشر الجاهزية الإلكترونية 2.0 للمؤسسات العالمية، مثل الاتحاد الدولي للاتصالات (ITU)، والمنتدى الاقتصادي العالمي (WEF)، ومنظمة الدول الأمريكية (OAS)، وبنك التنمية للدول الأمريكية (IDB)، والبنك الدولي وغيرها من المنظمات، إطار عمل ومنهج مجاني لمبادراتها ونقاشاتها الدولية.

فيما يلي وصف مُفصّل للعناصر الأساسية السبعة لمنهجية مؤشر الجاهزية الإلكترونية 2.0. يحتوي كل قسم على أحد العناصر الأساسية مع عشرة مؤشرات داعمة على الأقل للتقييم، بحيث تمثل عند دمجها معاً مخطط الدولة للجاهزية الإلكترونية. علاوة على ذلك، تم ذكر أمثلة لبعض الدول لتوضيح الحلول المبتكرة ومتعددة الثقافات لتحقيق الجاهزية الإلكترونية. بالرغم من أن هذه الأمثلة ليست شاملة بأي شكل من الأشكال إلا أنها تسلط الضوء على المنهجيات الفريدة على مستوى الدول.

1. الإستراتيجية الوطنية

المجال الأول – والأهم – الذي يدل على الجاهزية الإلكترونية للدولة هو صياغة ونشر إستراتيجية وطنية للأمن الإلكتروني تنظم النظرة الاقتصادية للدولة بشكل يتماشى مع ضروريات أمنها الوطني. الإنترنت، وشبكات النطاق العريض، وتطبيقات الهواتف الخلوية، وخدمات تكنولوجيا المعلومات، والمعدات الحاسوبية تشكل أساسات

الاقتصاد الرقمي والمستقبل الرقمي للدولة.[17] لقد أصبح الإنترنت وتكنولوجيا المعلومات والاتصالات العمود الفقري للمنصات العائلية (مثل فيسبوك™ وتويتر™، إنستغرام™، رينن™، في كونتاكت™، إلخ.)، محركات الأعمال، الخدمات والبنى التحتية ذات الأهمية الحساسة، والاقتصاد العالمي.[18] للاعتماد المتبادل والاتصال المفرط أثر على كل قطاع من هذه القطاعات. فعلى سبيل المثال، يستخدم التصنيع المتقدم أنظمة الضبط الصناعية والروبوتات لزيادة الإنتاجية وتقليل الحاجة للتدخل اليدوي. وتركب الزراعة الحديثة أدوات بروتوكول الإنترنت (IP) على المحاصيل لتحديد متطلبات الأسمدة ولتعديل كمية مياه الري. كما يتم تركيب أدوات بروتوكول الإنترنت (IP) على الماشية لتحديد الأماكن التي ترعى فيها والتي تستهلك المياه فيها ولتقييم صحة الحيوانات على نحو شبه ثابت. أصبحت التجارة الإلكترونية، والتدفق الحر للبضائع والخدمات عبر الحدود، تحل محل المتاجر التقليدية، وتقدم تشكيلة واسعة من المنتجات وتوصلها مباشرة إلى منازل المتسوقين عبر الإنترنت بعد وضعهم لطلباتهم عبر الإنترنت. وأصبحت أنظمة النقل الآن تستخدم المستشعرات والأدوات المتنقلة والأكشاك الإلكترونية لإدارة حركة المرور ولتقديم التذاكر. وتستخدم الدول المتصلة بالإنترنت أدوات تحديد المواقع الجغرافية لتتبع سرعة وموقع المركبات لمعرفة فيما إن كان السائق يمتثل لقوانين القيادة. وتعمل مبادرات التحديث في مجال الرعاية الصحية على رقمنة السجلات الصحية للمواطنين واستخدام الحوسبة السحابية لتمكين الوصول السريع لسجلات الرعاية الصحية في أي مكان في العالم. ويستخدم الطب عن بعد اتصال الإنترنت عالي السرعة لتقديم النصائح والخدمات الطبية للمناطق المحرومة. أخيراً، تتبادل الأسواق المالية ترليونات الدولارات يومياً، وتتداول أسواق السلع باستعمال العملة الرقمية، وأدت صيرفة الإنترنت إلى الاستغناء عن المصارف المحلية الفعلية.

التهديدات التي تواجه البنى التحتية المتصلة بالشبكات آخذة بالازدياد. ولقد بدأت الدول بفهم هذه التهديدات وبإدراك الحاجة لحماية البنى التحتية، وحماية البيانات، والدفاع عن أراضيها، وغيرها من العناصر الوصفية. ينبغي على الإستراتيجية الشاملة للأمن الإلكتروني الوطني أن تصف التهديدات التي تواجه الدولة من الناحية الاقتصادية وأن توضح الخطوات والبرامج والمبادرات اللازمة التي ينبغي تبنيها لمعالجة تلك التهديدات وحماية الاتصال بالإنترنت ووسائل تكنولوجيا المعلومات والاتصالات التي يستخدمها المواطنون والمنظمات الخاصة والعامة.[19] وينبغي أن ترتكز الإستراتيجية على قدرة الاقتصاد على تبني الإنترنت وتكنولوجيا المعلومات والاتصالات وينبغي أن تشتمل على مبادرات تساعد على خفض تآكل إجمالي ناتج المحلي الذي تتسبب به التهديدات الإلكترونية، بالإضافة إلى زيادة أمن الدولة ومرونتها بشكل عام.

ينبغي أن تعكس الإستراتيجيات الوطنية للأمن الإلكتروني الأهمية الاقتصادية للأمن الإلكتروني.

إن صياغة الإستراتيجية السليمة للأمن الإلكتروني الوطني غير كافية بحد ذاتها. بل ينبغي أن تكون الإستراتيجية قابلة للتنفيذ. في يومنا هذا، تشمل الموضوعات الرئيسة التي تتكون منها معظم الإستراتيجيات: التخطيط لإنشاء سلطة تنظيمية وموضعية داخل الحكومة؛ تعزيز الوعي والتعليم بين المواطنين؛ بناء القدرات للاستجابة للحوادث والأزمات ولإدارتها؛ توسيع صلاحية سلطات تطبيق القانون للتعامل مع الجرائم الإلكترونية؛ تسهيل الشراكات بين القطاعين العام والخاص؛ وتطوير نقاط موثوقة لتبادل المعلومات؛ وتوجيه الموارد نحو أجندة قائمة على الأبحاث والتطوير (R&D) والابتكار. تبدأ العديد من الإستراتيجيات بالإحصاءات، وبالتحديد الكمي لحجم الحادثة ومعدل إصابة البنية

التحتية وبتسمية الأنواع المختلفة من التهديدات. وتستخدم البيانات لتبرير المسؤولية التنظيمية والتمويل الإضافي للمهام والمنظمات. نادراً ما تمنح هذه الإستراتيجيات الأولوية للخدمات والبنى التحتية الأكثر عرضة للخطر، ولا تتماشى كذلك مع الإجراءات الأمنية ومع متطلبات الموارد اللازمة لخفض مستوى التعرض للخطر ولخفض الخسائر الاقتصادية. ينبغي على الإستراتيجية السليمة للأمن الإلكتروني أن تذكر المشكلة أو المشاكل الإستراتيجية من الناحية الاقتصادية؛ وأن تحدد وتُمكن السلطة المعنية [20] المسؤولة عن تنفيذ الإستراتيجية؛ وأن تشمل أهدافاً مُحددة وقابلة للقياس وقابلة للتحقيق وقائمة على النتائج وقائمة على الوقت ضمن خطة للتنفيذ؛ وأن تعترف بالحاجة للالتزام بموارد محدودة (مثل الإرادة السياسية، والمال، والوقت والناس) في بيئة تنافسية لتحقيق النتائج الأمنية والاقتصادية اللازمة.

لقد قامت سبعة وستون دولة على الأقل بنشر إستراتيجية أمنها الإلكتروني (بينما لا تزال دول أخرى في طور أعدادها)، وتوضح هذه الإستراتيجيات الخطوات الرئيسة التي تهدف لرفع مستوى أمنها الوطني ومرونتها[21]. لدى العديد من الدول الأخرى إستراتيجيات وطنية (غير خاصة بالأمن الإلكتروني فحسب) تهدف لتوجيه وتنسيق جهودها لتحسين وضع الأمن الإلكتروني لديها. ولكن، دولاً قليلة فقط، تربط بشكل صريح بين أجنداتها الاقتصادية والأمنية الوطنية وبين الاعتراف بالأهمية الاقتصادية للأمن الإلكتروني. أما الدول التي تبني إستراتيجيات قابلة للتنفيذ فعددها أقل من ذلك. بالتالي، لدى جميع الدول فرصة مراجعة أو تطوير إستراتيجياتها لتعكس الأهمية الاقتصادية للأمن الإلكتروني.

ينبغي أن تشمل عناصر الإستراتيجية الوطنية الشاملة للأمن الإلكتروني ما يلي:

البيان:

أ. نشر إستراتيجية وطنية للأمن الإلكتروني تشمل الفرص الاقتصادية والمخاطر المرتبطة بتبني تكنولوجيا المعلومات والاتصالات (ICT)؛

التنظيم:

أ. تعيين سلطة مختصة وتحديد سلطتها الموضعية بشكل واضح؛

ب. تحديد الجهات الحكومية الرئيسة التي تتأثر بالإستراتيجية الوطنية للأمن الإلكتروني و/أو المسؤولة عن تنفيذها؛

ج. تحديد جهات القطاع التجاري التي تتأثر بالإستراتيجية الوطنية للأمن الإلكتروني و/أو المسؤولة عن تنفيذها (الاعتراف بتبعيات القطاع التجاري):

الموارد:

أ. تحديد الموارد المالية والبشرية المطلوبة والمُخصصة لتنفيذ الإستراتيجية.

ب. تحديد نسبة إجمالي الناتج المحلي المتوقع كسبها أو خسارتها (بشكل إجمالي) عند تنفيذ الإستراتيجية؛

التنفيذ:

أ. تحديد الآليات المطلوبة لتأمين البنية التحتية الإلكترونية المهمة وتبني تكنولوجيا المعلومات والاتصالات (ICT)؛

ب. تحديد الخدمات ذات الأهمية الحساسة (وليس البنى التحتية ذات الأهمية الحساسة) التي تنوي الإستراتيجية زيادة مستوى أمنها ومرونتها؛ و

ج. تحديد المعايير الوطنية لاستمرارية اتفاقيات الخدمة (24 ساعة/7 أيام في الأسبوع) ومتطلبات الإبلاغ عن الانقطاعات لكل خدمة وصناعة وبنية تحتية ذات أهمية حساسة.

تمثل نتائج هذا العنصر الأساسي، كما في المجالات الستة الأخرى، لقطة زمنية لمشهد ديناميكي ودائم التغير. فبينما تقوم الدول بتطوير إستراتيجياتها للأمن الإلكتروني، ستعكس التحديثات على هذا العنصر الأساسي تلك التغيرات وستعمل على مراقبة وتتبع وتقييم التطورات الجوهرية والبارزة. بالتالي، سيستمر مؤشر الجاهزية الإلكترونية 2.0 في تقديم خطة مع أمثلة جديدة ليتطلع عليها الآخرون عند صياغة إستراتيجياتهم أو مراجعتها.

2. التعامل مع الحوادث

يشتمل العنصر الأساسي الثاني الذي يشير إلى الجاهزية الإلكترونية للدولة على تأسيس والحفاظ على قوة وطنية فعالة للاستجابة للحوادث. في الغالب، تكون هذه القوة على شكل فريق واحد أو أكثر من الفرق الوطنية للاستجابة لحوادث أمن الحواسيب (National CSIRTs) أو فرق الاستجابة لطوارئ الحاسوب (CERTs) – وسيُشار إلي كليهما فيما يلي بمصطلح CSIRTs – مسؤولة عن إدارة التعامل مع الحوادث في حال تعرض الخدمات الحساسة والبنى التحتية للمعلومات لكوارث إلكترونية طبيعية أو من صنع الإنسان.[22] في الوقت الحاضر، تم تأسيس مئة واثنين فريق CSIRTs في جميع أنحاء العالم ويجري حالياً تطوير أربعة فرق CSIRTs.[23]

تضم فرق CSIRTs في العادة مزيجاً من خبراء وممارسي أمن تكنولوجيا المعلومات من السلك الأكاديمي والقطاع الخاص والحكومة. بالإضافة إلى تقديم الكفاءة التقنية الخاصة للاستجابة للحوادث الإلكترونية ذات الأهمية الوطنية، تعمل فرق التعامل مع الحوادث هذه على تقوية قدرات الحكومة الوطنية على فهم ومحاربة التهديدات الإلكترونية. بالتالي، فإن تشغيل فريق CSIRT وطني يشكل العنصر الجوهري للإستراتيجية الشاملة للدولة لتأمين وللحفاظ على الخدمات والبنى التحتية الحيوية بالنسبة للأمن الوطني والنمو الاقتصادي.[24]

وتخدم فرق CSIRT، على عكس الفرق الحكومية البحتة، فئة واسعة تتراوح من الدوائر الحكومية إلى المؤسسات الخاصة والعامة والمواطنين. وتوفر فرق CSIRT الوطنية المُعدة بشكل جيّد خدمات تفاعلية أكثر من غيرها من الفرق – أي القدرة على التعامل مع الحوادث من خلال احتواء الحوادث والتخفيف منها فور وبالرغم من أن الشكل التنظيمي المُحدد الخاص بفرق CSIRT واحتياجات الدول ومواردها قد تختلف من دولة لأخرى، إلا أن هذه الوحدات المُتخصصة والخاصة ينبغي أن توفر مجموعة من الوظائف الاستباقية والتفاعلية على حد سواء، بالإضافة إلى الخدمات الوقائية والتعليمية وخدمات إدارة جودة الأمن. وتشمل هذه الخدمات، دون الحصر: تأسيس فهم مشترك للتهديدات التي تواجه الدولة؛ نشر التنبيهات والتحذيرات حول نقاط الضعف والتهديدات الإلكترونية، وتعزيز الوعي حول الأمن الإلكتروني والممارسات المُثلى؛ وتحديد، والكشف عن، واحتواء، وإدارة التهديدات الأمنية والتحضير للحوادث المحتملة؛ وتنسيق نشاطات التعامل مع الحوادث؛ وتحليل حوادث الأمن الحاسوبية وتقديم التغذية الراجعة والدروس المستفادة (للتعلم المشترك)؛ والترويج للنشاطات التي تزيد من المرونة؛ ودعم الإستراتيجية الوطنية للأمن الإلكتروني.

على سبيل المثال، تم تطوير فريق CSIRT الوطني في سنغافورة (SingCERT) بواسطة Infocomm Development Authority of Singapore (IDA) بالتعاون مع جامعة سنغافورة الوطنية (NUS) في عام 1997. وأصبح الفريق منذ ذلك الوقت جزءاً من وكالة الأمن الإلكتروني السنغافورية (CSA). تم تصميم فريق SingCERT كمركز شامل للاستجابة للحوادث؛ ولتسهيل الكشف عن الحوادث، وحل المشاكل، وتجنب الحوادث الأمنية على الإنترنت. ويوفر فريق SingCERT المساعدة التقنية وينسق التعامل مع الحوادث الأمنية الإلكترونية ويحدد ويتتبع توجهات التطفل الإلكترونية، وينسق مع الوكالات الأمنية الأخرى من أجل حل الحوادث الأمنية الحاسوبية.[26] كما نشط فريق SingCERT أيضاً في مجال تنظيم واستضافة تمارين اتحاد دول جنوب شرق آسيا (ASEAN) وفريق الاستجابة لطوارئ الحاسوب في آسيا والمحيط الهادئ (APCERT). إضافة إلى ذلك، تستضيف سنغافورة سبعة من أعضاء منتدى فرق التعامل مع الحوادث والأمن (FIRST).

تتألف قدرات البرازيل للاستجابة للحوادث من فريق وطني للاستجابة لطوارئ الحاسوب، CERT.BR، ومن ثلاثين فريق CSIRT إقليمي موزعة على أربع ولايات وتخضع جميعها لسلطة اللجنة البرازيلية التوجيهية للإنترنت. وهذه اللجنة هي لجنة غير حكومية ومتعددة المساهمين وهي الجهة الرئيسة المسؤولة عن الدفاع عن الشبكات وعن التعامل مع الحوادث في البرازيل.[27] ففريق *CERT.BR* مسؤول عن التعامل مع الحوادث، وزيادة الوعي، وجمع البيانات حول التهديدات وعمليات التطفل الإلكترونية، والتنسيق مع العديد من أصحاب العلاقة من فرق CSIRT وأعضاء السلك الأكاديمي والقطاع الخاص. علاوة على ذلك، تشمل فرق CSIRT البرازيلية فرقاً من القطاع المالي، والجيش، والحكومة، والجامعات.[28]

إلى جانب فرق CSIRT الوطنية، تم تأسيس جهات إقليمية مماثلة لتحسين وتنسيق نشاطات التعامل مع الحوادث ضمن بعض الأقاليم الجغرافية المُحددة. على سبيل المثل، فريق AfricaCERT، هو منظمة غير ربحية تشمل إحدى عشر دولة أفريقية وتقدم منتدى للتعاون ولتبادل المعلومات التقنية بين مشغلي الشبكات المتصلة بالإنترنت في المنطقة. وتشمل الأهداف الرئيسة لفريق AfricaCERT، دون الحصر: تنسيق التعاون بين فرق CSIRT الأفريقية للتعامل مع الحوادث الأمنية الحاسوبية؛ والمساعدة في تأسيس فرق CSIRT في الدول التي تفتقر حالياً لقدرات التعامل مع الحوادث؛ رعاية ودعم برامج التوعية والتعليمية للوقاية من الحوادث في مجال أمن تكنولوجيا المعلومات والاتصالات (ICT)؛ وتشجيع مشاركة المعلومات؛ وتشجيع الممارسات المثلى للأمن الإلكتروني. وعلى نحو مشابه، يتكون فريق APCERT من شبكة من ثمانية وعشرين فريق CERT عضو وخبراء أمنيين موثوقين آخرين في المنطقة، وتهدف لتحسين مستوى الوعي والكفاءة فيما يتعلق بحوادث أمن الحاسوب وتحسين قدرات التعامل مع الحوادث في مختلف أنحاء منطقة آسيا والمحيط الهادئ.[29] مهمة فريق APCERT هي السعي لضمان "نظافة وأمن وموثوقية" الفضاء

مرونة الخدمات ذات الأهمية الحساسة هي من العناصر الحيوية والمهمة للأمن الوطني والنمو الاقتصادي.

الإلكتروني من خلال التعاون الدولي. من أجل الإبلاغ بشكل فعّال عن التهديدات الإلكترونية، يعتمد إطار العمل التنظيمي لفريق APCERT على نظام نقطة الاتصال (POC)، الذي تقوم فيه كل دولة بانتداب أحد أعضاء فريق APCERT ليكون نقطة الاتصال (POC) خلال أوقات الطوارئ للمساعدة في تسهيل الاستجابة في الأوقات المناسبة.[30] وعلى نحو مشابه، فإن فريق الاستجابة لطوارئ الحاسوب الخاص بمنظمة التعاون الإسلامي (OIC-CERT) – والذي يشمل دولاً أعضاء من جنوب شرق آسيا، وجنوب آسيا، والشرق الأوسط، وأفريقيا، وآسيا الوسطى – يعمل أيضاً لتحسين التعاون بين فرق CERT الخاصة بالدول الأعضاء وبين فريق OIC-CERT.

بالإضافة إلى تطوير قدرات التعامل مع الحوادث، تشارك الدول أيضاً في تدريبات التعامل مع الحوادث الإلكترونية. وتساعد هذه التدريبات الدول على ممارسة وتطوير مهاراتها في الإدارة الفعّالة للأزمات وللتحقق من القدرة التشغيلية لفرق CSIRT على الاستجابة تحت الضغط. على سبيل المثال، في شهر نوفمبر 2011، أجرى الفرع التنفيذي الألماني تدريباً ليوم واحد في مجال التخطيط/ الجاهزية للأزمات. وكان الهدف من التدريب تطوير إجراءات الحكومة للاستجابة لهجوم متعدد المحاور شمل: هجمات رفض الخدمة الموزعة (DDoS) على منشآت حساسة؛ وحقن البرامج الخبيثة في نظام الصيرفة مما تسبب بأزمة في أجهزة الصرف الآلي (ATM) والبطاقات الائتمانية؛ وإدخال حركات كاذبة في نظام مراقبة الحركة الجوية.[31] الوكالة السويدية المدنية للطوارئ (MSB)، وسلطة البريد والاتصالات الهاتفية (PTS)، ومؤسسة إذاعة الدفاع الوطني (FRA) تستضيف أيضاً دورات تعاونية منتظمة بعنوان "كبير ضباط أمن المعلومات (CIAO)" للموظفين ذوي الصلة الذين يعملون في مستويات إدارية عليا. وتبلغ الدورة ذروتها بأحد التمارين المُتقدمة – محاكاة إدارة الأزمات الإلكترونية – التي تشمل أصحاب مصلحة عامين وخاصين في عملية اتخاذ القرارات، لتشمل البرلمان والمدراء التنفيذيين (CEO) لشركات مسؤولة عن الخدمات ذات الأهمية الحساسة في السويد. ويسلط التمرين الضوء على مواضع القصور القانونية والسياسية الحاسمة، ويُثقف في الوقت نفسه المشاركين حول الأمن الإلكتروني. [32] إضافة إلى ذلك، أجرت جمهورية التشيك تمريناً للاستجابة للحوادث في شهر أكتوبر 2015 ركُز على التهديدات التي تواجه البنى التحتية ذات الأهمية الحساسة مع التركيز بشكل خاص على محطات الطاقة النووية.[33] كما تجري بعض الدول أيضاً تمارينا استجابة لحوادث إلكترونية حدثت بالفعل. على سبيل المثال، أمرت رئيسة كوريا الجنوبية بارك غيون هي بإجراء تمارين وتدريبات على الحرب الإلكترونية لجميع الموظفين نتيجة للكشف عن برامج خبيثة في عدة محطات لشركة كوريا للطاقة المائية والنووية (KHNP).[34]

علاوة على ذلك، تختبر التدريبات الدولية القدرات التشغيلية للاستجابة للحوادث وتنشط في الوقت نفسه التعاون بين الدول. فعلى سبيل المثال، تجري الولايات المتحدة، مرتين في العام تدريباً على عاصفة إلكترونية تسعى من خلاله إلى تقوية الجاهزية الإلكترونية في القطاعين العام والخاص. ويبني كل تمرين من تمارين العاصفة الإلكترونية على الدروس المستفادة من حوادث سابقة حدثت بالفعل لضمان تمتع المشاركين بالفرصة للتدرب على التعامل مع الحوادث الإلكترونية الأكثر تعقيداً. سيضم تمرين العاصفة الإلكترونية للعام 2016 ستة عشر ولاية، وإحدى عشر دولة، وأربعة عشر وكالة فدرالية.[35] كما يعقد الاتحاد الأوروبي أيضاً تمارين للاستجابة للحوادث الإلكترونية مرتين سنوياً بين الدول الأعضاء والقطاع الخاص تحت اسم Cyber Europe.[36] خلال أحد التمارين الإلكترونية التي استمرت لمدة 24 ساعة في عام 2014، سمح Cyber Europe لجميع الدول الأعضاء في الاتحاد الأوروبي تقريباً بتجربة قدراتها على الاستجابة لما يصل إلى ألفي هجمة إلكترونية حقيقية شملت هجمات DDoS، وهجمات تشويه مواقع الإنترنت، وتهريب البيانات، وهجمات إلكترونية ضد البنى التحتية ذات الأهمية الحساسة.[37] علاوة على ذلك، تجري وكالة الدفاع الأوروبية (EDA) ومنظمة معاهدة أمريكا الشمالية (NATO)

تمارين مُعقدّة على صعيد الإقليم في مجال إدارة الأزمات الإلكترونية بهدف تقوية القدرات على التعامل مع الحوادث الإلكترونية بين الدول الأعضاء وفهم التبعيات العابرة للحدود.[38] أعلنت الولايات المتحدة والمملكة المتحدة مؤخراً بأنها ستختبر طريقة استجابة المراكز المالية على طرفي المحيط الأطلسي لهجوم إلكتروني ضخم. وجرى التمرين في شهر نوفمبر من عام 2015 واختبر استجابة الدول والتنسيق والاتصالات عبر المحيط الأطلسي.[39]

بالإمكان أيضاً استعمال فرق CSIRT كآلية لبناء الثقة بين الدول ولتعزيز التعاون فيما بينها. فعلى سبيل المثال، قامت دول الصين واليابان وكوريا – التي كانت تعاني من توترات فيما بينها على مر التاريخ – بعقد اجتماع سنوي ثلاثي الأطراف حول فرق CSIRT لمناقشة آليات التعامل مع الحوادث الإلكترونية. وساعدت الاجتماعات على زرع الثقة والاستئمان ونتج عن ذلك إنشاء "خط ساخن" إلكتروني للإبلاغ عن الحوادث الإلكترونية المهمة.[40]

قدرات التعامل مع الحوادث الإلكترونية، والاجتماعات المشتركة، والتمارين هي مجرد أمثلة قليلة على الآليات الأساسية التي يمكنها المساعدة في تحضير الدول بشكل استباقي والتخفيف من تداعيات أي حادثة إلكترونية كبرى. ففرق CSIRT تزيد من سرعة الدولة ومن تعافيها ومرونتها في وجه التهديدات الإلكترونية، الأمر الذي يُرجح أن يقلل من الأثر الاقتصادي والتشغيلي العام للهجمات أو الحملات ذات الأهمية الوطنية. من بين الشروط المسبقة الرئيسة للنشر الناجح لفرق التعامل مع الحوادث هذه الموظفين المُدربين بشكل جيّد، والأدوات الفعّالة والقابلة للنشر بشكل سريع. فهذه العوامل تسهل من قدرة فريق التعامل مع الحوادث على تعزيز التعاون والتنسيق في تجنب الحوادث، وتمكن من الاستجابة السريعة للحوادث، وتعزز مشاركة المعلومات بين أصحاب المصلحة على الصعيدين المحلي والدولي على حد سواء.

وينبغي أن تشمل عناصر القدرات الوطنية السليمة للاستجابة للحوادث:

البيان:

أ. نشر خطة استجابة للحوادث للحالات الطارئة والأزمات؛

ب. تحديد وتخطيط التبعيات بين القطاعات التي تهدف لاستمرارية العمليات وآليات التعافي من الكوارث؛

ج. الدليل على التدرب على الخطة وتحديثها بشكل منتظم؛

د. نشر وتوزيع تقييم (تقييمات) للتهديدات الإلكترونية الوطنية في الحكومة، والبنى التحتية ذات الأهمية الحساسة؛ وخدمات الشبكات الأساسية؛

التنظيم:

أ. تأسيس فريق CSIRT وطني لإدارة التعامل مع الحوادث وخدمة فئة واسعة من الدولة (غير الحكومة والجهات المزودة للبنى التحتية ذات الأهمية الحساسة)؛

ب. تحديد شبكة من نقاط الاتصال الوطنية الرسمية للجهات الحكومية والتنظيمية؛

ج. تحديد شبكة من نقاط الاتصال الوطنية الرسمية للمجالات الأساسية لتشغيل وتعافي الخدمات والبنى التحتية ذات الأهمية الحساسة؛

د. تطوير نظام معلوماتي للتحذير والتنبيه يُمكن للمراكز الوطنية للأزمات/الاستجابة استعماله لتلقي ومعالجة ونقل المعلومات العاجلة بشكل فعّال وسريع؛

الموارد:

أ. تحديد الموارد المالية والبشرية اللازمة والمُخصصة لفريق CSIRT الوطني لتنفيذ المهام المُوكلة إليه؛

ب. تحديد تمويل إضافي لتفعيل واختبار نظام المعلومات للتحذير والتنبيه بشكل منتظم، ولقياس مستوى استعداد ومرونة الدولة للتعامل مع الحوادث والأزمات الإلكترونية من خلال التمارين الوطنية للأمن الإلكتروني؛

التنفيذ:

أ. الكفاءة المُثبتة في احتواء الحوادث وإدارتها والمرونة وعمليات التعافي للخدمات والبنى التحتية ذات الأهمية الحساسة؛

ب. القدرة المُثبتة للمراكز الوطنية للأزمات/للاستجابة على معالجة التنبيهات ونقلها في الوقت المناسب؛

ج. الدليل على طرق البحث المستمرة التي تُحلل التوجهات أو مجموعات حوادث الحاسوب الأمنية ذات الأهمية الوطنية – لها نفس المنفذين أو التكتيكات، والتقنيات والإجراءات – من أجل تحديد الأنماط؛

د. تطوير وتنفيذ نظام/برنامج لاختبار وقياس مرونة الدولة بشكل منتظم تجاه الحوادث والأزمات الإلكترونية من خلال التمارين الوطنية للأمن الإلكتروني.

تعتمد النتائج الأولية في هذا العنصر الأساسي على مخزونات فرق CSIRT الوطنية التي يوفرها قسم CERT في جامعة كارنجي ميلون (CMU)،[41] والوكالة الأوروبية لأمن المعلومات والشبكات (ENISA) [42] ومنتدى فرق التعامل مع الحوادث والأمن (FIRST)،[43] والاتحاد الدولي للاتصالات (ITU). وتتم استشارة مصادر أولية وثانوية إضافية، مثل المواقع الإلكترونية لفرق CSIRT الوطنية ومقالات الأخبار ذات الصلة للتأكد من وجود الكفاءات وتمويلها. مع بدء الدول في إدراك أهمية تأسيس فرق CSIRT وطنية، ستقوم التحديثات لهذا العنصر الأساسي بمراقبة وتتبع وتقييم تلك التطورات.

3. الجريمة الإلكترونية وتطبيق القانون

العنصر الأساسي الثالث الذي يدل على الجاهزية الإلكترونية للدولة يتضح من خلال التزامها بحماية مجتمعها من الجريمة الإلكترونية. الجريمة الإلكترونية ليست مجرد مسألة محلية؛ فهي تتجاوز الحدود الوطنية وبالتالي تتطلب حلولاً عالمية. ينبغي على الدول أن تبدي التزاما دولياً لتأمين المجتمع من الجريمة الإلكترونية. في الغالب، تكون هذه الكفاءة على شكل المشاركة مع المنتديات الدولية المعنية بمعالجة مسائل الجريمة الإلكترونية الدولية بالإضافة إلى تأسيس آليات قانونية وتنظيمية محلية لمحاربة الجريمة الإلكترونية. ينبغي على السلطات القانونية والتنظيمية المعنية التي توكل إليها مهمة إجراء هذه النشاطات تحديد النشاطات التي تعتبر من الجرائم الإلكترونية وتمكين الجهات الحكومية وتزويدها بالآليات والخبراء والموارد للتحقيق ولملاحقة نشاطات الجريمة الإلكترونية بشكل فعّال.

الاتفاقان الدوليان اللذان يساعدان في إثبات التزام الدولة بحماية المجتمع من الجريمة الإلكترونية هما: "اتفاقية الجريمة الإلكترونية" الخاصة بالمجلس الأوروبي، و"اتفاقية التعاون في مجال ضمان أمن المعلومات العالمي" الخاصة بمنظمة شانغهاي للتعاون. بدأ تطبيق "اتفاقية الجريمة الإلكترونية" الخاصة بالمجلس الأوروبي منذ 1 يوليو 2004، وعادة ما يُشار إليها باتفاقية بودابست،

وهي توفر آلية يمكن من خلالها التنسيق بين القوانين الوطنية المتشعبة للجرائم الإلكترونية وتشجيع التعاون في مجال تطبيق القانون. [44] ولكن فعالية اتفاقية بودابست محدودة إلى حد ما لأنها تسمح للدول المُوقعة عليها بتنفيذ عناصر مُحددة تختارها الدول من بين عناصر اتفاقية بودابست إذا أشارت نتائج الأبحاث إلى أن القيام بغير ذلك "يمس بسيادتها، أو بأمنها، أو النظام العام فيها أو مصالح أساسية أخرى."[45] أما "اتفاقية التعاون في مجال ضمان أمن المعلومات العالمي" الخاصة بمنظمة شانغهاي للتعاون والتي وُقعّت في عام 2009 والتي يُشار إليها أحياناً باتفاقية يكاترينبورغ، فهي تضم مبادئ تتماشى مع منهج تطبيق القانون الذي تنص عليه اتفاقية بودابست. فهي الأخرى تسعى لتحسين القاعدة المعلوماتية القانونية ولوضع آليات عملية للتعاون بين الأطراف لضمان أمن المعلومات الدولي.[46] بموجب هذه الاتفاقيات، توافق الدول على تبني تشريعات مناسبة، وعلى تعزيز التعاون الدولي، ومحاربة الجرائم الجنائية من خلال تسهيل الكشف عنها والتحقيق والملاحقة القانونية على الصعيدين المحلي والدولي. مؤشر الجاهزية الإلكترونية 2.0 يكافئ ويمنح درجات أعلى للدول التي صادقت أو انضمت إلى أي من هاتين الاتفاقيتين لأن الدول التي تقوم بذلك تصبح مُلزمة بموجب قانونها المحلي بالحفاظ على التزامها على صعيد دولي.

بالإضافة إلى الآليات الدولية المذكورة أعلاه، هناك مناهج أخرى دولية ومتعددة الجنسيات وإقليمية تسعى لمعالجة الجرائم الإلكترونية الدولية. على سبيل المثال، مررت الجمعية العامة للأمم المتحدة (UNGA) مجموعة متنوعة من القرارات المتعلقة بالجرائم الإلكترونية، مثل قرار 2001 حول "محاربة سوء الاستخدام الإجرامي لتكنولوجيا المعلومات"، وقرار 2003 حول "إنشاء ثقافة عالمية للأمن الإلكتروني وحماية البنى التحتية ذات الأهمية الحساسة."[47] ومن الجدير بالذكر أن مجموعة الأمم المتحدة لخبراء الحكومات (GGE) التي تضم عشرين دولة حققت اختراقاً هاماً عندما اتفقت على التعاون على ملاحقة الإرهابيين والاستخدام الإجرامي لتكنولوجيا المعلومات والاتصالات (ICT). وتم تدوين التزامات هذه الدول في تقرير يونيو 2015 لمجموعة الأمم المتحدة لخبراء الحكومات (GGE) *حول التطورات في مجال المعلومات والاتصالات الهاتفية على صعيد الأمن الدولي*.[48] وأجرى منتدى التعاون الاقتصادي لدول آسيا والمحيط الهادي (APEC) كذلك مشروعاً لبناء القدرات حول الجريمة الإلكترونية لاقتصادات الدول الأعضاء من أجل تأسيس أطر قانونية ولبناء القدرات للتحقيق في الجرائم الإلكترونية. وكجزء من هذا المشروع، دعمت الاقتصادات المتقدمة في منتدى التعاون الاقتصادي لدول آسيا والمحيط الهادي (APEC) اقتصادات الدول الأعضاء الأخرى من خلال تدريب السلطات التشريعية وموظفي التحقيق.[49]

يستند مؤشر الجاهزية الإلكترونية 2.0 إلى هذه المنهجيات الدولية ومتعددة الجنسيات والإقليمية لتقييم الجاهزية الإلكترونية للدولة. إضافة إلى ذلك، يشمل مؤشر الجاهزية الإلكترونية 2.0 أيضاً معلومات حول الدول فيما يتعلق بالجريمة الإلكترونية من اتحاد دول جنوب شرق آسيا (ASEAN) والاتحاد الدولي للاتصالات (ITU) ومن جهات أخرى

بالرغم من وجود النية للتعاون في مجال الجرائم الإلكترونية وبالرغم من أهمية المصادقة على اتفاقيات الجرائم الإلكترونية، إلا أن ذلك لا يدل بالضرورة على الجاهزية لمحاربة الجريمة الإلكترونية. فينبغي على الدول العمل على بناء قدرات محلية لتطبيق القانون الإلكتروني وبشكل استباقي. على سبيل المثال، يعمل المركز المتقدم للأبحاث، والتطوير والتدريب في القانون والأدلة الجنائية الإلكترونية في كلية القانون الوطنية في جامعة الهند في بنغالور على ترجمة القانون إلى مصطلحات تقنية والعكس من خلال تقديم التدريب والتعليم للضباط القضائيين والمدعين العامين ووكالات التحقيق وموظفي الأمن الإلكتروني وأخصائيي التكنولوجيا وغيرهم. يحظى المركز بتمويل من دائرة الإلكترونيات وتكنولوجيا المعلومات (DeitY) في

وزارة الاتصالات وتكنولوجيا المعلومات الهندية، وهو يقدم عناصر تدريبية عملية فريدة من نوعها في مختبر الأدلة الجنائية الإلكترونية لتسهيل الفهم السريع للمسائل المُعقدة. [50]

من الأمثلة الأخرى على ذلك إطلاق منظمة الشرطة الدولية (INTERPOL) مؤخراً لمجمع الإنتربول العالمي للابتكار (IGCI) في سنغافورة. تُمكن هذه المنشأة مسؤولي تطبيق القانون من الانضمام إلى خبراء المجال لتطوير تقنيات تدريبية جديدة واستعمال الأدوات المتقدمة لمجابهة الجريمة الإلكترونية ولتعزيز الأمن الإلكتروني.[51] على سبيل المثال، أنشأت الإنتربول لعبة محاكاة لتعليم مسؤولي تطبيق القانون حول تقاطع وخطورة شبكة Darknet والعملات التشفيرية. لقد خلقت شبكة Darknet اقتصاداً خفياً (غير قانوني) لبيع المعلومات الشخصية القابلة للتعريف (PII)، والمعلومات الاستخبارية العسكرية، وتصاميم الأسلحة، والبرامج الخبيثة النموذجية، وهجمات zero-day، ومفاتيح وشهادات التشفير الخاصة، والعديد من الأنواع الأخرى من البيانات التي يتم الحصول عليها بشكل غير قانوني. وتم إجراء تمرين المحاكاة/التدريب الأول للإنتربول في يوليو 2015.[52]

إلى جانب بناء القدرات في مجال الجريمة الإلكترونية وتطبيق القانون، ينبغي على الدول العمل أيضاً على تنظيف الإصابات في بناها التحتية المتصلة بالشبكات، والتي تعرف باسم botnets.[53] في الوقت الحالي، تُقدّر نسبة الحواسيب المصابة بشبكات botnets من خمسة إلى اثني عشر بالمائة من الحواسيب حول العالم. ويُقدر مكتب التحقيقات الفدرالي (FBI) إصابة ثمانية عشرة نظاماً في الثانية من خلال جيوش botnet مما يتسبب بأضرار تقدر قيمتها بـ 110 مليار دولار أمريكي حول العالم. [45] لقد عملت بعض الدول على مواجهة هذه التهديد وحققت بعض النجاح. على سبيل

خفض عدد الأدوات المصابة المتصلة بالشبكة هو استثمار هام في مجال محاربة الجريمة الإلكترونية.

تُشكّل الجريمة الإلكترونية والاحتيال عبئاً كبيراً على النمو الاقتصادي.

المثال، قام مشروعا DarkSpace Project-Advanced وDark Space Analysis for Predictive Analytics - Indicators of Cyber Activity التابعان للحكومة الكندية بقيادة Bell Canada وبمشاركة فريق من الخبراء من الوكالات الحكومية الكندية والمؤسسات الأكاديمية وخبراء المجال – بتقديم دراسة جدوى لحل "الأنابيب النظيفة" لمجابهة التهديدات الإلكترونية من خلال توفير مجموعة من الأدلة المُقنعة لدعم احتواء التهديدات التي تواجه كندا من الإنترنت بشكل استباقي. وأدت نتائج المشروع إلى إنشاء إستراتيجية وطنية للأنابيب النظيفة وكان لها أثر كبير في "معيار الأمن الإلكتروني لمزودي خدمات الاتصالات الهاتفية".[55] ومن الأمثلة الأخرى، مركز "The Cyber Clean Center"في اليابان، وهو جهد ممول استمر لمدة خمس سنوات قام بتشغيله فريق CERT الياباني (JPCERT) من 2006 إلى 2011.[56] كان هذا المركز ثمرة التعاون متعدد التخصصات بين فريق JP-CERT، ووكالات أمنية متنوعة، وشركات تزويد خدمة الإنترنت (ISPs)؛ وقام بإنشاء "شبكة حماية" مؤتمتة ضد الإصابة بعدوات برامج botnet الخبيثة والتعرض للاستغلال منها. كما وفر أيضاً حلولاً مُعدة حسب الطلب لمعالجة بعض البرامج الخبيثة المُحددة على بعض الحواسيب.[57] ولقد استمرت جهود مركز "The Cyber Clean Center" في Telecom-ISAC Japan.[58] أخيراً، تهدف iCode الأسترالية، وهي شراكة عامة-خاصة من خلال المبادرة الأسترالية لأمن الإنترنت (AISI)، للترويج لثقافة أمنية بين مزودي خدمة الإنترنت (ISPs) من خلال خفض عدد الأدوات الحاسبة العرضة للخطر في أستراليا. وتشجع iCode جميع مزودي خدمات الإنترنت الأستراليين على الانضمام إلى المبادرة الأسترالية لأمن الإنترنت (AISI)،

وتزويد مزودي خدمات الإنترنت الأعضاء في المبادرة ببيانات يومية حول الإصابات بالبرامج الخبيثة وحول قابلية إصابة الخدمة بهذه البرامج. [59]

تُشكّل الجريمة الإلكترونية والاحتيال عبئاً كبيراً على النمو الاقتصادي. لقد وصلت قيمة أضرار الجريمة الإلكترونية حول العالم إلى ما يُقدر بـ 445 مليار دولار أمريكي، وأحدثت أثراً سلبياً في الاقتصادات الوطنية بنسبة لا تقل عن 1 بالمئة من إجمالي الناتج المحلي وفقدان ما يصل إلى مئتي ألف وظيفة.[60] الاستثمار في محاربة الجريمة الإلكترونية ورفع قدرات تطبيق القانون هو استثمار ضروري للاقتصاد. من خلال تطوير قدرات تطبيق القانون لمحاربة الجريمة الإلكترونية من خلال المصادقة على وثائق الاتفاقيات، والتعاون الدولي، وتطوير القدرات، وتشغيل البرامج المضادة لشبكة botnet بالإضافة إلى مبادرات أخرى، تستطيع الدول التخفيف من مخاطرها الإلكترونية ودفع عجلة نموها الاقتصادي المستقبلي إلى الأمام.

ينبغي أن تشمل العناصر الأساسية للالتزام السليم على المستويين المحلي والعالمي بحماية المجتمع من الجريمة الإلكترونية ما يلي:

البيان:

أ. التزام وطني ودولي مُثبت لحماية المجتمع من الجريمة الإلكترونية من خلال المصادقة على الاتفاقيات الدولية حول الجرائم الإلكترونية أو الاتفاقيات المماثلة الأخرى لمحاربة الجرائم الإلكترونية؛

ب. الالتزام المُثبت لتأسيس آليات قانونية وسياسية محلية خصيصاً من أجل خفض مستوى النشاط الإجرامي المنبثق من الدولة وتعزيز آليات التنسيق لمعالجة الجريمة الإلكترونية على الصعيدين المحلي والعالمي؛

التنظيم:

أ. تأسيس قدرات مؤسساتية ناضجة لمحاربة الجرائم الإلكترونية، بما في ذلك التدريب لقضاة المحاكم، والمدعين العامين، والمحامين، ومسؤولي تطبيق القانون، وأخصائيي الأدلة الجنائية والمحققين الآخرين؛

ب. تأسيس وكالة للتنسيق تكون مهمتها وسلطتها الأولية ضمان تلبية جميع المتطلبات الدولية للجرائم الإلكترونية على الصعيد المحلي وعلى صعيد السلطات القضائية المختلفة (أي التعاون بين الدول)؛

الموارد:

أ. تحديد الموارد المالية والبشرية المطلوبة والمُخصصة لمحاربة الجريمة الإلكترونية؛

ب. تأسيس آلية محاسبة لتحديد النسبة السنوية من إجمالي الناتج المحلي التي تتأثر بالجريمة الإلكترونية (الخسارة الفعلية بالعملة الحقيقية)، من أجل تقييم العلاقة التبادلية بين التكلفة والفائدة على نحو وطني ومُنظم وتخصيص الموارد وفقاً لذلك؛

التنفيذ:

أ. الدليل المُثبت لالتزام الدولة بمراجعة وتحديث القوانين الحالية وآليات الحوكمة التنظيمية، وتحديد مواقع الفجوات والمواقع التي يمكن للسلطات المتراكبة البقاء فيها، وتوضيح ومنح الأولوية للمجالات التي تحتاج للتحديث (مثل القوانين الحالية، مثل قانون الاتصالات القديم)؛

ب. تأسيس جرائم جنائية بموجب القانون المحلي للأعمال الموجهة ضد سرية وسلامة وتوافر أنظمة الحاسوب والشبكات وبيانات الحاسوب بالإضافة إلى سوء استخدام مثل هذه الأنظمة والشبكات والبيانات لتشمل الانتهاك الدولي لحقوق الطبع والنشر؛ و

ج. الدليل المُثبت لفعالية الدولة في خفض عدد الإصابات المنبثقة من بناها التحتية ومن شبكاتها (مثل إنشاء مبادرات لمحاربة شبكات botnet ولمعالجة البرامج الخبيثة).

تعتمد النتائج الأولية في هذا العنصر الأساسي على مراجعة للكشف عن ما إذا قامت الدولة بالمصادقة على أو الانضمام إلى اتفاقية بودابست أو اتفاقية يكاترينبورغ الخاصة بمنظمة شانغهاي للتعاون وإن كانت الدولة مشاركة بشكل فعّال في الجهود الإقليمية أو متعددة الجنسيات أو الدولية لمعالجة الجرائم الإلكترونية. إضافة إلى ذلك، يُستخدم النشاط الحالي لشبكات botnet (كل من عقد الأوامر والتحكم والعدد الكلي للإصابات) المنبثقة من الدولة لتقييم فعالية مبادراتها لمحاربة شبكات botnet. يستند مؤشر الجاهزية الإلكترونية 2.0 إلى موارد أولية وثانوية ليُحدد فيما إن كانت الدولة قد وضعت آليات قانونية وتنظيمية ونشاطات أخرى لخفض المخاطر وخصصت التمويل لضمان التنفيذ الناجح. وستراقب التحديثات التي تطرأ على هذا العنصر الأساسي وستتبع وستقيم التطورات الجوهرية والبارزة.

4. مشاركة المعلومات

العنصر الرابع الذي يدل على الجاهزية الإلكترونية للدولة هو قدرتها على وضع والحفاظ على آليات لمشاركة المعلومات يمكن من خلالها تبادل المعلومات الاستخبارية القابلة للتنفيذ و/أو المعلومات بين الحكومات وقطاعات الصناعة. النشاطات الرئيسة مثل التحديد والتقييم والاستجابة للهجمات المستهدفة – التي قد يكون لها تداعيات كبيرة على الاتصالات والتجارة والأعمال العالمية – تتطلب أكثر من مجرد آليات تقليدية للمراقبة والحماية. على الصعيد العالمي، قامت معظم الحكومات والمنظمات بوضع برامج لمشاركة المعلومات لتحسين فهم المخاطر التي تفرضها الجهات الحكومية وغير الحكومية وحسّنت من مستوى تعرضها للهجمات وما يصاحبها من إصابات وخروقات.

الآليات الرسمية لمشاركة المعلومات، الشبيهة ببعض الخدمات التي تقدمها فرق CSIRT و CERT الوطنية، يمكن أن تساعد في تعزيز التنسيق في مجال التعامل مع الحوادث، وأن تسهل المشاركة الفورية للمعلومات الاستخبارية والتهديدات وأن تساعد على تحسين فهم كيفية استهداف القطاعات، والمعلومات المفقودة، والطرق التي يمكن استخدامها للدفاع عن الأصول المعلوماتية. لقد برزت أربعة نماذج مختلفة على الأقل لمشاركة المعلومات لمجابهة التهديدات الإلكترونية ولمساعدة المؤسسات على تأمين أصولها المعلوماتية وهي: (1) النموذج القائم على الحكومة؛ (2) النموذج القائم على القطاع (3) النموذج القائم على الشراكة غير الربحية (4) النموذج القائم على الشراكة الهجينة بين القطاع الأكاديمي والحكومة والقطاعات. ولكل طريقة تحدياتها الفريدة والخاصة مثل الموازنة بين الحاجة لتبادل معلومات الأمن الإلكترونية القابلة للتنفيذ في الوقت المناسب وحماية سرية البيانات في الوقت نفسه، وحماية الحريات المدنية، وإدارة الموارد والمصالح المالية والبشرية المتنافسة. ولكن هناك عاملان ضروريان لنجاح أي من النماذج الأربعة وهما: المساهمة والثقة، واللذان ينبغي أن يستندان إلى أهداف وأدوار ومسؤوليات

ينبغي أن ترتكز مشاركة المعلومات على الثقة وعلى المساهمة من طرف أصحاب المصلحة كافة.

ونتائج مُحددة بشكل واضح. إذا أردنا التعبير عن ذلك بشكل أبسط يمكننا القول أنه عندما يشارك أحد الأطراف بشكل متردد أو دفاعي، فإنه من الصعب تحقيق النجاح. [61]

علاوة على ذلك، ينبغي أن يكون أصحاب المصلحة قادرين على مشاركة المعلومات القيّمة حول الحوادث الخطرة، الأمر الذي يتطلب وضع تعريفات واضحة حول نوع المعلومات التي تنبغي مشاركتها والأشخاص الذين سيسمح لهم بالوصول إليها والإجراءات الأمنية التي ينبغي اتخاذها لحماية المعلومات بعد نشرها بواسطة مالكها الأصلي. مستوى التعقيد لهذا التبادل للمعلومات الحسّاسة ينمو بشكل متناسب مع حجم المجموعة، وربما بشكل تصاعدي عندما يكون أعضاء تلك المجموعات دول سيادية لها مخاوفها الأمنية الوطنية الخاصة

لقد قامت العديد من الدول الفردية بتطوير برامج وطنية قوية لمشاركة المعلومات بالإمكان اعتبارها بمثابة ممارسات مثلى يمكن للدول الأخرى التعلم منها. وتركّز هذه البرامج على توزيع أصحاب المصلحة المتشابهين على مجموعات ومن ثم توزيع المجموعات على برنامج وطني. على سبيل المثال، قامت هولندا بإنشاء المركز الوطني للأمن الإلكتروني (NCSC) – وهو عبارة عن مبادرة بقيادة الحكومة تطورت من فريق GOVCERT الهولندي لتصبح شراكة ناجحة بين القطاعين العام والخاص – وهو مسؤول عن الأمن الرقمي وعن مشاركة المعلومات في الدولة.[62] إحدى المهام الرئيسة للمركز هي المراقبة المستمرة لجميع المصادر التي يحتمل بأن تكون مشبوهة على الإنترنت وتنبيه السلطات والمنظمات العامة حول أي تهديد إلكتروني يتم التعرف عليّه. كما أن المركز الوطني للأمن الإلكتروني (NCSC) مرتبط بشكل مباشر بجميع مراكز مشاركة وتحليل المعلومات (ISAC) في الدولة وتتم مشاركة المعلومات تحت بروتوكول Traffic Light Protocol (TLP) الذي يُصنّف المعلومات إلى أربعة مستويات: أحمر، أصفر، أخضر وأبيض. لقد تم تصميم البرنامج الهولندي لمشاركة المعلومات استناداً إلى مركز المملكة المتحدة الوطني لتنسيق أمن البنى التحتية (NISCC)، الذي يُقدم نصائح أمنية معلوماتية إلى الشركات التجارية المعنية بإدارة البنى التحتية الوطنية ذات الأهمية الحساسة. [63] وعلى نحو مشابه، فإن الوكالة اليابانية لتشجيع تكنولوجيا المعلومات (IPA) تتصرف بمثابة السلطة المؤسساتية المسؤولة عن مشاركة المعلومات بين الحكومة والقطاعات ذات الأهمية الحساسة، وهي تتمتع بسجل مُثبت من العلاقات الموثوقة مع جميع الشركات الكبرى في الدولة وبتوفير المعلومات الاستخبارية الفعالة وفي الوقت المناسب. إضافة إلى ذلك، تعمل وكالة تشجيع تكنولوجيا المعلومات (IPA) بشكل لصيق مع وزارة الاقتصاد والتجارة والصناعة (METI)، والمركز الوطني لأمن المعلومات (NISC)، والفريق الاستشاري للإنقاذ الإلكتروني (J-CRAT) من أجل الاستجابة لجميع الحوادث الإلكترونية الكبيرة التي تصيب البنى التحتية ذات الأهمية الحساسة.[64]

من جهة أخرى، وفي الولايات المتحدة، يساعد مركز مشاركة وتحليل معلومات الخدمات المالية (FS-ISAC) – وهو مبادرة قائمة على القطاعات تم تطويرها بواسطة قطاع الخدمات المالية – على تسهيل الكشف عن الحوادث الإلكترونية ونشاطات الاحتيال والوقاية منها والاستجابة لها. ولقد بنى المركز علاقات قوية مع مزودي الخدمات المالية؛ ومع شركات الأمن التجاري؛ والوكالات الفدرالية/الوطنية، ووكالات الدولة، ووكالات الحكومة المحلية؛ ومؤسسات تطبيق القانون؛ وغيرها من الجهات الموثوقة الأخرى لتقديم تحذيرات موثوقة ودقيقة حول التهديدات الإلكترونية ومعلومات حساسة أخرى للشركات الأعضاء حول العالم. وكجزء من هذه الجهود، يستخدم مركز مشاركة وتحليل معلومات الخدمات المالية (FS-ISAC) بروتوكولات مختلفة من نوع Traffic Light Protocol من أجل تحديد الجماهير التي يمكنها وينبغي عليها تلقي المعلومات المُحددة.[65] ويتوسع مركز مشاركة وتحليل معلومات الخدمات المالية (FS-ISAC) بمشاركة معلومات التهديدات على الصعيد الدولي حيث يقدم خدماته إلى المملكة المتحدة وأوروبا. كما توجد مراكز ISAC أخرى في قطاعات عديدة، ولكنها لا تتمتع بنفس الفعالية.

الاتحاد الوطني للأدلة الجنائية والتدريب الإلكتروني (NCFTA) في الولايات المتحدة هو مؤسسة غير ربحية تهدف إلى تسهيل التعاون بين القطاعات الصناعية والأكاديمية وسلطات تطبيق القانون لتحديد التهديدات المُعقدة المتعلقة بالفضاء الإلكتروني والتخفيف منها وإبطالها. تضم هذه المبادرة غير الربحية القائمة على الشراكة ممثلين من الولايات وسلطات تطبيق القانون والصناعة، وإضافة إلى ذلك فهي تتمتع بممثلين دوليين من كندا، وأستراليا، والمملكة المتحدة، والهند، وألمانيا، وهولندا، وأوكرانيا، وليتوانيا. يعمل اتحاد NCFTA على تبادل المعلومات الاستخبارية حول التهديدات الإلكترونية بشكل مُبسّط وفي الوقت المناسب مع المؤسسات الأخرى، كما ينخرط في شراكات مع خبراء متخصصين في القطاعين العام والخاص وسلطات تطبيق القانون والقطاع الأكاديمي من أجل التخفيف من المخاطر والنشاطات الاحتيالية وجمع الأدلة اللازمة لملاحقة المجرمين قضائياً.[66]

المعلومات القابلة للتنفيذ والمباشرة بالوقت الحقيقي هي من العناصر الرئيسة للتخفيف من حدة التهديدات الإلكترونية.

أخيراً، المركز النرويجي للأمن الإلكتروني والمعلومات (CCIS) في كلية جامعة جيوفيك هو مبادرة مشتركة (بين القطاعات الأكاديمية والحكومية والصناعية) ويُمثل منهجاً آخراً لمشاركة المعلومات والتعاون بخصوص الأمن الإلكتروني. يُروّج مركز CCIS لمنهج نظامي على صعيد كامل الدولة فيما يتعلق بالأمن الإلكتروني والمعلوماتي ويقدم الخطط لحماية قدرة المجتمع على الكشف عن الحوادث الإلكترونية الخطرة والتحذير منها والتعامل معها. علاوة على ذلك، يدعم المركز الأبحاث الوطنية عالية الجودة وتطوير الحلول في مجال الأمن المعلوماتي والإلكتروني.

بالإضافة إلى البرامج المختلفة لمشاركة المعلومات التي تعمل الدول على تطويرها، فإن معظم وكالات الحكومات للدفاع والاستخبارات تجمع معلومات قيّمة متعلقة بالفضاء الإلكتروني، ولقد بدأت بعضها بالكشف عن هذا النوع من المعلومات الاستخبارية وبمشاركته مع الجهات الحكومية الأخرى ومع الصناعات ذات الأهمية الحساسة. وبالفعل، يُعد الوعي الظرفي بالوقت الحقيقي في الغالب من العناصر الرئيسة لتجنب التهديدات الإلكترونية أو للتخفيف منها. قامت بعض الدول، مثل البرازيل، بإعداد آليات لإلغاء سرية (بنظام الكتابة مقابل النشر) المعلومات القابلة للتنفيذ التي تُحذر الجهات الأخرى (العامة والخاصة) من نقاط الضعف، والتهديدات والتكتيكات المُحددة، والحلول الدفاعية المُحتملة كجزء من مبادراتها لمشاركة المعلومات.[67] يُعد تحسين الوضعية الدفاعية للدولة من الأمور الأساسية، وبعض الدول مُستعدة لإزالة صفة السرّية عن أجزاء من المعلومات الاستخبارية لضمان الأمن بشكل أفضل.

إن قدرة الدولة على مبادلة المعلومات الدقيقة والقابلة للتنفيذ في الوقت المناسب – ضمن وبين مؤسسات القطاعين العام والخاص – تُساعد في التقليل من نقاط الضعف والتعرض للخطر ويُمكنها بالتالي خفض المخاطر المرافقة لها. بما أن مشاركة المعلومات تزيد من التواتر والجودة، ينبغي على المؤسسات أن تكون قادرة على نشر تنبيهات التهديدات الإلكترونية إلى بناها التحتية المتصلة بالشبكات بشكل أسرع وأكثر استباقية. تأسيس برامج مشاركة المعلومات القابلة للتنفيذ والحفاظ عليها هو استثمار أساسي وهام للنمو الاقتصادي.

ينبغي أن تشمل عناصر البرنامج الوطني الفعّال لمشاركة المعلومات القابلة للتنفيذ والذي يغطي مختلف القطاعات:

البيان:

أ. صياغة ونشر سياسة حول مشاركة المعلومات بين مختلف القطاعات تُمكّن من تبادل الاستخبارات/المعلومات بين الحكومات وقطاعات الصناعة؛

التنظيم:

أ. تعيين كيان مؤسسي لنقل المعلومات الرسمية من المصادر الحكومية إلى الوكالات الحكومية والصناعات ذات الأهمية الحساسة (من الحكومة إلى الحكومة)؛

ب. تعيين كيان مؤسسي يضمن وجود آليات (خطط للتبليغ، تكنولوجيا، إلخ) لتبادل معلومات الحوادث بين القطاعات (بشكل ثنائي الاتجاهات)، بنوعيها التشغيلي (القريب من الوقت الحقيقي) والأدلة الجنائية (ما بعد الحادثة) (من الحكومة إلى الصناعة/من الصناعة إلى الصناعة)؛

ج. وضع آلية أكاديمية أو آلية غير ربحية لتبادل المعلومات حول نقاط الضعف أو الحوادث أو الحلول (النموذج البديل، مثل NCFTA أو قاعدة البيانات الوطنية لنقاط الضعف)؛[68]

الموارد:

أ. تحديد الموارد المالية والبشرية اللازمة والمُخصصة لتبادل المعلومات الرسمية الحكومية أو كيان/كيانات مؤسسية أخرى متخصصة في آليات تبادل المعلومات؛

التنفيذ:

أ. الدليل المُثبت على أن آليات التنسيق بين القطاعات وبين أصحاب المصلحة التي تهدف لمعالجة الاعتمادات المتبادلة الحساسة – بما في ذلك الوعي الظرفي حول الحوادث وإدارة الحوادث بين أصحاب المصلحة – يتم الحفاظ عليها بشكل مناسب ويتم اختبارها لضمان فعالية أداءها؛ و

ب. الدليل المُثبت على قدرة الحكومة وعلى عملياتها المناسبة زمنياً لإلغاء سريّة (بنظام الكتابة مقابل النشر) المعلومات الاستخبارية الإلكترونية القابلة للاستعمال ومشاركتها مع بقية الجهات الحكومية والصناعات ذات الأهمية الحساسة.[69]

تعتمد النتائج الأولية في هذا العنصر الأساسي على مراجعة لتقييم فيما إن كانت الدولة قد وضعت آليات لمشاركة المعلومات أو آليات أخرى للتنسيق. بالاعتماد على الموارد الأولية والثانوية، يحدد مؤشر الجاهزية الإلكترونية 2.0 وجود مثل هذه الآليات وتمويلها بشكل مناسب من عدمه. وتعمل تحديثات هذا العنصر الأساسي على مراقبة وتتبع وتقييم التطورات الجوهرية والبارزة.

5. الاستثمار في البحث والتطوير

العنصر الخامس الذي يدل على الجاهزية الإلكترونية للدولة هو وضع أولوية وطنية والاستثمار في الأبحاث الأساسية والتطبيقية في مجال الأمن الإلكتروني ومبادرات تكنولوجيا المعلومات والاتصالات على نطاق واسع. لقد أحدثت التطورات في مجال تكنولوجيا المعلومات والاتصالات ثورة في جميع قطاعات الاقتصاد تقريباً، وحولت الأعمال التجارية، والحكومات، والتعليم، وطريقة عيش وعمل ولعب المواطنين. تقود هذه المبادرات النمو الاقتصادي وبإمكانها تحسين المرونة وتحسين الوضع الأمني وتقويته.

لكل من الحكومة والأعمال التجارية دور لتلعبه وبإمكانهما دمج قوة ميزانياتهما للبحث والتطوير لتحسين الجيل القادم من تكنولوجيا المعلومات والاتصالات والتقنيات والحلول المدعومة بالإنترنت. الأعمال التجارية والحكومات آخذة بتبني الإنترنت المتنقل، والحوسبة السحابية، والبيانات الضخمة، والحوسبة الكمية، وإنترنت الأشياء (IoT) وينبغي عليها الاستثمار في ثقة، وأمن، ومرونة هذه الخدمات والتقنيات الرقمية. من خلال الاستثمار في البحث والتطوير الإلكتروني والابتكارات الأخرى، تستطيع الدول والجامعات والشركات تحسين قدرتها على سد الفجوة بين انعدام أمنها الإلكتروني وبين قدرات المهاجمين. على سبيل المثال،

خصص برنامج Horizon 2020 التابع للاتحاد الأوروبي مبلغاً يُقدّر بـ 80 مليار يورو لمبادرات البحث والتطوير التكنولوجي. ومع المبدأ التأسيسي للاتحاد الأوروبي القائم على الوصول المفتوح، يهدف البرنامج لتعزيز نتائج البحث، وتسريع الابتكار، وخلق فعالية أكبر، وتحسين الشفافية. يتكون برنامج Horizon 2020 من ثلاثة عناصر رئيسة. المجال الأول هو "العلوم الممتازة"، وهو يُركز على العلوم الأساسية والتطبيقية ويخطط لتمويل تدريب درجة الدكتوراه لخمسة وعشرين ألف مُرشح إضافي لشهادة الدكتوراه خلال السنوات السبع القادمة. ويُركز المجال الثاني على "القيادة في مجال التمكين والتقنيات الصناعية،" مع التركيز على تكنولوجيا المعلومات والاتصالات، وتكنولوجيا النانو، والمواد المُتقدمة، والمعالجة، وغيرها من المجالات. ويموّل المجال الثالث الحلول لمعالجة المشاكل الاجتماعية والاقتصادية مثل الصحة والطاقة والنقل والأمن. ومن معايير التقييم لهذا الاستثمار التعاون الانتقالي بين الشركات والحلول التي تلبي احتياجات عموم أوروبا. [70]

ينبغي على ابتكار البحث والتطوير في مجال الأمن الإلكتروني أن يُحسّن من ثقة، وأمن، ومرونة مجتمعنا المستقبلي المُتصل بالشبكات.

وعلى نحو مشابه، تمنح الولايات المتحدة الأمريكية الأولوية، وتنسق، وتُخصص أكثر من 4 مليارات دولار سنوياً للأبحاث المتشعبة من خلال برنامج بحث وتطوير الشبكات وتكنولوجيا المعلومات (NITRD). تشمل مجالات الأبحاث الحاصلة على الأولوية للأعوام 2016-2020: البيانات الضخمة، الأنظمة المادية-الإلكترونية، البحث والتطوير في مجال الأمن الإلكتروني والخصوصية، الحوسبة المُتقدمة، والمشاركة عبر الطيف اللاسلكي.[71] برنامج بحث وتطوير الشبكات وتكنولوجيا المعلومات (NITRD) هو المصدر الأول للولايات المتحدة للأعمال الممولة فدرالياً في مجال تقنيات المعلومات المتقدمة في قطاعات الحوسبة والشبكات والبرمجيات. يسعى البرنامج لتسريع التطوير ونشر تقنيات المعلومات المتقدمة من أجل تحسين الدفاع الوطني والأمن الداخلي بالإضافة إلى تحسين إنتاجية الولايات المتحدة وتنافسيتها الاقتصادية. إضافة إلى ذلك، فإن وكالة مشاريع الدفاع المتقدمة (DARPA)، ونشاط مشاريع الأبحاث الاستخبارية المتقدمة (IARPA)، ووكالة مشاريع الأبحاث المتطورة للأمن الداخلي (HSARPA) لديها تمويل مُخصص للبحث والتطوير الإلكتروني. ولكن، في حال دمج كامل ميزانية البحث والتطوير الإلكتروني معاً، فإن المجموع الإجمالي سيبقى دون نسبة 1 بالمئة من إجمالي الناتج المحلي للولايات المتحدة. بالاعتماد على ضخامة المخاطر الإلكترونية الحالية والمستقبلية في الولايات المتحدة، فإن نسبة 1 بالمئة من إجمالي الناتج المحلي غير مناسبة لسد فجوة انعدام الأمن الإلكتروني.

تشجع المبادرات الأخرى التي تحظى برعاية حكومية على الابتكار في مجال الأمن الإلكتروني من خلال تقديم حوافز سوقية مثل الإعفاءات الضريبية للبحث والتطوير. على سبيل المثال، قامت إسرائيل مؤخراً بالموافقة على إعفاءات ضريبية كبيرة لشركات الدفاع الإلكتروني التي تنضم وتؤسس نشاطات لها في منتزه بئر السبع الإلكتروني إدراكاً منها بأن تشجيع استثمار المنظمات والشركات يتطلب في الغالب تشجيعاً والتزاماً من طرف الحكومة.[72] من خلال تشجيع هذا النظام البيئي الفريد بين القطاعات الصناعية والأكاديمية والجيش من خلال مشاركة المواقع للمواهب التقنية، أنشأت إسرائيل مركزاً للأمن الإلكتروني الاقتصادي والإستراتيجي. كما أن منتزه بئر السبع الإلكتروني يزيد من الشراكات بين القطاعين الخاص والعام في المجال الإلكتروني؛ ويخدم كمركز للتميز في مجال الإبداع؛ ويوفر التدريب الفعّال ومساراً للتوظيف.

المِنَح النقدية والدراسية هي من الآليات السوقية الأخرى المُستعملة لتطوير التعلم في مجال الأمن الإلكتروني، ولتطوير المعرفة، ولبناء المهارات. على سبيل المثال، يُقدّم برنامج "علوم بدون حدود" للحكومة البرازيلية المِنح الدراسية في جميع مجالات العلوم والتكنولوجيا والهندسة والرياضيات (STEM)، بما في ذلك علوم الحاسوب وتكنولوجيا المعلومات. وعلى نحو مشابه، فإن المجلس الوطني للتطوير العلمي والتكنولوجي (CNPq)، وهو وكالة ضمن وزارة العلوم والتكنولوجيا والإبداع، يوفر "مِنحة دراسية للتدريب العلمي" من أجل تحفيز الطلاب الشباب على الإقبال على التعليم في مجال تكنولوجيا المعلومات والاتصالات.[73]

تعمل مراكز الإبداع الإلكتروني على تسريع تحويل الأفكار والتقنيات إلى حلول.

تدعم مراكز الإبداع في مجال الأمن الإلكتروني، مثل Hague Security Delta (HSD) البحث والتطوير الإبداعيين في مجال الأمن الإلكتروني وتعزز التعاون بين شركات القطاع الخاص، والحكومات، ومؤسسات الأبحاث. مؤسسة HSD هي مؤسسة مدعومة من قبل بلدية لاهاي ووزارة الشؤون الاقتصادية الهولندية، وهي أكبر شبكة أمنية في أوروبا تملك جسور معرفية للشبكات الأمنية الرئيسة في الولايات المتحدة، وكندا، وسنغافورة، وجنوب أفريقيا. ويشمل برنامجها للأمن الإلكتروني مبادرات مثل "أكاديمية الأمن الإلكتروني" ومختبر تجارب الحوادث الإلكترونية. وتشمل برامجه الحالية بناء منصة متقدمة للكشف عن البرامج الخبيثة وتقديم الحلول للكشف عن نقاط الضعف الإلكترونية والإبلاغ عنها والتعامل معها من خلال أجهزة المسح النوعية.[74]

وظهرت "مراكز أخرى للإبداع الإلكتروني" تابعة للقطاع الخاص في سيليكون فالي، وتل أبيب، وبوسطن، ومدينة نيويورك، ولندن. على سبيل المثال، مركز الإبداع الإلكتروني في لندن "CyLon" أو "Cyber London"، هو أول مركز في أوروبا لتسريع الأعمال الناشئة في مجال الأمن الإلكتروني. يعمل مركز CyLon على رعاية النظام البيئي للابتكار الإلكتروني في لندن ويساعد الأعمال التجارية على تطوير منتجات متعلقة بأمن المعلومات.[75]

هذه المبادرات المختلفة في مجال البحث والتطوير ومراكز الإبداع الإلكتروني تعمل على تسريع تحويل الأفكار والتقنيات إلى حلول لتطوير السوق الرقمي، ولتحسين الأمن ومرونة الشبكات والبنى التحتية التابعة لها، وتحسين رفاهية المجتمع.

ينبغي أن تشمل عناصر التزام الدولة لتطوير البحث والتطوير الإلكتروني، وجهودها لبناء القدرات ما يلي:

البيان:

أ. التزام تعلن عنه الحكومة بشكل علني للاستثمار بشكل وطني في الأبحاث الأساسية والتطبيقية في مجال الأمن الإلكتروني؛

ب. آليات تحفيز مُعلن عنها بشكل علني (مثل إعفاءات ضريبية للبحث والتطوير) لتشجيع الابتكار في مجال الأمن الإلكتروني ونشر النتائج الجديدة، والتكنولوجيا، والتقنيات، والعمليات، والأدوات القاعدية؛

ج. آليات التحفيز الحكومية المُعلنة بشكل علني (مثل، المِنح النقدية والدراسية) لتشجيع التعليم، وإبداع المعرفة، وتطوير المهارات في مجال الأمن الإلكتروني؛

التنظيم:

أ. تعيين جهة واحدة على الأقل وتوكيلها بمسؤولية الإشراف على المبادرات الوطنية للبحث والتطوير في مجال الأمن الإلكتروني وأن تكون بمثابة نقطة الاتصال الوطنية والدولية لأغراض التعاون؛

ب. تأسيس برامج دراسية بدعم من المؤسسات في مجال الأمن الإلكتروني، أو أمن المعلومات أو المجالات التقنية المتقدمة المماثلة التي تُركّز على أمن البيئة الرقمية ومرونتها؛

ج. تأسيس كيان لقياس وتحضير التقارير عن معدل البرامج الحكومية أو التجارية المتحولة بنجاح (من البحث إلى منتج/خدمة) مع التركيز على الحلول التي تحسّن أمن ومرونة البيئة الرقمية؛

الموارد:

أ. تحديد الموارد المالية والبشرية اللازمة والمُخصصة للبحوث الأساسية والتطبيقية وللمبادرات في مجال الأمن الإلكتروني؛

ب. تحديد الموارد المالية والبشرية اللازمة والمُخصصة للنقل التجاري أو الحكومي للتكنولوجيا المتقدمة والابتكار؛

التنفيذ:

أ. تنفيذ برامج مُخصصة لتطوير، ونشر وروتنة المعايير التقنية الآمنة والقابلة للتشغيل المتبادل، بحيث تكون مقبولة ومدعومة من قبل الجهات الدولية المعنية بالمعايير؛

ب. الدليل على وجود جهود حكومية وطنية لدعم، وتطوير، وتعزيز البحث والتطوير في مجال الأمن الإلكتروني، خاصة من ناحية الأدلة المثبتة بالنسبة لمعدل التحويل من البحث إلى الإنتاج (مثل النسبة المنفذة عملياً داخل الحكومة) ومعدل التبني التجاري للبرامج المتحولة بنجاح؛ و

ج. الدليل على وجود جهود تجارية (مثل مراكز الابتكار الإلكتروني) لدعم، وتطوير، وتعزيز البحث والتطوير في مجال الأمن الإلكتروني، خاصة من ناحية معدل التحويل من البحث إلى الإنتاج (مثل النسبة المنفذة عملياً داخل القطاع الخاص) ومعدل تبني الحكومة للبرامج المتحولة بنجاح من القطاع التجاري.

تعتمد النتائج الأولية في هذا العنصر الأساسي على مراجعة الدولة لمعرفة إن كانت تستثمر في مجال البحث والتطوير الإلكتروني، والتعليم، وإبداع المعرفة، وتطوير المهارات – بالإضافة إلى تمويل مبادرات الأمن الإلكتروني على نطاق أوسع. استناداً إلى الموارد الأولية والثانوية، يحدد مؤشر الجاهزية الإلكترونية 2.0 نوع آليات التحفيز الحكومية الموضوعة حالياً (إن وجدت) والموارد المُخصصة للمبادرات الشبيهة بتلك التي تمت مناقشتها أعلاه. ستعمل تحديثات هذا العنصر الأساسي على مراقبة، وتتبع، وتقييم التطورات الجوهرية والبارزة.

6. الدبلوماسية والتجارة

يتضح العنصر السادس من عناصر الجاهزية الإلكترونية من خلال مشاركة الدولة في المسائل الإلكترونية كجزء من سياستها الخارجية. من الناحية الجوهرية، تسعى الدبلوماسية الإلكترونية لإيجاد حلول مقبولة بشكل متبادل للتحديات الشائعة. تظهر المسائل الدبلوماسية في العديد من العلاقات الدولية المختلفة بما في ذلك حقوق الإنسان، والتطور الاقتصادي، والاتفاقات التجارية، وضبط الأسلحة وتكنولوجيات الاستخدام المزدوج، والأمن، والاستقرار، والسلام وحل النزاعات. بما أن المسائل الأمنية الإلكترونية تتشابك مع معظم الموضوعات تقريباً ومعظم المفاوضين خبراء في مجال مُحدد واحد فحسب (أي التجارة أو ضبط الأسلحة)، ففي الغالب لا يكون هؤلاء الخبراء على علم بالفرص أو المخاطر الإضافية التي تبرز على النطاق الإلكتروني. وبالتالي، فإن تأسيس مكتب مُخصص أو توظيف أشخاص تكون مهمتهم الرئيسة المشاركة الدبلوماسية في المسائل الإلكترونية ينبغي أن يكون أحد العناصر التكاملية للسياسة الخارجية للدولة.

نظراً للسرعة البطيئة للتعافي الاقتصادي، فإن العديد من الدول تتبع سياسات اقتصادية دولية جديدة تتخذ شكل اتفاقيات تجارية كوسيلة لتسريع النمو ولإنشاء فرص في السوق. مع ذلك، أصبحت هذه المبادرات الاقتصادية محافلاً لبحث المخاوف الأمنية الوطنية بشكل سرّي. على سبيل المثال، تم التوصل إلى اتفاقية الشراكة عبر الأطلسي (TPP) في 5 أكتوبر 2015. وكان هدف الاتفاقية تحسين التجارة والاستثمار بين الدول الشريكة في اتفاقية TPP، وتعزيز الابتكار، والنمو والتطور الاقتصادي، ودعم خلق الوظائف والحفاظ عليها. ولقد استدعى الوصول إلى هذه الاتفاقية خمس سنوات، ويعود جزء من السبب في ذلك إلى مسائل إلكترونية. فالدول الشريكة لم تستطع الاتفاق على مسائل رئيسة، بما فيها متطلبات حماية البيانات والخصوصية (مثل حماية الملكية الفكرية)، ورغبات تمركز البيانات، وقيود المواد.

تتفاوض الولايات المتحدة والاتحاد الأوروبي حول الشراكة الأطلسية للتجارة والاستثمار (TTIP)، وهي اتفاقية شبيهة باتفاقية TPP. وتسعى هذه الاتفاقية لزيادة النفاذ إلى السوق، وإلى إلغاء العوائق التنظيمية غير الضرورية، ووضع قوانين لتنظيم العلاقات التجارية المتشابكة بين الإقليمين، وخلق الوظائف، وتعزيز نمو إجمالي الناتج المحلي.[76] اثنتان من المسائل الرئيسة التي تؤخر هذه المفاوضات هي حماية البيانات والسرية. على مدى العقد الماضي، اتفقت أوروبا والولايات المتحدة على معايير حماية مشتركة لنقل

على الصعيد الجوهري، تسعى الدبلوماسية الإلكترونية إلى إيجاد حلول مقبولة بشكل متبادل للتحديات المشتركة.

وتخزين جميع البيانات الشخصية التي تنتقل و/أو تبقى بين الاتحاد الأوروبي والولايات المتحدة.[77] ولكن الوثائق التي سرّبها إدوارد سنودن فضحت نشاطات استخبارات حكومة الولايات المتحدة في جمع المعلومات حول الحكومات الأخرى والمواطنين، الأمر الذي أدى إلى انهيار الثقة بين الحكومات. ونتيجة لذلك، تطالب العديد من الدول الأوروبية وضع معايير للخصوصية، وقوانين التشفير، وأطر عمل قانونية متبادلة على مستوى الدول من أجل مواكبة التكنولوجيا سريعة التقدم ولتحميل الدول مسؤولية حماية البيانات بشكل مناسب. إضافة إلى ذلك، نقضت محكمة عدل الاتحاد الأوروبي مؤخراً اتفاقية "الملاذ الآمن" (Safe Harbor) لمعايير حماية البيانات بين الاتحاد الأوروبي والولايات المتحدة التي دامت لفترة طويلة. وسمح القرار التنفيذي لاتفاقية "الملاذ الآمن" للشركات الأمريكية بالمصادقة الذاتية من أجل توفير "الحماية المناسبة" لبيانات المستخدمين الأوروبيين تماشياً مع توجيه حماية البيانات الأوروبي ومع الحقوق الأوروبية

الأساسية، مثل حق الخصوصية. لا تزال المفاوضات جارية لتحديث اتفاقية "الملاذ الآمن"، ولكن لم يتم تقديم إطار زمني لإنجاز ذلك، الأمر الذي زاد من تعقيد مفاوضات اتفاقية TTIP.[78] الوقت الحاضر، تُقدّر غرفة التجارة الأمريكية للاتحاد الأوروبي بأن مراجعة اتفاقية "الملاذ الآمن" قد تكلف الاتحاد الأوروبي ما يصل لغاية 1.3 بالمئة من إجمالي الناتج المحلي.[79]

وتخضع حالياً للتفاوض اتفاقية إقليمية أخرى للتجارة الحرة، وهي اتفاقية الشراكة الاقتصادية الإقليمية الشاملة (RCEP) بين الدول الأعضاء في اتحاد دول جنوب شرق آسيا (ASEAN)، والصين، والهند، واليابان، وكوريا، وأستراليا، ونيوزيلندا. ويبلغ عدد سكان الدول الستة عشر المشاركة في اتفاقية RCEP نصف سكان العالم تقريباً، وهي مسؤولة عن 30 بالمئة من إجمالي الناتج المحلي للعالم، وأكثر من ربع صادرات العالم. وهدف اتفاقية RCEP هو التقليل من حواجز التجارة، وتعزيز التعاون الاقتصادي والتقني، وحماية الملكية الفكرية، وتشجيع المنافسة، وتسهيل تسوية النزاعات، وتحسين الوصول إلى الأسواق لمُصدّري البضائع والخدمات. وكجزء من هذه المفاوضات، تسعى بعض الدول لشمل آليات تحمي بياناتها، للتأكيد على حق سيادة البيانات لأغراض الأمن الوطني.[80]

كما أن هناك مجموعة كاملة من المفاوضات التي تجري حالياً في مجال الأمن مع التركيز على التقنيات. فعلى سبيل المثال، تسوية واسينار حول ضوابط التصدير للأسلحة التقليدية والبضائع والتقنيات ذات الاستخدام المزدوج، والتي وَقّعت عليها إحدى وأربعين دولة من بينها الولايات المتحدة، والمملكة المتحدة، وروسيا، ومعظم دول الاتحاد الأوروبي، وافقت مؤخراً على فرض قيود على بيع "أنظمة مراقبة الاتصالات" و"برمجيات التطفل" على الإنترنت المُصممة أو المُعدّلة خصيصاً لتجنب اكتشافها بواسطة أدوات المراقبة، أو للتغلب على إجراءات الحماية المضادة.[81] لدى الدول مخاوف مختلفة حول التطبيقات مزدوجة الأغراض لهذه التقنيات. فعلى سبيل المثال، تستخدم أداة تقييم نقاط الضعف في الغالب حالات استغلال هجمات يوم الصفر (zero day) لاكتشاف نقاط الضعف المتصلة بالشبكات. وبالإمكان استعمال نفس هذه التقنيات كأسلحة. بالتالي، فإن إخضاع هذه التقنيات لأنظمة ضبط الصادرات يدل على الاعتقاد بأن التقنيات المتقدمة قد تتغلب على الدفاعات الوطنية للدول وتشكل تهديداً للأمن الوطني.

وهناك مفاوضات ومباحثات دبلوماسية أخرى جارية تسعى لوضع فهم مشترك و/أو قواعد لزيادة الاستقرار والأمن في البيئة العالمية في مجال تكنولوجيا المعلومات والاتصالات. ويشمل هذا تقوية آليات التعاون لمعالجة الحوادث الأمنية المتعلقة بتكنولوجيا المعلومات والاتصالات ولمعالجة الطلبات المتعلقة بالبنية التحتية لتكنولوجيا المعلومات والاتصالات (مثل النشاط غير القانوني الصادر من الدولة بسبب الإصابة بشبكة (bot-net)). كما أن الدبلوماسية تُستَخدم أيضاً لتحديد نوع النشاطات الإلكترونية التي ينبغي السماح بها أو منعها (مثل المعايير للسلوكيات المقبولة للدول)، والتي عادة ما يُشار إليها بقواعد السلوك الإلكتروني. على سبيل المثال، سلّطت مجموعة الأمم المتحدة لخبراء الحكومات (GGE) الضوء على الطبيعة العالمية لبيئة تكنولوجيا المعلومات والاتصالات، وللتهديدات الموجودة الحالية والتهديدات المحتملة في مجال أمن المعلومات، والإجراءات التعاونية المحتملة لمعالجة تلك التهديدات. لقد وجدت مجموعة الأمم المتحدة لخبراء الحكومات (GGE) أن الالتزام بالقانون الدولي، وخاصة بالتزامات ميثاق الأمم المتحدة، يوفر إطار عمل أساسي لاستعمال الدول لتكنولوجيا المعلومات والاتصالات. حيث وافقت الدول على وضع إطار عمل لمعايير أو قواعد أو مبادئ إلكترونية للسلوك المسؤول للدول، وإجراءات لبناء الثقة (CBMs).[28] من بين إجراءات بناء الثقة، وافقت مجموعة الأمم المتحدة لخبراء الحكومات (GGE) على تقوية الآليات التعاونية بين الوكالات المعنية للدول من أجل معالجة الحوادث الأمنية في مجال تكنولوجيا المعلومات والاتصالات وتطوير آليات تقنية، وقانونية، ودبلوماسية إضافية لمعالجة الطلبات المتعلقة بالبنية التحتية لتكنولوجيا المعلومات والاتصالات (مثل تأسيس فريق CSIRT أو منظمة رسمية أخرى لأداء هذه الأدوار). ومنذ فترة قصيرة، اتفق رئيس الولايات المتحدة باراك أوباما مع الرئيس الصيني تشي جينبينج (بشكل مبدئي) على اتباع توصيات مجموعة الأمم المتحدة لخبراء الحكومات (GGE)

والالتزام بقواعد سلوكيات الإنترنت التي أقرتها الأمم المتحدة؛ وخاصة القواعد التي تنظم استخدام الهجمات الإلكترونية لإيذاء البنى التحتية الحساسة التي تخص الأطراف الأخرى خلال فترة السلم.[83]

استناداً إلى بعض الموضوعات المشتركة من مجموعة الأمم المتحدة لخبراء الحكومات (GGE)، اتفق قادة البرازيل، وروسيا، والهند، والصين، وجنوب أفريقيا (بريكس) على التعاون فيما بينها من أجل معالجة التحديات المشتركة في مجال أمن تكنولوجيا المعلومات والاتصالات. حيث وافقت هذه الدول على مشاركة المعلومات والممارسات المُثلى المتعلقة بأمن استعمال تكنولوجيا المعلومات والاتصالات، والتنسيق لمحاربة الجريمة الإلكترونية، وتأسيس شبكة POC في الدول الأعضاء، والتعاون فيما بين دول مجموعة بريكس باستعمال فرق CSIRT الحالية. كما حثّت أيضاً المجتمع الدولي على تركيز جهوده على إجراءات بناء الثقة (CBMs)، وبناء القدرات، وعدم استعمال القوة، وتجنب النزاعات المعتمدة على تكنولوجيا المعلومات والاتصالات.[84] إضافة إلى ذلك، في يناير 2015، قدمت منظمة شنغهاي للتعاون (SCO) إلى الجمعية العامة للأمم المتحدة (UNGA) مدونة سلوك دولية مُعدلة حول أمن المعلومات سعت من خلالها لتحديد حقوق الدول ومسؤولياتها في فضاء المعلومات، ولتعزيز السلوك البنّاء والمُتجاوب، ولتحسين التعاون لمواجهة التهديدات المتبادلة في مجال تكنولوجيا المعلومات والاتصالات.[85] وقامت منظمة شنغهاي للتعاون بمراجعة صيغة إصدار 2011 من مدونة السلوك وتعديلها بمصطلحات لغوية من تقارير العامين 2012 و2013 لمجموعة الأمم المتحدة لخبراء الحكومات من أجل زيادة قبول مدونة السلوك بين أعضاء مجموعة الـ77.

تخلط المحافل الدولية الأخرى بين موضوعات الاقتصاد، والتطوير، والأمن سعياً منها لتحقيق أهداف مُحددة. فعلى سبيل المثال، يعقد الاتحاد الدولي للاتصالات (ITU) نقاشات دولية منتظمة حول السياسة، والتكنولوجيا، والبيئة التنظيمية لتكنولوجيا المعلومات والاتصالات والإنترنت خلال أربعة اجتماعات من اجتماعاته الدولية وهي: القمة العالمية لمجتمع المعلومات (WSIS)، والمؤتمر العالمي للاتصالات الدولية (WCIT)، والمؤتمر العالمي لتطوير الاتصالات (WTDC)، والاجتماع الدولي لتقييس الاتصالات (WTSA).[86] إضافة إلى ذلك، قامت منظمة الدول الأمريكية (OAS) وبنك التنمية للدول الأمريكية (IDB) بتوحيد جهودهما للعمل مع الدول الأعضاء على معالجة الأمن الإلكتروني بشكل منظم كجزء من ثلاثة مجالات للمسائل: (1) التطوير الشامل اجتماعياً والمُستدام بيئياً؛ (2) تكنولوجيا المعلومات والاتصالات كأداة لتوليد الدخل والتوظيف، وتوفير الوصول للأعمال التجارية وللمعلومات، وتمكين التعليم الإلكتروني، وتسهيل النشاطات الحكومية؛ و (3) أمن بناها التحتية الرئيسة والخدمات المواجهة للمواطنين.[87]

الأمن الإلكتروني متشابك مع جميع عناصر السياسة الخارجية والتجارة.

من الواضح أن مسائل الأمن الإلكتروني قد بدأت بالظهور في العديد من المحافل الدبلوماسية المتنوعة. فالأمن الإلكتروني ليس مجرد مشكلة أمنية فحسب، بل هو عنصر أساسي للتجارة، والسياسة الخارجية والاقتصادية، وقدرة الدولة على النمو الاقتصادي في المستقبل. تشمل العناصر الرئيسة لقدرة الدولة على المشاركة الدبلوماسية الفعّالة في المسائل الإلكترونية تأسيس كادر خاص ومُدرب من الموظفين، وتطوير هياكل تنظيمية خاصة، وتخصيص التمويل للنقاشات والمفاوضات الدولية حول المسائل المتعلقة بالأمن الإلكتروني. على سبيل المثال، عيّنت إسرائيل وجمهورية التشيك مُلحقين إلكترونيين في سفاراتهما في المدن الرئيسة، من بينها واشنطن العاصمة وبروكسيل.[88]

وأقامت الولايات المتحدة كذلك برنامجاً تدريبياً في مجال التوعية الإلكترونية لمدة أسبوع واحد للموظفين الدبلوماسيين العاملين في آسيا.[89] إن تطوير هذا الكادر من الموظفين هو من العناصر الأساسية التي تساعد الدولة في تحقيق أهداف سياستها الخارجية، وسياستها الاقتصادية، وأهدافها التجارية وأهداف نموها الاقتصادي.

ينبغي أن تشمل عناصر قدرات المشاركة الدبلوماسية السليمة في مجال الأمن الإلكتروني ما يلي:

البيان:

أ. التحديد المُعلن للأمن الإلكتروني كعنصر أساسي من السياسة الخارجية والأمن الوطني (مثل مباحثات رسمية تضم عادة القادة السياسيين والعسكريين رفيعي المستوى في نقاشات ثنائية ومتعددة الأطراف)؛

ب. التحديد المُعلن لتكنولوجيا المعلومات والاتصالات وللأمن الإلكتروني كعنصر أساسي للسياسة الاقتصادية الدولية، والمفاوضات، والتجارة؛

التنظيم:

أ. تعيين موظفين مدربين ومتخصصين في المكتب الخارجي للدولة أو في المنظمات المماثلة تكون مهمتهم الأولية المشاركة الدولية النشطة في النشاطات الدبلوماسية للأمن الإلكتروني؛

ب. التناسق المُثبت بين أعداد ورُتب الموظفين الدبلوماسيين الخارجيين المُختصين في المجال الإلكتروني والالتزام المُعلن للدولة بالمشاركة في دبلوماسية الأمن الإلكتروني بصفتها مسألة ذات أهمية وطنية من الدرجة الأولى؛

الموارد:

أ. تحديد الموارد المالية والبشرية اللازمة والمُخصصة للمشاركة الدبلوماسية الإلكترونية؛

التنفيذ:

أ. المشاركة المُثبتة في تحديد، وتوقيع، وفرض اتفاقات دولية، ومتعددة الجنسيات، وإقليمية و/أو ثنائية تسعى لتحقيق حلول مقبولة بشكل متبادل للتحديات المشتركة؛ و

ب. الدليل المُثبت على الجهود للتأثير على مفاوضات التجارية الدولية المتعلقة باستعمال تكنولوجيا المعلومات والاتصالات، على الصعيد الإقليمي، و/أو الجوانب المشتركة وطنياً من البنية التحتية الإلكترونية، والخدمات والتقنيات ذات الأهمية الحساسة.

تعتمد النتائج الأولية في هذا العنصر الأساسي على مراجعة فيما إن قامت الدولة بشكل واضح بتعيين أو تأسيس مكتب حكومي أو كانت قد أوكلت أفراد بمسؤوليات دبلوماسية تشمل كل من الجوانب الاقتصادية والأمنية للمسائل الإلكترونية. يستند مؤشر الجاهزية الإلكترونية 2.0 على الموارد الأولية والثانوية لتحديد مدى مشاركة المكتب/المكاتب الحكومية أو الأفراد وتأثيرهم في المفاوضات الدولية حول المسائل المتعلقة بالأمن الإلكتروني. ستعمل تحديثات هذا العنصر الأساسي على مراقبة، وتتبع، وتقييم التطورات الجوهرية والبارزة.

7. الدفاع والتعامل مع الأزمات

العنصر السابع والأخير للجاهزية الإلكترونية هو قدرة القوى المسلحة للدولة و/أو وكالة الدفاع ذات الصلة على حماية الدولة من التهديدات الصادرة من الفضاء الإلكتروني. تعمل الدول المهتمة

بهذا النوع من القدرات على توجيه قواها الدفاعية لإنشاء قدرات أو خبرات للاستجابة للتهديدات الإلكترونية التي ترتقي إلى مستوى النزاعات "الإلكترونية" ذات الأهمية الوطنية. [90]

لقد أصبحت الدول أكثر اتصالاً واعتماداً على الإنترنت بشكل يجعلها أكثر عرضة للنشاطات الإلكترونية التخريبية والمدمرة. الوضعيات الدفاعية لمعظم الدول ضعيفة في وجه الهجمات الإلكترونية المُعقّدة. الطبيعة المتصلة عالمياً للمنافسات والنزاعات الحديثة تُشجّع الخصوم المتمكنين من الناحية الإلكترونية على التحرك أفقياً عبر الأنظمة الوطنية وعلى استهداف المنظمات التجارية وغير الحكومية للدولة. على سبيل المثال، في أغسطس 2012، تعرضت شركة أرامكو السعودية إلى هجوم استخدمت فيه البرامج الخبيثة لتدمير البيانات وتخريب ما يقارب الخمسة وسبعين بالمئة من البنية التحتية لتكنولوجيا المعلومات الخاصة بالشركة.[91] ادعى مسؤولو الشركة أن الحادثة كانت تهدف للتأثير على إنتاج النفط. وبعدها بأشهر قليلة، في مارس 2013، تعرضت عدة مؤسسات مالية في كوريا الجنوبية، بما فيها بنك شينهان – رابع أكبر بنك في الدولة – إلى أضرار بسبب برامج خبيثة شبيهة بتلك التي استخدمت ضد أرامكو السعودية. حيث تعطلت الخدمات الإلكترونية للبنك وتم تدمير بياناته. وقُدّرت الأضرار الاقتصادية الناتجة عن هذه الحادثة بحوالي 800 مليار دولار.[92] في ديسمبر 2014، تلاعب القراصنة بنجاح وعطّلوا أنظمة التحكم في إحدى معامل الفولاذ الألمانية، مما تسبب بإغلاق فرن الصهر فيه بشكل غير صحيح مما نتج عنه أضرار كبيرة.[93] في نفس السنة، وقعت شركة سوني بيكتشرز ضحية لهجوم إلكتروني تم فيه نسخ مواد فلمية غير منشورة بشكل غير قانوني، وسرقة رسائل إلكترونية للشركة ومن ثم تسريبها، والكشف عن وثائق مالية. كما تم نسخ بيانات حساسة تخص عشرات الآلاف من موظفي سوني، وتم تدمير ما يقارب 80 بالمئة من أصول تكنولوجيا المعلومات الخاصة بالشركة، من البيانات إلى الأجهزة بواسطة البرامج الخبيثة الفتاكة.[94]

ينبغي أن تكون الدول مستعدة للدفاع عن مصالحها المتصلة والمرتبطة بالشبكات للنزاعات الحالية والمستقبلية. تساعد سرعة ومدى انتشار الإنترنت على ربط جميع جوانب المجتمع وتوفر الوصول السهل للأسلحة الإلكترونية عسكرية المستوى، الأمر الذي يمنح العديد ميزة غير متناسقة. بالفعل، تنوع الجهات الخبيثة بما في ذلك النشطاء السياسيين، والمجرمين، والإرهابيين، والجهات الحكومية وغير الحكومية، والذين يتمتع جميعهم بدوافع مختلفة، يشدد ويؤكد أهمية وجوب الاستعداد لأسوأ السيناريوهات المحتملة. في الوقت الحالي، طورت أكثر من ستين دولة قدرات للتجسس والهجوم الإلكتروني، وفي الوقت نفسه تبدي اهتماماً كبيراً في شراء أو تطوير قدرات دفاعية وهجومية استباقية.[95] إضافة إلى ذلك، بدأت الدول بإعداد إستراتيجيات وأدوات مختلفة لترقية دفاعاتها الإلكترونية على المستوى الوطني. وسعت معظم الدول بصورة

تتطلب النشاطات الإلكترونية التخريبية والتدميرية دفاعاً إلكترونياً موثوق.

غريزية لزيادة القدرات الدفاعية الحالية التي هي قادرة بالفعل على العمل في وعبر الفضاء الإلكتروني خارج حدودها الوطنية (أي التنظيم الدفاعي أو الخدمات الاستخباراتية). بينما سعت دول أخرى لوضع هذه القدرات في منظمات أمنية غير موجودة بشكل مباشر ضمن تنظيماتها العسكرية. [96]

على سبيل المثال، في عام 2010 أنشأت الولايات المتحدة وحدة عسكرية خاصة – مركز الولايات المتحدة للقيادة الإلكترونية – لحماية البنية التحتية العسكرية من التهديدات الإلكترونية. وتم توسيع مهمة هذه الوحدة في عام 2015 عندما نشرت حكومة الدفاع إستراتيجيتها الإلكترونية الثانية لتوجيه تطوير القوى الإلكترونية لوزارة الدفاع (تحت قيادة وسيطرة مركز الولايات المتحدة للقيادة الإلكترونية) ولتقوية دفاعاتها الإلكترونية وقوة ردعها الإلكترونية. سَلّطت هذه الإستراتيجية الجديدة الضوء على التمتع "بالجاهزية لحماية أراضي الولايات المتحدة والمصالح الحيوية للولايات المتحدة من الهجمات التخريبية أو التدميرية ذات العواقب الكبيرة،" ولبناء، والحفاظ على، واستعمال خيارات إلكترونية قابلة للتطبيق لضبط تصعيد النزاعات وتشكيل بيئة الصراع في جميع المراحل. [97]

على نحو مشابه، أصدر الاتحاد الروسي في ديسمبر 2014 عقيدته العسكرية الجديدة التي تُبرز التطوير الروسي للقدرات الحربية الإلكترونية للأغراض الهجومية والدفاعية على حد سواء بالإضافة إلى «الردع غير النووي». [98] تقارن الورقة البيضاء لوزارة الدفاع الروسية في عام 2011 بعنوان «آراء مفاهيمية حول نشاطات القوات المُسلحة للاتحاد الروسي في فضاء المعلومات،» بين الجوانب المختلفة لعقيدة الدفاع الروسية، ولكنها تضم وبشكل واضح آراء عامة وتشدد على الحاجة لإطلاع وسائل الإعلام حول أوضاع النزاعات المتطورة لأغراض وقف التصعيد. [99] وفقاً لوسائل الإعلام الروسية، فإن القيادة الروسية تنوي نشر عقيدة جديدة لأمن المعلومات في عام 2016، يُزعم أنها لغرض تطوير قوات لحرب المعلومات وأنظمة معلومات للردع الإستراتيجي وتجنب النزاعات. [100]

كما أنشأت جمهورية كوريا الجنوبية والبرازيل أيضاً منظمات عسكرية مماثلة تهدف لتأمين القدرات الهجومية والدفاعية وقدرات الاستجابة بالإضافة إلى ضمان النصر الكامل في الحرب الإلكترونية. [101] وتعمل كوريا الجنوبية على توسيع قدراتها الإلكترونية وتشير التقارير إلى أنها تدرب أكثر من أربعمائة جندي إلكتروني جديد لمركز قيادة الدفاع الإلكتروني لجمهورية كوريا الجنوبية، بحيث سيصبح مجموعهم حوالي الألف فرد. [102]

إضافة إلى ذلك، بالرغم من أن جمهورية الصين الشعبية لم تنشر بعد علناً أي عقيدة إستراتيجية رسمية للتطبيقات العسكرية الإلكترونية أو المعلوماتية، إلا أنها نشرت مبادئ توجيهية إستراتيجية عسكرية لتقدم الإرشاد لسياسة الدفاع. [103] الورقة البيضاء لعام 2013 لجمهورية الصين الشعبية بعنوان: «*التوظيف المتنوع للقوى المسلحة الصينية*» و»الرأي حول زيادة قوة عمل أمن المعلومات» الصادر في 2014 يشددان على تطوير القدرات الإلكترونية الدفاعية. وتؤكد الوثائق على أن جيش التحرير الشعبي (PLA) لن يهجم إلا في حال الهجوم عليه، ولكن في حال الهجوم عليه، فإنه سيشن هجوم مُضاد في الفضاء الإلكتروني. [104]

لا ينبغي أن تكون وكالة الدفاع الإلكتروني وكالة نظامية ضمن الجيش الوطني. فبإمكان قوات الشرطة الوطنية أو القوات الاستخبارية أن تكون بمثابة مركز القدرات المركزية للحكومة للدفاع في الفضاء الخارجي، وبالرغم من ذلك، ينبغي تحديث القوات المسلحة أيضاً وأن يتم تجهيزها للمزيد من النزاعات التقليدية. على سبيل المثال،

ركّزت أيسلندا قوات دفاعها الإلكترونية خارج قواتها المسلحة. في الماضي، كانت مسؤوليات الأمن الإلكتروني الأيسلندية موزعة على وزارة الداخلية، وإدارة البريد والاتصالات، وسلطة حماية البيانات، والشرطة الأيسلندية. ولكن، في عام 2015 قامت أيسلندا بمركزة جميع قدراتها الإلكترونية تحت سلطة المأمور الوطني للشرطة الأيسلندية.[105] وتسلط الإستراتيجية الإلكترونية الوطنية لأيسلندا الصادرة في شهر يونيو 2015 الضوء على الدور التكاملي لتحالف الناتو في الدفاع الإلكتروني الأيسلندي.[106]

أخيراً، وبالرغم من عدم تمتع إسرائيل «بمركز قيادة إلكتروني» رسمي في الوقت الحالي، إلا أنه لديها قدرات في مجال الأمن الإلكتروني وهي موزعة في مختلف أقسام جيش الدفاع الإسرائيلي (IDF) ومديرية الاستخبارات العسكرية. تتولى مديرية الاستخبارات العسكرية القدرات الهجومية، بينما تتولى الأجهزة الحماية. الشين بيت، والذي هو الجهاز الأمني الداخلي لإسرائيل، هو الجهة المسؤولة عن الدفاع عن أنظمة الحكومة وعن البنى التحتية الوطنية ذات الأهمية الحساسة، وتؤمّن قوة المهام الإلكترونية الوطنية الشبكات ذات الأهمية الحساسة والصناعة الخاصة وتحميها من القرصنة والتجسس.[107] ولكن هذا الأمر قد يتغير، لأنه في شهر يونيو 2015، أعلن الفريق جادي آيزنكوت، قائد الجيش الإسرائيلي، عن نيته لتأسيس كتيبة جديدة في جيش الدفاع الإسرائيلي – على قدم المساواة مع القوة البحرية والجوية – تكون مسؤولة عن كافة الأنشطة الإلكترونية. في حال موافقة وزير الدفاع على الكتيبة الجديدة، سيكون جيش الدفاع الإلكتروني الجديد جاهزاً للعمل في غضون عامين. وبعد أن يبدأ بالعمل، ستقوم القيادة الإلكترونية الجديدة بدمج القدرات الدفاعية التي يوفرها حالياً جيش الدفاع الإسرائيلي مع القدرات الهجومية والاستخبارية التي تؤديها الوحدة 8200 والمجموعات الاستخبارية والعسكرية الأخرى.[108] ويتماشى هذا مع الخطة الخمسية الجديدة لجيش الدفاع الإسرائيلي، المسماة «Gideon»، والتي نُشرت في أغسطس 2015. تدعو خطة «Gideon» بشكل خاص إلى زيادة عدد المبادرات لصد الهجمات الإلكترونية والتهديدات غير المتناسقة الأخرى التي قد تصدر عن جهات غير تابعة لدول وعن مجموعات إرهابية في المنطقة.[109]

قدرات الدفاع الإلكترونية ضرورية للدول لضمان أمنها الوطني والاقتصادي. مع ازدياد اعتماد الدول على الإنترنت وأنظمة تكنولوجيا المعلومات والاتصالات، تزداد فرصة إصابتها بالتهديدات الإلكترونية «منخفضة المستوى» وبالنشاطات غير المتناسقة. تواجه الدول معضلات لا مفر منها، والتبني المتزايد لتكنولوجيا المعلومات والاتصالات ضروري للنمو، ولكن كلما زادت نسبة اتصال الدولة كلما زاد عدد المخاطر التي تتعرض لها. لم يعد الاستغناء عن اقتصاد الإنترنت من الخيارات المقبولة. لذا ينبغي على الدول أن تكون جاهزة للدفاع عن نفسها في الفضاء الإلكتروني. إن كانت الدولة غير قادرة عن الدفاع عن نفسها، فهي غير جاهزة إلكترونياً.

عناصر التزام الدولة بتطوير ونشر وحدات دفاع وطنية متخصصة تتمتع بقدرات/مسؤوليات دفاعية إلكتروني قد تشمل:

البيان:

أ. نشر بيانات وطنية تُوكل مهمة الدفاع الوطني الإلكتروني لإحدى المنظمات بصفتها مهمة من المستوى الأول؛

ب. وضع سياسات لمنظمة الدفاع الإلكتروني لتستجيب للتهديدات الإلكترونية.

ج. صياغة بيانات وطنية توجه منظمة الدفاع الإلكتروني نحو تطوير القدرات للاستجابة للتهديدات داخل الإقليم السيادي أو خارجه؛

التنظيم:

أ. تأسيس منظمة على المستوى الوطني، داخل الجيش، تكون مهمتها الأولية الدفاع الإلكتروني عن الدولة؛

ب. ب. تأسيس منظمة على المستوى الوطني، خارج الجيش، تكون مهمتها الأولية الدفاع الإلكتروني عن الدولة؛

الموارد:

أ. تحديد الموارد المالية والبشرية المطلوبة والمُخصصة للمنظمة، داخل الجيش، التي تشمل مهمتها بشكل واضح الدفاع الإلكتروني عن الدولة؛

ب. تحديد الموارد المالية والبشرية المطلوبة والمُخصصة للمنظمة، خارج الجيش، التي تشمل مهمتها بشكل واضح الدفاع الإلكتروني عن الدولة؛

التنفيذ:

أ. الدليل على التمارين التي تم إجرائها على مستوى الحكومة والتي تُثبت الجاهزية الوطنية للدفاع الإلكتروني؛

ب. الدليل على التمارين التي تم إجرائها على المستوى الوطني بمشاركة الجهات التجارية المُتأثرة والتي تُثبت الجاهزية الوطنية للدفاع الإلكتروني؛

ج. الدليل على التمارين التي تم إجرائها مع الشركاء الدوليين (مثل الدفاع المشترك مع الناتو أو تمرين APCERT) والتي تُثبت التعاون من خلال تبادل المعلومات والمساعدة؛

د. وضع معايير للسلوك المسؤول للدولة في الفضاء الإلكتروني وتحديد العتبات الحديّة التي تسمح بالتدخل للدفاع الإلكتروني؛ و

ه. وضع آليات للمساعدة السريعة (قابلة للانفصال عن فرق CERT أو الجهات المساوية لها) للحكومة أو لصناعات مُحددة في حال وقوع حوادث إلكترونية كبرى.

تعتمد النتائج الأولية في هذا العنصر الأساسي على مراجعة لتقييم فيما إن كانت الدولة قد أعلنت بشكل رسمي إنشاء قوى دفاعية بحيث يكون الدفاع الإلكتروني عن الدولة من مهامها من المستوى الأول.

يستند مؤشر الجاهزية الإلكتروني على الموارد الأولية والثانوية لتحديد مستوى النضج التشغيلي. ستعمل تحديثات هذا العنصر الأساسي على مراقبة، وتتبع، وتقييم التطورات الجوهرية والبارزة.

الخلاصة

تفتقر جميع الدول للجاهزية الإلكترونية.

التهديدات التي تواجه أنظمتنا وبنانا التحتية المُتصلة بالشبكات حقيقية وآخذة بالنمو وهي تفرض تكاليف كبيرة على المستوى الاقتصادي بالنسبة للدول والمجتمعات. ينبغي توحيد الأجندات الاقتصادية وأجندات الأمن الوطني لجلب الشفافية لانعدام الأمن الإلكتروني. فعرض هذه الشراكة الحيوية قد يجذب الاهتمام الوطني والدولي لمعالجة هذا التآكل الاقتصادي. توفر المنهجية الشاملة والمقارنة والقائمة على الخبرة لمؤشر الجاهزية الإلكتروني 2.0 مُخططاً لتقييم مستوى نضج أي دولة والتزامها بتأمين بنيتها التحتية وخدماتها الإلكترونية التي يعتمد عليها مستقبلها الرقمي ونموها.

يُحدد مخطط مؤشر الجاهزية الإلكترونية 2.0 أكثر من سبعين مؤشر بياني فريد موزع على سبعة عناصر أساسية هي: الإستراتيجية الوطنية، والتعامل مع الحوادث، والجريمة الإلكترونية وتطبيق القانون، ومشاركة المعلومات، والاستثمار في البحث والتطوير، والدبلوماسية والتجارة، والدفاع والتعامل مع الأزمات. وتوفر هذه المؤشرات والعناصر الأساسية إطار عمل للدولة لتطوير وتقوية وضعها الأمني لتتمكن من مجابهة تآكل إجمالي الناتج المحلي. في الواقع، يتحدى مؤشر الجاهزية الإلكترونية 2.0 الحكمة التقليدية

التي تنص على أن الأمن الإلكتروني هو بالدرجة الأولى مسألة أمن وطني. بإمكان مؤشر الجاهزية الإلكترونية 2.0 أن يثبت مدى الترابط اللصيق بين الأمن الوطني والاتصال بالإنترنت والتبني السريع لتكنولوجيا المعلومات والاتصالات التي يمكن أن تؤدي إلى النمو والازدهار الاقتصادي عندما تكون آمنة.

بدلاً من مجرد دراسة المشكلة، يوفر مؤشر الجاهزية الإلكترونية إطار عمل للدولة لتقييم قوة قدرتها على تجنب التآكل الاقتصادي الناتج عن انعدام الأمن الإلكتروني. سيتم تحديث مؤشر الجاهزية الإلكترونية 2.0 بشكل منتظم مع إضافة معايير للتقييم دون فقدان المصداقية المقارنة مع أي تقييمات سابقة. بهذه الطريقة، سيوضّح مؤشر الجاهزية الإلكترونية 2.0 تقدم وتطور الدول نحو تأمين البنية التحتية والخدمات الإلكترونية التي يعتمد عليها مستقبلها الرقمي ونموها.

لا تستطيع أي دولة تحمل تكلفة انعدام الأمن الإلكتروني والخسائر الناتجة عنه. بإمكان بيانات مؤشر الجاهزية الإلكترونية 2.0 ومنهجيته مساعدة قادة الدول على رسم المسار لتحقيق اقتصاد أكثر أمناً ومرونة في هذا العالم الإلكتروني بشدة والتنافسي والعُرضة للنزاعات.

للمزيد من المعلومات أو لتقديم البيانات لمنهجية مؤشر الجاهزية الإلكترونية 2.0، يُرجى الاتصال بـ:

CyberReadinessIndex2.0@potomacinstitute.org

قائمة المراجع

1. تم إعداد مؤشر الجاهزية الإلكترونية 2.0 بناءً على مؤشر الجاهزية الإلكترونية 1.0 السابق الذي قدّم إطار عمل منهجي لتقييم الجاهزية الإلكترونية قائم على خمسة عناصر أساسية هي: الإستراتيجية الوطنية الإلكترونية، والتعامل مع الحوادث، والجريمة الإلكترونية والصلاحية القانونية، ومشاركة المعلومات، والبحث والتطوير الإلكتروني. طبّق مؤشر الجاهزية الإلكترونية 1.0 هذه المنهجية على مجموعة أولية مكونة من خمسة وثلاثين دولة. للمزيد من المعلومات حول مؤشر الجاهزية الإلكترونية 1.0، يُرجى الاطلاع على: ميليسا هاثاواي، "مؤشر الجاهزية الإلكترونية 1.0، " *Hathaway Global Strategies LLC (2013), http://belfercenter.ksg.harvard.edu/files/cyber-readiness-index-1point0.pdf*"

2. التشابك بين البنية التحتية والإنترنت هو الاعتماد المتبادل على اتصال الإنترنت لتقديم الخدمات الرئيسة مثل الماء والكهرباء والنقل والاتصالات والصحة إلخ. للمزيد من المعلومات حول التشابك بين البنى التحتية والإنترنت يُرجى الاطلاع على: ميليسا هاثاواي: "الخيارات المتصلة: كيف يتحدى الإنترنت القرارات السيادية، "اهتمامات السياسة الخارجية الأمريكية 36، العدد 5 (نوفمبر 2014): 301.

3. من الأمثلة على الإستراتيجيات الاقتصادية المُدعمة بتكنولوجيا المعلومات والاتصالات (ICT) والمطبقة حول العالم: *السوق الأوروبي الرقمي الواحد*؛ *السوق الرقمي الهندي (ID)*؛ خطة *Internet Plus (+)* في الصين؛ و*ITU Connect 2020*.

4. مجلس الدولة الصيني، "Internet Plus" *جوو فا 40* (2015) . ترجمة وزارة الخارجية الأمريكية.

5. حكومة الهند، "ركائز البرنامج،" الهند الرقمية: القوة للتمكين، *http://www.digitalindia.gov.in/content/programme-pillars*.

6. المفوضية الأوروبية، "السوق الرقمي الواحد: إزالة الحواجز للكشف عن فرص الإنترنت،" *http://ec.europa.eu/priorities/digital-single-market/*

7. ميليسا هاثاواي وفرانشسكا سبيداليري، "التطور المستدام والآمن: إطار عمل للمجتمعات المرنة والمتصلة،" في *مرصد الأمن الإلكتروني في أمريكا اللاتينية والكاريبي* (النشرة القادمة لشهر ديسمبر 2015 لمنظمة الولايات المتحدة).

8. البنك الدولي، "نظرة عامة،" برنامج تقنيات الاتصالات والمعلومات، آخر تعديل 2 أكتوبر 2014، *http://worldbank.org/en/topic/ict/overview*

9. ديفيد دين وآخرون، "البيان الرقمي: كيف يمكن للشركات والدول الفوز في الاقتصاد الرقمي،" تقرير *Boston Consulting Group* (يناير 2012): 2.

10. بيتر سي. إيفانز وماركو أنونزياتا، "الإنترنت الصناعي: دفع حدود العقول والماكينات، "*General Electric* (26 نوفمبر 2012): 13.

11. ميليسا هاثاوي، "مؤشر الجاهزية الإلكترونية 2.0 والدروس المستفادة من تصميم الإستراتيجيات الوطنية للأمن الإلكتروني الوطني،" (عرض تقديمي في ورشة عمل OAS-IDB الإقليمية حول سياسات الأمن الإلكتروني، واشنطن العاصمة، 23 أكتوبر 2014)).

12. Frontier Economics London، *تقدير آثار الاقتصاد العالمي والآثار الاجتماعية للتزوير والقرصنة: تقرير بتفويض من Business Action to Counterfeiting and Piracy*، (لندن، Frontier Economics Ltd، 2011): 47

13. المكتب الوطني للأبحاث الآسيوية، "تقرير لجنة IP: تقرير اللجنة حول سرقة الملكية الفكرية الأمريكية،" المكتب الوطني للأبحاث الآسيوية (مايو 2013)

14. ميليسا هاثاواي، "الخيارات المتصلة: كيف يتحدى الإنترنت القرارات السيادية،" *اهتمامات السياسة الخارجية الأمريكية* 36، العدد 5 (نوفمبر 2014): 301.

15. يعود لهارفي بوبل الفضل في اختراع كرات هارفي في السبعينيات من القرن العشرين بينما كان يعمل كمستشار لدى Booz Allen Hamilton

16. حسب تصنيفات البنك الدولي لإجمالي الناتج المحلي للعام 2013

17. منظمة التعاون الاقتصادي والتنمية، نظرة استشرافية لمنظمة التعاون الاقتصادي والتنمية على الاقتصاد الرقمي 2015 (باريس، فرنسا: منشورات منظمة التعاون الاقتصادي والتمنية، 2015)، *http://dx.doi.org/10.1787/9789264232440-en*.

18. ميليسا هاثاواي، الشفافية والثقة وشبكة الإنترنت الخاصة بنا،" (عرض تقديمي في مؤتمر GTEC، أوتاوا، كندا، 20 أكتوبر 2015).

19. تشمل البنية التحتية لتكنولوجيا المعلومات والاتصالات قطاعي الاتصالات الثابتة والمتنقلة (الصوتية والبيانات) من السوق – كل من الاشتراكات والوصول المنزلي إلى البيانات – والاستثمار في قطاع الاتصالات والأرباح التي يحققها.

20. السلطة المختصة هي أي شخص أو منظمة تتمتع بالسلطة أو القدرة أو الصلاحية المفوضة أو الممنوحة بشكل قانوني لإنجاز أي من الوظائف المُوكلة لها.

21. اتحاد الاتصالات الدولي، "الإستراتيجيات الوطنية،" *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx*.

22. يشير المصطلحان CSIRT و CERT إلى فريق من خبراء أمن تكنولوجيا المعلومات توكل إليه مهمة الاستجابة إلى حوادث أمن الحاسوب. ويُستخدم كلا المصطلحين بشكل متبادل، ولكن مصطلح CSIRT هو المصطلح الأكثر دقة.

23. اتحاد الاتصالات الدولي، "برنامج CIRT،" *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx*.

24. جون هولر، ساموبل ميريل، ماثيو بوتكوفيتش، وبرادفورد ويلكي، الممارسات المُثلى للأمن الإلكتروني الوطني: بناء قدرات وطنية لإدارة حوادث أمن الحواسيب، الإصدار 2.0 (بيتسبرغ، فيلادلفيا: معهد هندسة البرمجيات، جامعة كارينج ميلون، 2011)، *http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9999*.

25. أولاف كريوهوف، "تطور فرق CERT الوطنية والشركاتية – الثقة والعامل الرئيس،" في الممارسات المُثلى في الدفاع عن شبكات الحاسوب: الكشف عن الحوادث والاستجابة لها، ميليسا إي. هاثاواي، (أمستردام سلسلة الناتو للعلوم من أجا السلام والأمن، دار IOS للنشر، فبراير 2014).

26. فريق سنغافورة للاستجابة لطوارئ الحاسوب، "الأسئلة الشائعة،" *https://www.csa.gov.sg/singcert/about-us/faqs*.

27. Ministério das Comunicações, "Portaria Interministerial N 147, de 31 de Maio de 1995," *http://cgi.br/portarias/numero/147*.

28. *rb.trec*، معلومات حول *rb.TREC*،" *http://www.cert.br/about/*.

29. "الوثائق،" APCERT. APCERT. Org، 13 أكتوبر 2015. *http://www.apcert.org/documents/index.html*.

30. "إطار العمل التشغيلي لفريق آسيا والمحيط الهادئ للاستجابة لطوارئ الحاسوب" APCERT. APCERT. org، 13 أكتوبر 2015. *http://www.apcert.org/documents/pdf/OPFW(26Mar2013).pdf*.

31. ميليسا هاثاواي، "الممارسات المُثلى في الدفاع عن شبكات الحاسوب: الكشف عن الحوادث والاستجابة لها، "المركز العالمي للأمن الإلكتروني (سبتمبر 2013): 12.

32. إنغفار هيلكويست (عقيد متقاعد)، مستشار أقدم ولارس نيكاندر، مدير، مركز دراسات التهديدات غير المتناسقة، جامعة الدفاع السويدية، "دورة CATS والتمرين الإلكتروني،" (مقابلة بواسطة ميليسا هاثاواي في ستوكهولم، السويد، 17 أكتوبر 2012) وكلية الدفاع الوطني السويدية، "رسالة CATS الإخبارية." مركز CATS لدراسات التهديدات غير المتناسقة (ربيع 2013).

33. دوستان نافراتيل، مدير السلطة الأمنية الوطنية للجمهورية التشيكية وروبرت كاهوفر، مُساعد خاص، "التشيك الإلكترونية 2015 – تمرين أمني إلكتروني تقني وطني، "مقابلة بواسطة ميليسا هاثاواي في واشنطن العاصمة، أكتوبر 2015).

34. "كوريا الجنوبية تقول أن الدودة النووية لا تدعو للقلق، " TheRegister.co.uk، 30 ديسمبر 2014، *http://www.theregister.co.uk/2014/12/30/south_korea_says_nuclear_worm_is_nothing_to_worry_about* و "ناشطون يخترقون أنظمة حاسوب KNHP، "الأخبار النووية العالمية 22 ديسمبر 2014، *http://www.world-nuclear-news.org/C-Activists-hack-KHNPs-computer-systems-2212141.html*

35. وزارة الأمن الداخلي، "العاصفة الإلكترونية: تأمين الفضاء الإلكتروني،" *http://www.dhs.gov/cyber-storm-securing-cyber-space*.

36. المفوضية الأوروبية، "إستراتيجية إلكترونية للاتحاد الأوروبي: فضاء إلكتروني مفتوح وآمن ومأمون، "رسالة مشتركة إلى البرلمان الأوروبي، المجلس، واللجنة الاقتصادية والاجتماعية الأوروبية ولجنة الأقاليم، (يوليو 2013): 7 وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات، "أوروبا الإلكترونية/" *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe*.

37. دوغ درينكووتر، "تواجه المئات من الشركات ألفي هجمة إلكترونية في تمرين للاتحاد الأوروبي، "مجلة SC، 31 أكتوبر 2014 في الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)، "ENISA أوروبا الإلكترونية 2014: تغطية إعلامية،" *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/cyber-europe-2014-media-coverage*.

38. وكالة الدفاع الأوروبية، "تمرين لإدارة أزمة إلكترونية مُعقدة في فيينا،" 16 سبتمبر 2015، *https://www.eda.europa.eu/info-hub//16/09/press-centre/latest-news/2015complex-cyber-crisis-management-exercise-in-vienna* "انطلاق أكبر تمرين للدفاع الإلكتروني للناتو في التاريخ،" 21 نوفمبر 2014، *http://www.nato.int/cps/en/natohq/news_114902.htm?selectedLocale=en*.

39. كيتي بو ويليامز، "الولايات الأمريكية المتحدة والمملكة المتحدة ستختبر الأمن الإلكتروني للقطاع المالي هذا الشهر،" The Hill، 2 نوفمبر 2015، *http://thehill.com/policy/cybersecurity/258827-us-uk-to-test-finance-sector-cybersecurity-this-month*.

40. CNCERT/CC، "إقامة الاجتماع السنوي الثاني لفريق CSIRT الخاص بالصين واليابان وكوريا للاستجابة لحوادث الأمن الإلكتروني في كوريا،" *www.cert.org.cn/publish/english/552/2014091614573929599608 4/2014/html._01409161457392959960 84*.

41. جامعة كارينج ميلون، "قائمة فرق CSIRT الوطنية، "قسم CERT، *http://www.cert.org/incident-management/national-csirts/national-csirts.cfm*.

42. الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)، "مخزون ENISA- CERT: مخزون فرق CERT والنشاطات في أوروبا، " ENISA الإصدار 2.16 (يونيو 2014)، *http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe*.

43. منتدى التعامل مع الحوادث والفرق الأمنية (FIRST)، "أعضاء FIRST،" *http://www.first.org/members/teams*.

44. المجلس الأوروبي، مؤتمر الجريمة الإلكترونية (23 نوفمبر 2001) ومنظمة شنغهاي للتعاون، التعاون في مجال أمن المعلومات، الاجتماع الكامل 61 (16 يونيو 2009).

45. نفس المرجع السابق.

46. منظمة شنغهاي للتعاون، التعاون في مجال أمن المعلومات، الاجتماع الكامل 61 (16 يونيو 2009، *https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf*.

47. القاضي ستين سكولبرغ وأماندا ام. هابارد، "موائمة المنهجيات القانونية الوطنية حول الجريمة الإلكترونية،" اتحاد الاتصالات الدولي (1 يوليو 2005): 6.

48. تضم الدول العشرون التي وقعّت على تقرير مجموعة الأمم المتحدة لخبراء الحكومات (GGE): بيلاروسيا، البرازيل، الصين، كولومبيا، مصر، استونيا، فرنسا، ألمانيا، غانا، إسرائيل، اليابان، كينيا، ماليزيا، المكسيك، باكستان، كوريا، روسيا، إسبانيا، المملكة المتحدة، والولايات المتحدة الأمريكية. أنظر: الأمم المتحدة، تقرير مجموعة خبراء الحكومات حول التطوير في مجال المعلومات والاتصالات في سياق الأمن الدولي، A/65/201 و A/68/98 (26 يونيو 2015)

49. إرنستو يو. سافونا، الجريمة والتكنولوجيا: آفاق جديدة للأنظمة، وتطبيق القانون، والبحث (دوردرشت، هولندا: سبرنجر، 2004): 50.

50. المركز المتقدم للبحث والتطوير التدريب في القوانين والأدلة الجنائية الإلكترونية، "البرامج الأكاديمية" الكلية الوطنية للقانون في جامعة الهند، *https://www.nls.ac.in/index.php?option=com_content&view=article&id=502&Itemid=32*.

51. إنتربول، "مجمع الإنتربول الدولي للابتكار،" تم الدخول إليه في 17 سبتمبر 2015، http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation.

52. مادان ام، أوبيرو، "الشبكة المظلمة والعملة التشفيرية،" (عرض تقديمي في Cyber 360: اجتماع مغلق لـ Synergia، بنغالور، الهند، 30 سبتمبر 2015).

53. البوت (bot) هو شكل خبيث من البرمجيات بإمكانه استعمال حاسوبك لإرسال رسائل إلكترونية غير مرغوب بها، واستضافة موقع انتحالي، أو سرقة هويتك من خلال مراقبة ضرباتك على لوحة المفاتيح. ومن ثم يتم التحكم بالحواسيب المصابة بواسطة أطراف ثالثة وبالإمكان استعمالها لشن هجمات إلكترونية. للمزيد من

المعلومات، أنظر: ميليسا هاثاواي وجون سافاج، "إدارة الفضاء الإلكتروني: واجبات مزودي خدمات الإنترنت،" الحوار الإلكتروني 2012 (مارس 2012) .

54. ألاستير ستفنسون، "مكتب التحقيقات الفدرالي يُحذر، شبكات البوتنت تصيب 18 نظام في الثانية،" V3.cok. uk، 16 يوليو 2014، *http://www.v3.co.uk/v3-uk/news/2355596/botnets-infecting-18-systems-per-second-warns-fbi*.

55. بل كندا وغيره، "مشروع الفضاء المُظلم،" اللجنة الاستشارية للاتصالات الأمنية (2011): 13، *https://citizenlab.org/cybernorms2012/cybersecurityfindings.pdf*.

56. يوري إيتو، "مركز النظافة الإلكترونية،" (مقابلة عن بعد مع فريق مؤشر الجاهزية الإلكترونية، واشنطن العاصمة، 10 نوفمبر 2015)..

57. وزارة الشؤون الداخلية والاتصالات ووزارة الاقتصاد والتجارة والصناعة، "ما هو مركز النظافة الإلكترونية،" مركز النظافة الإلكترونية -*https://www.telecom-isac.jp/ccc/en_index* ومايكل ام. لوسافيو، جي. إيجل شات وديبورا ولسون كيلنج، "تغيير اللعبة: النماذج الاجتماعية والعدلية لتحسين الأمن الإلكتروني،" المجلد 2 من حماية البنية التحتية الإلكترونية لطارق سعداوي، لويس اتش، جوردان جونيور وفنسنت بودرو (كلية الحرب في الجيش الأمريكي، دراسات إستراتيجية، 2013): 101.

58. مركز Telecom-ISAC اليابان، "رسالة الرئيس،" 12 مايو 2011، *https://www.telecom-isac.jp/english/index.html*.

59. المبادرة الأسترالية لأمن الإنترنت (AISI)، "نظرة عامة على المبادرة الأسترالية لأمن الإنترنت،" *http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative*.

60. McAfee: McAfee ومركز الدراسات الدولية والإستراتيجية (CSIS): إيقاف الجريمة الإلكترونية قادرة على التأثير بشكل إيجابي على اقتصادات العالم،" 9 يونيو، 2014، *http://www.mcafee.com/us/about/news/2014/q2-20140609-01.aspx* والمكتب الوطني للأبحاث الآسيوية، تقرير لجنة IP: تقرير اللجنة حول سرقة الملكية الفكرية الأمريكية،" المكتب الوطني للأبحاث الآسيوية (مايو 2013).

61. ميليسا هاثاواي، "سبب أهمية الشراكات الناجحة بالنسبة تعزيز الأمن الإلكتروني،" The New New Internet، 7 مايو 2010.

62. وزارة الأمن والعدل الهولندية، "المركز الوطني للأمن الإلكتروني (NCSC)، *https://www.ncsc.nl/english*.

63. في فبراير 2007، تم دمج مركز التنسيق الأمني للبنى التحتية الوطنية في المملكة المتحدة مع المركز الاستشاري للأمن الوطني (NSAC) ليشكلا معاً مركز حماية البنى التحتية الوطنية (CPNI). للمزيد من المعلومات حول مركز CPNI، أنظر: مركز حماية البنى التحتية الوطنية، *http://www.cpni.gov.uk*.

64. وكالة تشجيع تكنولوجيا المعلومات (IPA)، مركز أمن تكنولوجيا المعلومات في اليابان، *مبادرة مشاركة معلومات الأمن الإلكتروني، شراكة اليابان* (J-CSIP) التقرير السنوي للنشاطات للسنة المالية 2012، (أبريل 2013).

65. مركز مشاركة وتحليل المعلومات والخدمات المالية، "نظرة عامة على FS-ISAC،" تم الدخول إليه في 17 سبتمبر 2015، *www//:sptth fsisac.com/sites/default/files/FS-ISAC_Overview_2011_05_09.pdf*.

66. الاتحاد الوطني للأدلة الجنائية والتدريب الإلكتروني، "كن أحد شركاء NCFTA،" *https://www.ncfta.net/become-ncft-partner.aspx*.

67. رافايل ماندارينو، " MT2: الشراكة بين القطاعين الخاص والعام،" مجلس الأمن المؤسسي، دائرة أمن المعلومات والاتصالات، مكتب الرئيس، (عرض تقديمي في المؤتمر الأمني الأول للإنتربول، هونغ كونغ، 15-17 سبتمبر 2010).

68. المعهد الوطني للمعايير والتكنولوجيا، "قاعدة البيانات الوطنية لنقاط الضعف،" *https://nvd.nist.gov*.

69. لقد وضعت المملكة المتحدة والبرازيل آليات لإلغاء سرية (نظام الكتابة مقابل النشر) المعلومات الاستخبارية ومشاركتها مع القطاعات المعنية بشكل أفضل بكثير من الولايات المتحدة.

70. المفوضية الأوروبية، "البحث والابتكار في مجال تكنولوجيا المعلومات والاتصالات،" Horizon 2020: برنامج إطار عمل الاتحاد الأوروبي للبحث والابتكار، *http://ec.europa.eu/programmes/horizon2020/en/area/ict-research-innovation*.

71. للمزيد من المعلومات حول برنامج بحث وتطوير الشبكات وتكنولوجيا المعلومات (NITRD) ومجالات بحثه، انظر: *www.nitrd.gov/Index.aspx* "برنامج بحث وتطوير الشبكات وتكنولوجيا المعلومات،" مُلحق لميزانية الرئيس للسنة المالية 2016 (فبراير 2015)، *https://www.whitehouse.gov/sites/default/files/microsites/ostp/fy2016nitrdsupplement-final.pdf*.

72. القنصلية العامة لإسرائيل في نيويورك، "مجلس الوزراء يوافق على تخفيضات ضريبية للمنتزه الإلكتروني الوطني، "القنصلية العامة لإسرائيل في نيويورك، 7 يونيو 2014، *http://embassies.gov.il/wellington/NewsAndEvents/Pages/Cabinet-approves-tax-break-for-National-Cyber-Park-6-Jul-2014.aspx*.

73. Ciência Sem Fronteiras، "الأسئلة الشائعة"، *http://www.cienciasemfronteiras.gov.br/3-v1_2105-web/csf-eng/faqEGTI_2013*، التنسيق لتحسين موظفي التعليم العالي (CAPES)، "التنسيق لتحسين موظفي التعليم العالي (CAPES)"، *http://www.iie.org/Programs/CAPES*, and CNPq, "Programas Institucionais de Iniciação Científica e Tecnológica," *http://www.cnpq.br/web/guest/piict*.

74. "الأمن الإلكتروني،" *The Hague Security Delta*, *https://www.thehaguesecuritydelta.com/cyber-security*.

75. زاك كتلر، "5 مراكز نامية للأمن الإلكتروني حول العالم، "Entrepreneur، 3 سبتمبر 2015، *http://www.entrepreneur.com/article/250024*.

76. المفوضية الأوروبية، "معلومات حول الشراكة الأطلسية للتجارة والاستثمار (TTIP)، *http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/*.

77. "أهلاً بكم في الملاذ الآمن في أمريكا-الاتحاد الأوروبي،" *http://www.export.gov/safeharbor/eu/eg_main_018365.asp*.

78. محكمة عدل الاتحاد الأوروبي، "أعلنت محكمة العدل أن قرار المفوضية عن الملاذ الآمن في الولايات المتحدة لاغٍ،" البيان الصحفي 117/15 (6 أكتوبر 2015)، *http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf*.

79. غرفة التجارة الأمريكية للاتحاد الأوروبي، "قرار محاكم عدل الاتحاد الأوروبي في قضية شرمس قد يعيق الأعمال التجارية عبر المحيط الأطلسي، ويضر باقتصاد الاتحاد الأوروبي ويعرض السوق الرقمي الواحد للخطر، بيان صحفي، 6 أكتوبر 5102، *http://www.amchameu.eu/sites/default/files/press_releases/press_-_ecj_decision_on_schrems_will_disrupt_transatlantic_business.pdf*.

80. ميليسا هاثاواي: "الخيارات المتصلة: كيف يتحدى الإنترنت القرارات السيادية،" 302 وأرون موهان سوكمار، "اللعبة الكبيرة الجديدة في آسيا،" The Hindu، 25 أغسطس 2015، تم الدخول إليها في 16 سبتمبر 2015، *http://www.thehindu.com/opinion/op-ed/arun-mohan-sukumar-column-the-new-great-game-in-asia/article7575755.ece*.

81. "تسوية واسينار حول ضوابط التصدير للأسلحة التقليدية والبضائع والتقنيات ذات الاستخدام المزدوج" آخر تحديث 16 سبتمبر 2015، *http://www.wassenaar.org/index.html*.

82. الأمم المتحدة، تقرير مجموعة خبراء الحكومات حول التطوير في مجال المعلومات والاتصالات في سياق الأمن الدولي، A/65/201 و A/68/98 (26 يونيو 2015).

83. مكتب السكرتير الإعلامي في البيت الأبيض، "ورقة معلومات: زيارة الرئيس تشي جينبينج إلى الولايات المتحدة الأمريكية،" 25 سبتمبر 2015، *https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states*.

84. جامعة تورنتو، "4: قمة بريكس 2015 إعلان أوفا،" مركز معلومات بريكس، 9 يوليو 2015، *http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html*.

85. الأمم المتحدة، الجمعية العامة، "رسالة بتاريخ 9 يناير 2015 من الممثلين الدائمين للصين، وكازاخستان، وقيرغستان، والاتحاد الروسي، وطاجاكستان، وأوزبكستان إلى الأمم المتحدة موجهة إلى الأمين العام، "التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، A/69/723 (13 يناير 2015)، *http://daccess-dds-ny.un.org/doc/PDF//02/014/UNDOC/GEN/N15/N1501402.pdf?OpenElement*.

86. ميليسا هاثاواي، "ورقة نقاش للجنة العالمية لحكومة الإنترنت،" (ورقة قُدمّت في ستوكهولم السويد، 27 مايو 2014).

87. بنك التنمية للدول الأمريكية، "بنك التنمية للدول الأمريكية ومنظمة الدول الأمريكية يوحدان جهودهما للترويج لسياسات أفضل للأمن الإلكتروني في أمريكا اللاتينية والكاريبي، "22 أكتوبر 2014، *http://www.iadb.org/en/news/news-releases/2014-10-22/cybersecurity-workshop-for-latin-america,10957.html*.

88. دوسان نافراتيل، مدير السلطة الوطنية الأمنية لجمهورية التشيك وروبرت كاهوفر، المساعد الخاص، " Cyber Czech 2015 – تمرين وطني في مجال الأمن الإلكتروني التقني،" (مقابلة بواسطة ميليسا هاثاواي

في واشنطن العاصمة، أكتوبر 2015) ورويوفن أزار، نائب رئيس البعثة ود. إيفياتار ماتانيا، مدير المكتب الإلكتروني الوطني (مقابلة بواسطة ميليسا هاثاواي في روكفيل، ماريلاند، 2 يونيو 2015).

89. كري غال. هول، القنصل العام الأمريكي، الهند، (مقابلة بواسطة ميليسا هاثاواي في كولكاتا، الهند، 23 سبتمبر 2015).

90. يختلف الصراع الإلكتروني عن الحرب الإلكترونية أو المعركة الإلكترونية. فالنوع الثاني تكنولوجي بحت وبالإمكان إجراؤه بالكامل، من ناحية المبدأ، داخل الشبكة. وهو في العادة عنصر من عناصر النوع الأول. الصراعات الإلكترونية هي الصراعات العدوانية والتخريبية التي يكون لها أثر كبير على صعيد الدولة بشكل لا يمكن فيه للأحداث التي تحدد النتيجة المستقبلية أن تحدث دون آليات "إلكترونية" (أي تقنيات متصلة بالشبكات) في منعطفات حساسة تقرر مسار الأحداث. كريس ديمتشاك، "المرونة، التعطيل، و"ويستفاليا الإلكترونية": خيارات للأمن الوطني في عالم النزاعات الإلكترونية،" في تأمين الفضاء الإلكتروني: مجال جديد للأمن الوطني، تحرير نيكولاس بيرنز وجوناثان برايس، (واشنطن، العاصمة: معهد أسبن، 2012).

91. كريستوفر برونك، "الهجوم الإلكتروني على أرامكو السعودية،" Survival 55 (أبريل-مايو 2013) 81-96.

92. ميليسا هاثاواي وجون سيتوارت، "المقالة الإلكترونية الخاصة رقم 4: السيطرة على المستقبل الإلكتروني،" مجلة جورجتاون للشؤون الدولية (25 يوليو 2014).

93. روبرت ام. لي، مايكل جيه. أسانتي، وتيم كونواي، "الهجوم الإلكتروني على مصنع الصلب الألماني،" أنظمة السيطرة الصناعية (30 ديسمبر 2014).

94. "حقيقة اختراق سوني بكتشرز، " TrendMicro، 22 ديسمبر 2014، *http://blog.trendmicro.com/reality-sony-pictures-breach/*، شون فيتزجيرالد، "كل ما حصل في فضيحة تسريب معلومات سوني،" Vulture، 22 ديسمبر 2014، *http://www.vulture.com/2014/12/everything-sony-leaks-scandal.html#*، و "احتمالية كشف اختراق سوني لبيانات الرواتب والرعاية الصحية الخاصة بالموظفين،" *Krebson Security*، 2 ديسمبر 2014، *http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/*.

95. جينيفر فالنتينو-ديفريس وداني يادرون،" فهرسة القوى الإلكترونية في العالم، "وول ستريت جورنال، 11 أكتوبر 2015، *http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710* والأمم المتحدة، الجمعية العامة، التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي: تقرير للأمين العام، A/70/172 (22 يوليو 2015)، *http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172*.

96. جيمز لويس وكارتينا تيملين، "الأمن الإلكتروني والحرب الإلكترونية 2011: تقييم أولي للعقيدة الوطنية والتنظيم،" مصدر معهد الأمم المتحدة لبحوث نزع السلاح (UNIDIR) ومركز الدراسات الإستراتيجية والدولية (2011): 3.

97. وزارة الدفاع، "الإستراتيجية الإلكترونية لوزارة الدفاع،" (أبريل 2015): 7-8.

98. رئيس الاتحاد الروسي، " العقيدة العسكرية للاتحاد الروسي، "الحكومة الروسية (2014) ترجمة توماس مور، *https://www.scribd.com/doc/251695098/Russia-s-2014-Military-Doctrine*.

99. وزارة دفاع الاتحاد الروسي، "آراء مفاهيمية حول نشاطات القوات المُسلحة للاتحاد الروسي في فضاء المعلومات،" (2011) ترجمة وزارة الخارجية الأمريكية.

100. "العقيدة الجديدة لأمن المعلومات لفتت الانتباه لخطر زعزعة الاستقرار من خلال الإنترنت، "الأخبار الروسية، 10 سبتمبر 2015، *http://en.news-4-u.ru/the-new-doctrine-of-information-security-pointed-out-the-danger-of-destabilization-via-the-internet.html*.

101. أصدرت وزارة الدفاع البرازيلية كذلك مؤخراً تعليمات لهيئة الأركان المشتركة للقوات المسلحة (EMCFA) لتحسين الدفاع الإلكتروني الوطني من خلال إنشاء مركز قيادة للدفاع الإلكتروني ثلاثي الخدمات (ComDCiber). سيضم مركز ComDCiber جميع الخدمات الثلاث، وسيتولى الجيش قيادته. سيتم إنشاء ComDCiber استناداً إلى نواة مركز الدفاع الإلكتروني البرازيلي (NU CDCiber) الذي تم إنشاؤه في وقت سابق في برازيليا. أنظر إيلينجو جيفارا، "البرازيل تنوي تأسيس مركز قيادة إلكترونية،" IHS Jane's Defence Weekly، 4 نوفمبر 2014 وديبغو رافايل كانابارو وتياغو بورن، "البرازيل وضباب الحرب (الإلكترونية)،" المركز الوطني للحوكمة الرقمية (2013): 5. بالنسبة للقدرات الإلكترونية لكوريا، أنظر: جمهورية كوريا، "الورقة البيضاء للدفاع،" (2014)، 57، *http://www.mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_201506161156164570.pdf*.

102. زاكاري كيك، "كوريا الجنوبية تسعى للحصول على قدرات إلكترونية هجومية،" TheDiplomat، 11 أكتوبر، 2014، *http://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/*.

103. للاطلاع على نظرة عامة لإستراتيجية الصين الإلكترونية، أنظر: آمي تشانغ، "الدول المتحاربة،" مركز الأمن الأمريكي الجديد، (ديسمبر 2014).

104. المكتب الإعلامي للدولة، "الورقة البيضاء: التوظيف المتنوع للقوى المسلحة الصينية،" أبريل 2013، *http://eng.mod.gov.cn/Database/WhitePapers/* وتشي جينبينج، اللجنة العسكرية المركزية، "رأي حول تعزيز قوة العمل الأمني للمعلومات العسكرية،" ترجمة جزئية من آمي تشانغ، "الدول المتحاربة،" مركز الأمن الأمريكي الجديد، (ديسمبر 2014): 20

105. المدراء العامين للمجلس الشمالي، "المسؤوليات الإلكترونية الأيسلندية،" (لقاء بين ميليسا هاثاواي والمدراء العامين ووفود المجلس الشمالي المسؤولين عن الفرق الوطنية للاستجابة لطوارئ الحاسوب، ستوكهولم، 19 نوفمبر، 2014).

106. وزير الداخلية، "الإستراتيجية الوطنية الأيسلندية للأمن الإلكتروني 2015-2026: خطة عمل،" وزير الداخلية الأيسلندي (يونيو 2015)، *http://eng.innanrikisraduneyti.is/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf*.

107. ياكوف كاتز، الأمن والدفاع،" The Jerusalem Post، 8 أكتوبر 2010 في جيمس لويس وكارتينا تيملين، "الأمن الإلكتروني والحرب الإلكترونية 2011: تقييم أولي للعقيدة الوطنية والتنظيم،" مصدر معهد الأمم المتحدة لبحوث نزع السلاح (UNIDIR) ومركز الدراسات الإستراتيجية والدولية (2011)، 14 و "عين على الصادرات التقنية، إسرائيل تُطلق مركز للقيادة الإلكترونية،" رويترز، 18 مايو 2011، *http://www.reuters.com/article/2011/05/18/us-israel-security-cyber-idUSTRE74H27H20110518*.

108. ميتش جينسبرغ، "الجيش سيؤسس قوات إلكترونية موحدة،" The Times of Israel، 16 يونيو، 2015

109. مايكل هيرزوج، "نشر الإستراتيجية الجديدة لجيش الدفاع الإسرائيلي بشكل علني،" معهد واشنطن: مرصد السياسات 2479 (28 أغسطس 2015)، *http://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public*.

المؤلفون

ميليسا هاثاواي هي واحدة من الخبراء الرائدين في مجال سياسة الفضاء الإلكتروني والأمن الإلكتروني. وهي تشغل منصب زميل أول وعضو في مجلس الأوصياء في معهد بوتوماك للدراسات السياسية وهي مستشارة أولى في مركز بلفر للعلوم والشؤون الدولية التابع لكلية كينيدي في هارفارد. وهي أيضاً زميلة متميزة في مركز ابتكار الحوكمة الدولية في كندا وتم تعيينها لتكون عضوة في اللجنة الدولية لحكومة الإنترنت (لجنة بيلدت). كما خدمت في إدارتين رئاسيتين حيث ترأست مراجعة سياسة الفضاء الإلكتروني للرئيس باراك أوباما وقادت المبادرة الشاملة للأمن الإلكتروني الوطني للرئيس جورج دبليو بوش. ولقد طوّرت منهجية فريدة لتقييم وقياس مستوى الجاهزية لبعض أنواع مخاطر الأمن الإلكتروني، وعُرفت هذه المنهجية باسم مؤشر الجاهزية الإلكترونية. وهي تؤلف منشورات منتظمة حول مسائل الأمن الإلكتروني التي تتأثر بها الشركات والدول. ويمكن الاطلاع على معظم مقالاتها على الموقع الإلكتروني التالي: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html*.

كريس دمتشاك هي خبيرة مجال مختصة في مشروع مؤشر الجاهزية الإلكترونية لمعهد بوتوماك للدراسات السياسية. وتشمل مجالات بحثها المرونة الرقمية، والنزاع الإلكتروني، وهياكل الفضاء الإلكتروني ومخاطره. ولقد صممت نموذج تنظيمي رقمي يُعرف باسم "Atrium" يساعد الشركات الكبرى على الاستجابة للمفاجئات في أنظمتها والتعامل معها. كما أنها مؤلفة «حروب التعطيل والمرونة: النزاع الإلكتروني، القوة والأمن الوطني».

جيسون كيربن هو خبير مجال مختص في مشروع مؤشر الجاهزية الإلكترونية لمعهد بوتوماك للدراسات السياسية. كما يعمل كمستشار أول لعدة وزارات ووكالات في المسائل المتعلقة بأمن المعلومات والأمن الإلكتروني. وهو يُركز، على وجه التحديد، على الأنظمة القانونية والتنظيمية التي تؤثر على مهام المنظمات. ويطوّر منهجيات وأساليب لتقييم وإدارة المخاطر الأمنية الإلكترونية ويقدم الاستشارات حول مجموعة ضخمة من النشاطات المُحددة في مجال الأمن الإلكتروني بما فيها المبادئ الدولية التي تحكم تقنيات المعلومات والاتصالات، والهوية وإدارة الوصول، والتشخيص المستمر والتخفيف من الآثار والتأمين الإلكتروني.

جينيفر مكأرديل هي زميلة في مركز الفكر العلمي الثوري في معهد بوتوماك للدراسات السياسية. وتُركّز أبحاثها الأكاديمية على الحرب الإلكترونية، وحرب المعلومات، والجغرافيا السياسية الآسيوية. وهي حالياً مُرشحة للحصول على درجة الدكتوراه في كلية كينجز كوليدج لندن في قسم دراسات الحروب.

فرانشسكا سبيداليريس هي خبيرة مجال مختصة في مشروع مؤشر الجاهزية الإلكترونية لمعهد بوتوماك للدراسات السياسية. كما تعمل أيضاً كزميلة أولى للقيادة الإلكترونية في مركز بيل، في جامعة سالفي ريجينا. وركّزت أبحاثها ومنشوراتها الأكاديمية على تطوير القيادة الإلكترونية، وإدارة المخاطر الإلكترونية، والتعليم والتوعية الإلكترونية، وتطوير القوى العاملة في مجال الأمن الإلكتروني. ولقد نشرت مؤخراً تقريراً بعنوان "وضع الولايات بالنسبة للأمن الإلكتروني،" طبقّت فيه مؤشر الجاهزية الإلكترونية 1.0 على مستوى الولايات المتحدة الأمريكية.

معهد بوتوماك للدراسات السياسية
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org