دليل لوضع استراتيجية وطنية للأمن السيبراني

التزام استراتيجي بالأمن السيبراني

ITU

CCDCOE

The Commonwealth Cybercrime Initiative

CTO

THE WORLD BANK

Deloitte.

Global Cyber Security Capacity Centre

GCSP

Microsoft

بعض الحقوق محفوظة

الحقوق والأُذون

شكر وعرفان

قام بوضع هذا الدليل اثنا عشر شريكاً من المنظمات الحكومية الدولية والمنظمات الدولية والقطاع الخاص وكذلك من الأوساط الأكاديمية والمجتمع المدني، ومن هذه المنظمات: أمانة الكومنولث (ComSec) ومنظمة الكومنولث للاتصالات (CTO) وشركة Deloitte ومركز جنيف لسياسات الأمن (GCSP) والمركز العالمي لقدرات الأمن السيبراني (GCSCC) في جامعة أكسفورد والاتحاد الدولي للاتصالات (ITU) وشركة Microsoft ومركز التميز التعاوني للدفاع السيبراني التابع لمنظمة حلف شمال الأطلسي (NATO CCD COE) ومعهد بوتوماك لدراسات السياسات وشركة RAND أوروبا والبنك الدولي ومؤتمر الأمم المتحدة للتجارة والتنمية (UNCTAD).

وضم الفريق كاتالاينا سابولو (ComSec) وشادراخ هارونا (ComSec) ومارتن كويابيه (CTO) وفارغاني تامبيايوك (CTO) وأندريا ريغوني (Deloitte) وكارولين فايسر (GCSCC) وماركو أوبيزو (ITU) وكاجا سيغليك (Microsoft) وكادري كاسكا (NATO CCD COE) وفرانشيسكا سبيداليري وميليسا هاثاواي (معهد بوتوماك لدراسات السياسات) وإريك سيلفرستين (RAND أوروبا) وديفيد ساتولا وساندرا سارجنت (البنك الدولي) وسيسيل بارايريه (UNCTAD).

وقدمت الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA) مساهمة كبيرة لوضع الدليل.

ويُعترف أيضاً بمساهمات كل من: غريس أكايو وروشين أفوتار ماوري وبن بيسيلي والكر وبول كورنش ولوك داندوراند ومايكل غولدسميث وكمال حسينوفتش وأندراس أندي كاستيليتش ومكسيم كوشتويف ولينا لاتيون وغوستاف ليندستروم وداميان مادالينا وإميلي مونرو ولارا بيس وسارة بويلو ألفونسو وفاليريا ريزوليا وتايلور روبرتس ومونيكا م. رويز وأيرين روبيو وآن فالياتاغا وجوليين رايت.

تصدير

انه لمن دواعي سروري أن أقدم – نيابة عن الشركاء المعنيين – 'دليل الاستراتيجية الوطنية للأمن السيبراني' الذي يرمي إلى توفير مجموعة متآلفة ومتوائمة من المبادئ والممارسات الجيدة بشأن وضع استراتيجيات وطنية للأمن السيبراني وتنفيذها.

وقد قام الاتحاد بدور الميسّر، حيث اتفق اثنا عشر شريكاً من القطاعين العام والخاص والأوساط الأكاديمية والمجتمع المدني على تبادل ما يتمتعون به من خبرات ومعارف وتجارب بغية وضع دليل يجمع ما يتوفر من الدراية لدى المنظمات المشاركة، فضلاً عن توفير المراجع للمنشورات التكميلية من أجل تسهيل الوصول إلى الموارد المتاحة.

وقد استفاد، على مدى العقدين الماضيين، آلاف الملايين من الناس في شتى أنحاء العالم من النمو المتضاعف لتكنولوجيا المعلومات والاتصالات ومن سرعة اعتمادها ومن الفرص الاقتصادية والاجتماعية المرتبطة بها. ونحن نشهد اليوم ثورة رقمية تحول مجتمعاتنا تحويلاً جذرياً.

والأمن السيبراني عامل أساسي في تحقيق التنمية الاجتماعية والاقتصادية. ومع ذلك، ليس هنالك سوى ستة وسبعون بلداً[1] حول العالم لديها استراتيجيات وطنية للأمن السيبراني متاحة للجميع. ولذلك من الأهمية بمكان تعزيز الجهود المبذولة لوضع هذه الاستراتيجيات. وكما يُستشف من العنوان، فإن الهدف من هذا الدليل هو استثارة التفكير الاستراتيجي ومساعدة القادة الوطنيين وواضعي السياسات في وضع استراتيجيات وطنية للأمن السيبراني وتنفيذها.

وأنا واثق من أن 'دليل الاستراتيجية الوطنية للأمن السيبراني' سوف يكون أداة مفيدة لدى جميع أصحاب المصلحة الذين يضطلعون بمسؤوليات في مجال الأمن السيبراني. وأود أن أعرب شخصياً عن امتناني للشركاء لما قدموه من دعم والتزام دائب وقيّم لكي يكلّل هذا المشروع بالنجاح كمثال ملموس للتعاون الناجح بين أصحاب المصلحة المتعددين.

براهيما سانو
مدير مكتب تنمية الاتصالات، الاتحاد الدولي للاتصالات

[1] بحسب الرقم القياسي العالمي للأمن السيبراني (GCI)، الاتحاد الدولي للاتصالات، 2017

جدول المحتويات

تمهيد

'دليل الاستراتيجية الوطنية للأمن السيبراني' هو واحد من أكثر الاستعراضات شمولاً لما يشكل استراتيجيات ناجحة للأمن السيبراني. وهو نتيجة لجهد تعاوني فريد ومتكافئ من جانب أصحاب المصلحة المتعددين، يستفيد من معارف وخبرات وتجارب العديد من المنظمات في مجال استراتيجيات وسياسات الأمن السيبراني الوطنية. وعلى وجه التحديد، قام بإعداد هذا الدليل اثنا عشر شريكاً من القطاعين العام والخاص، ومن الأوساط الأكاديمية والمجتمع المدني.

وأقدم الشركاء على هذا العمل من منطلق تقديرهم لضرورة تعزيز التعاون والتنسيق بين جميع الأطراف في المجتمع الدولي بشأن بناء القدرات في مجال الأمن السيبراني. والغرض من هذا الجهد هو دعم القادة الوطنيين وواضعي السياسات في وضع خطط دفاعية لمواجهة التهديدات السيبرانية، في شكل استراتيجية وطنية للأمن السيبراني، وفي التفكير استراتيجياً بشأن الأمن السيبراني والتأهب السيبراني والتصدي والصمود، وبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.

لقد وُضع 'دليل الاستراتيجية الوطنية للأمن السيبراني' من خلال نهج تكراري كان الغرض منه التوصل إلى اتفاق من خلال توافق الآراء. وهو يستند إلى الموارد المتوفرة ويرمي إلى تسهيل استخدامه من جانب أصحاب المصلحة الوطنيين. وحيثما أمكن، أدرجت المصادر والأدوات ذات الصلة المستخدمة لوضع كل مجموعة من التوصيات في قسم المراجع للتشجيع على استخدامها على نطاق أوسع.

والأمن السيبراني عنصر أساسي في تحقيق الأهداف الاجتماعية الاقتصادية التي تتوخاها الاقتصادات الحديثة. والأمل هو أن يكون 'دليل الاستراتيجية الوطنية للأمن السيبراني' أداة مفيدة لجميع أصحاب المصلحة، بمن فيهم واضعو السياسات الوطنية والمشرعون والهيئات التنظيمية، ممن يضطلع بمسؤوليات في مجال الأمن السيبراني. وبالإضافة إلى ذلك، قد يكون الدليل قابلاً للتطبيق على نطاق أوسع، إذ يمكن تطبيق المفاهيم على المستويات الإقليمية، أو البلدية، فضلاً عن تكييفها لدوائر الصناعة.

1 لمحة عامة عن الدليل

1.1 الغرض

الغرض من هذا الدليل هو توجيه القادة الوطنيين وواضعي السياسات لدى وضع استراتيجية وطنية للأمن السيبراني ولدى التفكير استراتيجياً بشأن الأمن السيبراني والتأهب السيبراني والصمود.

ويهدف هذا الدليل إلى وضع إطار مفيد ومرن وسهل الاستخدام لتحديد سياق رؤية البلد الاجتماعية–الاقتصادية والموقف الأمني الراهن ولمساعدة واضعي السياسات في رسم استراتيجية تأخذ في الاعتبار الوضع الخاص للبلد والقيم الثقافية والمجتمعية وللتشجيع على تحقيق الأمن والصمود وتطوير مجتمعات موصولة معززة بتكنولوجيا المعلومات والاتصالات.

والدليل مورد فريد، فهو يوفر إطاراً اتفقت عليه منظمات ذات خبرة واضحة ومتنوعة في هذا المجال، وهو يستند إلى أعمالها السابقة في هذا الصدد. ومن ثم فهو يقدم أحدث نظرة شاملة حتى الآن عما يشكل الاستراتيجيات الوطنية الناجحة في مجال الأمن السيبراني.

2.1 النطاق

يمثل الأمن السيبراني تحدياً معقداً يشمل العديد من الجوانب المختلفة للحوكمة والسياسة والجوانب التشغيلية والتقنية والقانونية. ويسعى هذا الدليل إلى تناول العديد من هذه المجالات وتنظيمها وترتيب أولوياتها بناء على نماذج وأطر ومراجع أخرى قائمة ومعترف بها.

ويركز الدليل على حماية الجوانب المدنية للفضاء السيبراني، ومن ثم فهو يسلط الضوء على المبادئ الشاملة والممارسات الجيدة التي يتعين النظر فيها في عملية صوغ استراتيجية وطنية للأمن السيبراني ووضعها وإدارتها.

ولهذه الغاية، يميز الدليل تمييزاً واضحاً بين ''العملية'' التي تعتمدها البلدان طوال دورة حياة الاستراتيجية الوطنية للأمن السيبراني (الاستهلال والتقييم والتحليل والإنتاج والتنفيذ والاستعراض) و''المحتوى''، أي النص الفعلي الذي سوف يظهر في وثيقة الاستراتيجية الوطنية للأمن السيبراني. ولا يشمل الدليل جوانب من قبيل تطوير القدرات السيبرانية الدفاعية أو الهجومية من جانب الجيش أو قوات الدفاع أو وكالات الاستخبارات في البلد، رغم قيام عدد من البلدان بتطوير هذه القدرات.

ورغبة في توفير التوجيه والممارسات الجيدة بشأن ''ما'' ينبغي تضمينه في الاستراتيجية الوطنية للأمن السيبراني، وبشأن ''كيفية'' وضع الاستراتيجية وتنفيذها واستعراضها، يتناول هذا الدليل كلا العنصرين.

ويوفر الدليل أيضاً لمحة عامة عن المكونات الأساسية لما يتطلبه الأمر لكي يصبح البلد متأهباً سيبرانياً، ويسلط الضوء على الجوانب الحرجة التي ينبغي للحكومات مراعاتها عند وضع استراتيجياتها الوطنية وخطط تنفيذها.

وأخيراً، يقدم هذا الدليل لواضعي السياسات استعراضاً شاملاً رفيع المستوى للنُهُج والتطبيقات القائمة، ويشير إلى الموارد الإضافية والتكميلية التي يمكن أن تساعد في جهود الأمن السيبراني الوطنية المحددة.

3.1 الهيكل العام للدليل واستخدامه

تم تنظيم هذا الدليل في المقام الأول كمورد لمساعدة أصحاب المصلحة الحكوميين في إعداد وصوغ وإدارة الاستراتيجية الوطنية للأمن السيبراني الخاصة بهم. ومن ثم تم تنظيم المحتوى لمتابعة عملية وترتيب وضع الاستراتيجية:

- القسم 2 – مقدمة: توفر لمحة عامة عن موضوع الدليل مع التعاريف ذات الصلة؛
- القسم 3 – دورة حياة وضع الاستراتيجية: تفصّل الخطوات في وضع الاستراتيجية وإدارتها طوال كامل دورة حياتها؛
- القسم 4 – المبادئ الشاملة للاستراتيجية: تحدد الاعتبارات الأساسية الشاملة التي يتعين أن تؤخذ في الاعتبار أثناء وضع الاستراتيجية؛
- القسم 5 – مجالات التركيز والممارسات الجيدة: تحدد العناصر والمواضيع الرئيسية التي ينبغي النظر فيها أثناء وضع الاستراتيجية؛
- القسم 6 – المواد المرجعية الداعمة: توفر مؤشرات أخرى للأدبيات ذات الصلة التي يمكن لأصحاب المصلحة استعراضها كجزء من جهود الصياغة.

وعلى وجه الخصوص، يتناول القسم 3 العملية والجوانب المتعلقة بوضع الاستراتيجية الوطنية للأمن السيبراني (مثل الإعداد والصياغة والتنفيذ والاستدامة الطويلة الأجل)، بينما يركز القسمان 4 و5 على محتوى الاستراتيجية الوطنية للأمن السيبراني، ذلك لأنهما يسلطان الضوء على المفاهيم والعناصر التي ينبغي أن تضمها الوثيقة.

4.1 الجمهور المستهدف

يستهدف هذا الدليل أولاً وقبل كل شيء واضعي السياسات المسؤولين عن وضع الاستراتيجية الوطنية للأمن السيبراني. أما الجمهور الثاني المستهدف فهو جميع أصحاب المصلحة الآخرين من القطاعين العام والخاص المشاركين في وضع وتنفيذ الاستراتيجية، ومنهم المسؤولون الحكوميون والهيئات التنظيمية وهيئات إنفاذ القانون ومقدمو خدمات تكنولوجيا المعلومات والاتصالات ومشغلو البُنى التحتية الحرجة والمجتمع المدني والأوساط الأكاديمية ومؤسسات البحوث. ويمكن أن يثبت الدليل فائدته أيضاً لدى مختلف أصحاب المصلحة في مجتمع التنمية الدولي الذين يقدمون المساعدة في مجال الأمن السيبراني.

2 مقدمة

استفاد على مدى العقدين الماضيين آلاف الملايين من الناس في شتى أنحاء العالم من النمو المتضاعف ومن سرعة اعتماد تكنولوجيا المعلومات والاتصالات ومن الفرص الاقتصادية والاجتماعية المرتبطة بها.

لقد تطورت الإنترنت، منذ نشأتها، من منصة لتبادل المعلومات إلى أن أصبحت العمود الفقري لأنشطة الأعمال الحديثة والخدمات والبُنى التحتية الحرجة والشبكات الاجتماعية والاقتصاد العالمي إجمالاً. ونتيجة لذلك، شرع القادة الوطنيون في وضع الاستراتيجيات الرقمية وتمويل المشاريع التي تعزز التوصيلية بالإنترنت والاستفادة من الفوائد الناجمة عن استخدام تكنولوجيا المعلومات والاتصالات لتحفيز النمو الاقتصادي وزيادة الإنتاجية والكفاءة وتحسين الخدمات والقدرات وتوفير النفاذ إلى أنشطة الأعمال والمعلومات وتمكين التعلم الإلكتروني وتعزيز مهارات القوى العاملة وتعزيز الحوكمة الرشيدة. و لم يعد بمقدور البلدان أن تتجاهل الفرص المرتبطة بالتوصيلية والمشاركة في اقتصاد الإنترنت.

وإذ يتزايد اعتماد مجتمعاتنا على البنية التحتية الرقمية فإن التكنولوجيا ما زالت بطبيعتها عرضة للتأثر. حيث تتعرض سرية البنية التحتية لتكنولوجيا المعلومات والاتصالات وسلامتها وتوفرها للتهديدات السيبرانية السريعة التطور، بما في ذلك الاحتيال الإلكتروني وسرقة الملكية الفكرية والمعلومات الشخصية القابلة للتعرف وتعطيل الخدمات وإتلاف الممتلكات أو تدميرها. وقد بلغت القوة التحويلية لتكنولوجيا المعلومات والاتصالات والإنترنت كحافز للنمو الاقتصادي والتنمية الاجتماعية نقطة حرجة حيث بدأت تتآكل ثقة المواطنين والثقة الوطنية في استخدام تكنولوجيا المعلومات والاتصالات جراء انعدام الأمن السيبراني.

وحرصاً على الاستفادة الكاملة من إمكانات التكنولوجيا، يتعين على الدول مواءمة رؤيتها الاقتصادية الوطنية مع أولويات أمنها الوطني. وإذا لم تتحقق موازنة المخاطر الأمنية المرتبطة بانتشار البنية التحتية المتمكنة من تكنولوجيا المعلومات والاتصالات وتطبيقات الإنترنت بشكل ملائم مع استراتيجيات الأمن السيبراني الوطنية الشاملة وخطط الصمود فلن تتمكن البلدان من تحقيق النمو الاقتصادي وبلوغ أهداف الأمن الوطني التي تسعى إليها.

واستجابة لذلك، تقوم البلدان بتطوير قدرات هجومية ودفاعية للوقاية من الأنشطة غير المشروعة وغير القانونية في الفضاء السيبراني واستباق الأحداث قبل أن تلحق الضرر بشعوبها. وتبحث هذه الوثيقة تحديداً في المبادرات الدفاعية، لاسيما في شكل استراتيجيات وطنية للأمن السيبراني.

ومن خلال وضع وتنفيذ استراتيجية وطنية للأمن السيبراني، يمكن للبلد أن يحسّن من أمن بنيته التحتية الرقمية وأن يسهم في نهاية المطاف في تحقيق تطلعاته الاجتماعية الاقتصادية الأوسع. ويتعين على القادة الوطنيين أن يتبعوا استراتيجية بشأن الفرص المتاحة والمخاطر التي تتعرض لها بلدانهم بسبب البيئة الرقمية، كما يتعين أن تكون لديهم رؤية واضحة للمستقبل الرقمي الذي يتطلعون إليه.

1.2 ما هو الأمن السيبراني

هنالك عدد من التعاريف الوطنية والدولية لمصطلح "الأمن السيبراني". ولأغراض هذه الوثيقة، يُقصد من مصطلح "الأمن السيبراني" وصف مجموعة الأدوات والسياسات والمبادئ التوجيهية وثُهُج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتقنيات التي يمكن استخدامها في حماية توفر وسلامة وسرية الأصول في البنى التحتية الموصولة التابعة للحكومة والمنظمات الخاصة والمواطنين، وتشمل هذه الأصول أجهزة الحوسبة الموصولة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات والبيانات في البيئة السيبرانية.[2]

2.2 فوائد الاستراتيجية الوطنية للأمن السيبراني وعملية وضع الاستراتيجية

قد تأخذ الاستراتيجيات الوطنية للأمن السيبراني أشكالاً متعددة وقد تكون على درجات متفاوتة من التفصيل تبعاً لأهداف ومستويات التأهب السيبراني في كل بلد. ولذلك، ليس هنالك من تعريف محدد ومتفق عليه لما يشكل استراتيجية وطنية للأمن السيبراني.

واستناداً إلى البحوث القائمة في هذا المضمار، تشجع هذه الوثيقة أصحاب المصلحة على التفكير في استراتيجية وطنية للأمن السيبراني تكون بمثابة:

- تعبير عن الرؤية والأهداف والمبادئ والأولويات الرفيعة المستوى التي ترشد البلد في تناول مسألة الأمن السيبراني؛
- نظرة عامة تشمل أصحاب المصلحة المكلفين بتحسين الأمن السيبراني للبلد وأدوارهم ومسؤولياتهم؛
- وصف للخطوات والبرامج والمبادرات التي يضطلع بها البلد لحماية البنية التحتية السيبرانية لديه، ومن ثم لتعزيز أمنه وقدرته على الصمود.

ومن شأن تحديد الرؤية والأهداف والأولويات تمكين الحكومات من تناول مسألة الأمن السيبراني من منظور كلي عبر البيئة الرقمية الوطنية بدلاً من منظور قطاع أو هدف محدد أو تصدياً لخطر معين، لأن ذلك يمكّنها من التفكير استراتيجياً. وتختلف أولويات الاستراتيجيات الوطنية للأمن السيبراني من بلد لآخر، فإذا كان التركيز في بلد ما على التصدي للمخاطر المرتبطة بالبنية التحتية الحرجة، فقد يكون التركيز في بلد آخر على حماية الملكية الفكرية، وتعزيز الثقة في بيئة الإنترنت، أو تحسين الوعي بالأمن السيبراني لدى عامة الجمهور، أو مزيج من هذه المساعي.

[2] تعريف مقتبس من https://www.bcmpedia.org/wiki/Cyber_Security.

وتتسم الحاجة إلى تحديد ماهية الاستثمارات والموارد ومن ثم تحديد أولوياتها بأهمية حاسمة للنجاح في إدارة المخاطر في مجال شمولي مثل الأمن السيبراني.

كما توفر الاستراتيجية الوطنية للأمن السيبراني الفرصة لمواءمة أولويات الأمن السيبراني مع الأهداف الأخرى المتصلة بتكنولوجيا المعلومات والاتصالات. فالأمن السيبراني أمر أساسي لتحقيق الأهداف الاجتماعية الاقتصادية في الاقتصادات الحديثة وينبغي أن تعكس الاستراتيجية كيفية دعم هذه الأهداف. ويمكن القيام بذلك بالرجوع إلى السياسات القائمة التي تسعى إلى تنفيذ جداول الأعمال الرقمية أو التنموية للبلد أو بتقييم كيفية تضمين الأمن السيبراني فيها.

وأخيراً، يجب أن تترجم عملية وضع الاستراتيجية الوطنية للأمن السيبراني رؤية الحكومة إلى سياسات متماسكة وقابلة للتنفيذ خليقة بأن تساعدها في تحقيق أهدافها. وهذا لا يقتصر على الخطوات والبرامج والمبادرات التي ينبغي اتخاذها فحسب بل يشمل أيضاً الموارد المخصصة لهذه الجهود وكيف ينبغي استخدامها. وكذلك ينبغي أن تحدد العملية المقاييس التي تستخدم للمساعدة في ضمان تحقيق النواتج المرجوة في حدود الميزانيات والمواعيد الزمنية المقررة.

3 دورة حياة الاستراتيجية الوطنية للأمن السيبراني

يقدم هذا القسم لمحة عامة عن مختلف مراحل وضع الاستراتيجية والتي تشمل:

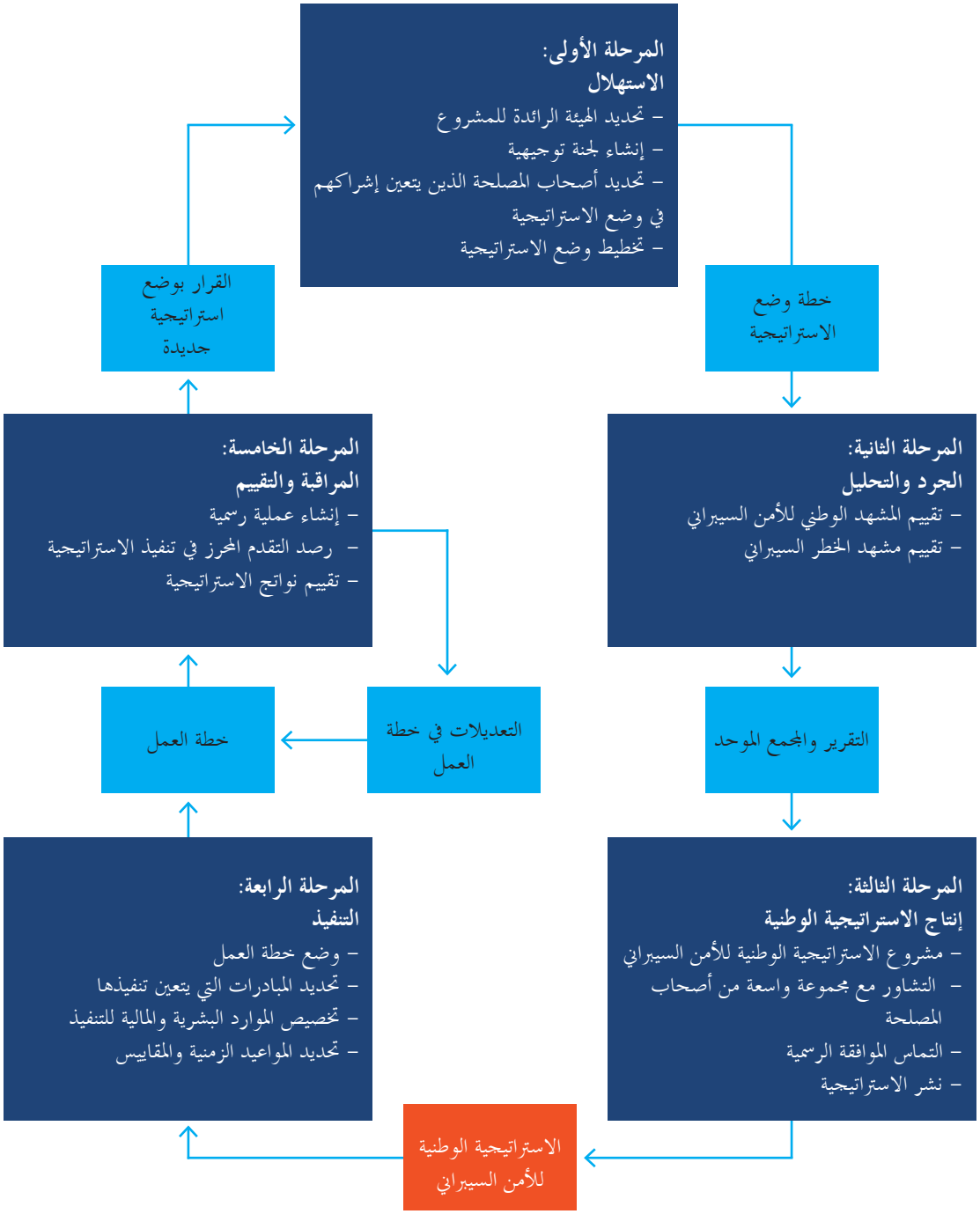
- المرحلة الأولى – الاستهلال
- المرحلة الثانية – الجرد والتحليل
- المرحلة الثالثة – الإنتاج
- المرحلة الرابعة – التنفيذ
- المرحلة الخامسة – المراقبة والتقييم

كما يتناول هذا القسم الكيانات الرئيسية التي ينبغي لها أن تشارك في وضع الاستراتيجية ويسلط الضوء على الجهات المعنية الأخرى التي يمكن أن تسهم في هذه العملية.

ويرمي هذا القسم في نهاية المطاف إلى تمكين القارئ من فهم الخطوات التي يتعين أن يتخذها البلد من أجل صوغ الاستراتيجية الوطنية والآليات الممكنة لتنفيذها وفقاً للاحتياجات والمتطلبات الخاصة بكل بلد، وذلك بتضمين المبادئ الشاملة (الواردة في القسم 4) والممارسات الجيدة (الواردة في القسم 5).

ومن شأن دورة الحياة هذه، كما هي موضحة في الشكل 1، أن ترشد مستعملي هذه الوثيقة في مجال التركيز على التفكير الاستراتيجي بشأن الأمن السيبراني على المستوى الوطني.

الشكل 1 – *دورة حياة الاستراتيجية الوطنية للأمن السيبراني*



1.3 المرحلة الأولى: الاستهلال

وفقاً لما جاء في القسمين 4 و5 من هذه الوثيقة، ترسي مرحلة استهلال الاستراتيجية الوطنية للأمن السيبراني الأسس اللازمة للكفاءة في وضعها. ومن المتوقع أن تركز هذه المرحلة على العمليات والمواعيد الزمنية وتحديد أصحاب المصلحة الرئيسيين الذين ينبغي أن يشاركوا في إنتاج الاستراتيجية. وحصيلة هذه المرحلة هي رسم خطة لوضع الاستراتيجية. وقد تتطلب الخطة، عندما تكون جزءاً من عملية الحوكمة، موافقة السلطة التنفيذية في البلد.[3]

1.1.3 تحديد الهيئة الرائدة للمشروع

تماشياً مع مبدأ تحديد القيادة الواضحة والأدوار وتخصيص الموارد (القسم 8.4)، ينبغي تنسيق عملية وضع الاستراتيجية من قبل هيئة مختصة واحدة. وينبغي للسلطة التنفيذية أن تعيّن هيئة عامة قائمة أو أن تنشئ هيئة جديدة، كوزارة أو وكالة أو إدارة، لقيادة عملية وضع الاستراتيجية. وينبغي لهذه الهيئة، المشار إليها في هذه الوثيقة بوصفها الهيئة الرائدة للمشروع، أن تعيّن بدورها شخصاً مسؤولاً عن تسيير عملية وضع الاستراتيجية.

وينبغي أن تكون الهيئة الرائدة للمشروع محايدة طوال عملية وضع الاستراتيجية. ولهذه الغاية، يوصى بأن تكون هذه الهيئة مختلفة عن الهيئة (أو الهيئات) التي سوف تضطلع بمسؤولية تنفيذ الاستراتيجية. وينبغي اعتماد هذه الآلية أو غيرها للتغلب على أي تحيز كامن والمساعدة على تجنب التنافس على الموارد بين دوائر الحكومة.

2.1.3 إنشاء لجنة توجيهية

ينبغي للسلطة التنفيذية أيضاً أن تنشئ لجنة توجيهية للعمل مع الهيئة الرائدة للمشروع في وضع الاستراتيجية. وينبغي تمكينها لتقديم التوجيه ولكي تنهض بدور في ضمان الجودة. وعلاوة على ذلك، ينبغي أن تضمن الشفافية والشمولية في العملية، وفقاً للمبدأ الخاص بالقيادة الواضحة والأدوار وتخصيص الموارد (القسم 8.4). وينبغي تحديد دور اللجنة التوجيهية وتركيبها وعضويتها بوضوح منذ البداية.

وبما أن اللجنة التوجيهية قد تحتاج إلى مراجعة وثائق حساسة، فينبغي تشكيلها وفقاً لذلك. ومن المهم أيضاً أن تعكس عضويتها مختلف المسؤوليات المسندة إلى هذه الهيئة، من خلال أقدمية التعيينات مثلاً.

[3] الفرد أو الهيئة المسؤولة عن عملية صنع القرار على المستوى الوطني.

3.1.3 تحديد أصحاب المصلحة للمشاركة في وضع الاستراتيجية

ينبغي للهيئة الرائدة للمشروع، في هذه الخطوة، تحديد مجموعة أولية من أصحاب المصلحة للمشاركة في وضع الاستراتيجية. كما ينبغي لها توضيح أدوار مختلف أصحاب المصلحة وتحديد كيفية تعاونهم من أجل إدارة التطلعات خلال العملية.

وقد يتعين على الهيئة الرائدة للمشروع، طوال هذه العملية، التواصل مع أصحاب مصلحة آخرين لضمان استخدام جميع المعارف والخبرات ذات الصلة. ويشمل ذلك مبدأ الشمولية (القسم 3.4) الذي يسلط الضوء على أهمية التعاون مع طائفة من أصحاب المصلحة في الحكومة والقطاع الخاص والمجتمع المدني. فقد تنظر الهيئة الرائدة للمشروع مثلاً في التواصل مع شركات تكنولوجيا المعلومات والاتصالات ومشغلي البنى التحتية الحرجة والخبراء الأكاديميين والمنظمات غير الحكومية التي تسعى إلى إذكاء الوعي بالأمن السيبراني والتأهب له، من بين أمور أخرى.

ويمكن أن تتخذ آلية التعاون هذه شكل لجنة استشارية تسهم في تزويد أعضاء للعمل في اللجنة التوجيهية، فضلاً عن استشارتها بشأن مختلف المراحل.

4.1.3 التخطيط لوضع الاستراتيجية

ينبغي للهيئة الرائدة للمشروع، في الخطوة النهائية من مرحلة الاستهلال، إعداد خطة لوضع الاستراتيجية الوطنية للأمن السيبراني. وبعد صوغ الخطة ينبغي تقديمها، حسب الاقتضاء، إلى اللجنة التوجيهية وإلى السلطة التنفيذية للموافقة عليها وفقاً لإجراءات الحوكمة الوطنية.

ولدى صوغ الخطة، ينبغي للهيئة الرائدة للمشروع أيضاً أن تنظر فيما إذا كانت الاستراتيجية الوطنية للأمن السيبراني سوف تتخذ شكل تشريعات أم سياسة، ذلك لأن خيارات مختلفة قد تؤثر على العمليات الرسمية التي يتعين اتباعها وكذلك على الإطار الزمني لاعتمادها.

وينبغي أن تحدد خطة وضع الاستراتيجية الخطوات والأنشطة الرئيسية وأصحاب المصلحة الرئيسيين والجداول الزمنية والمتطلبات من الموارد. وينبغي أن تحدد كيف ومتى يتوقع أن يشارك أصحاب المصلحة المعنيون في عملية وضع الاستراتيجية من أجل المساهمة بآرائهم وتعليقاتهم.

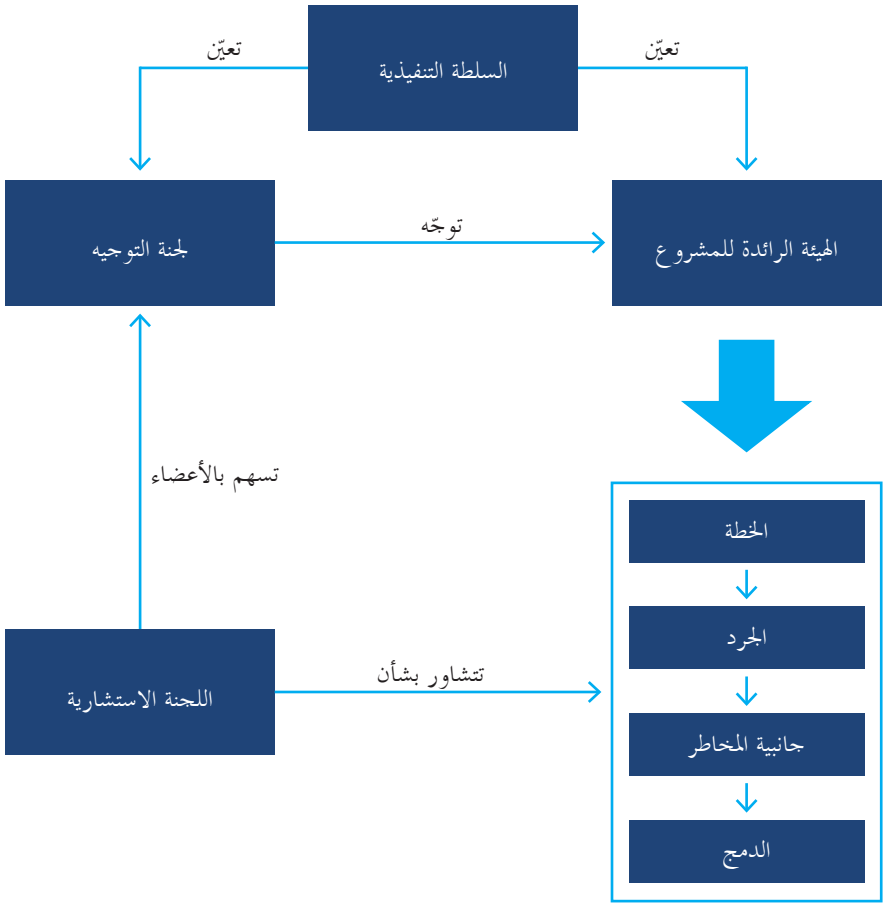
كما ينبغي أن تحدد الاستراتيجية الموارد البشرية والمالية اللازمة وأين يمكن الحصول عليها. حيث يمكن مثلاً التماس الخبرة المطلوبة من المنظمات الحكومية الدولية أو القطاع الخاص أو الأوساط الأكاديمية أو وكالات التنمية. وكذلك يمكن معالجة متطلبات التمويل من خلال إعادة توزيع تدفقات التمويل المخصصة في الميزانيات القائمة أو من خلال تمويل جديد متاح من أطراف ثالثة (المنظمات الدولية، مثلاً).

وينبغي إيلاء اهتمام خاص لضمان تمويل طويل الأجل لكامل دورة حياة الاستراتيجية الوطنية للأمن السيبراني، بما في ذلك وضعها وتنفيذها وتشذيبها. ولمزيد من التفاصيل بشأن تخصيص الموارد للتنفيذ، يرجى الاطلاع على ''تخصيص الموارد البشرية والمالية للتنفيذ'' (القسم 3.4.3) ولمزيد من التفاصيل بشأن التمويل طويل الأجل، يرجى الاطلاع على ''تخصيص الميزانية والموارد المخصصة'' (القسم 5.1.5).

ويبين الشكل 2 التفاعلات الممكنة وتوزيع الأدوار بين مختلف أصحاب المصلحة واللجان.

ثمة المزيد من المراجع في الصفحة 55.

الشكل 2 – *أصحاب المصلحة*



2.3 المرحلة الثانية: الجرد والتحليل

الغرض من هذه المرحلة هو جمع البيانات لتقييم المشهد الوطني للأمن السيبراني والمشهد الحالي والمقبل للخطر السيبراني تمهيداً لصوغ الاستراتيجية الوطنية للأمن السيبراني ووضعها. وينبغي أن يكون ناتج هذا التمرين عبارة عن تقرير يقدم لمحة عامة عن الموقف الوطني الاستراتيجي للأمن السيبراني ومشاهد الخطر التي يتعين تقديمها إلى اللجنة التوجيهية.

وقبل البدء في الإنتاج الحالي للنص، ينبغي أن تعكف الهيئة الرائدة للمشروع على تحليل وتقييم المعلومات التي جمعت أثناء مرحلة التقييم للتأكد من استبانة أي ثغرات في قدرات الأمن السيبراني وتقديم خيارات للتعامل معها. وينبغي أن يفضي التحليل إلى تقييم مدى تلبية السياسات الحالية والبيئات التنظيمية والتشغيلية للأهداف المعلنة للاستراتيجية وإبراز مواطن القصور فيها.

وكذلك، ينبغي استخدام هذه المرحلة لاستبانة القضايا الرئيسية المحددة، مثل الفجوات التعليمية والتدريبية.

وأخيراً، ينبغي أن يؤدي التحليل إلى تقييم لجميع النواتج المرجوة ذات الصلة للاستراتيجية، فضلاً عن الآثار والنواتج المحتملة للوسائل المختارة.

ثمة المزيد من المراجع في الصفحة 55.

1.2.3 تقييم المشهد الوطني للأمن السيبراني

حرصاً على فعالية الاستراتيجية الوطنية للأمن السيبراني، ينبغي لها أن تعكس الوضع السيبراني للبلد. ولهذه الغاية، ينبغي إجراء تحليل لمواطن القوة والضعف في الأمن السيبراني الراهن في البلد، وينبغي استشارة المواد والوثائق ذات الصلة بالتعاون مع أصحاب المصلحة المعنيين في مختلف دوائر الحكومة والقطاع الخاص والمجتمع المدني. وينبغي أن تتضمن هذه الخطوة مبدأ النهج الشامل والأولويات المخصصة (الوارد في القسم 2.4).

وكجزء من هذه الجهود، ينبغي أن تقوم الهيئة الرائدة للمشروع بتحديد الأصول والخدمات الحيوية لأداء المجتمع والاقتصاد على نحو سليم، وجرد القوانين والأنظمة والسياسات والبرامج والقدرات الوطنية القائمة من حيث صلتها بالأمن السيبراني. كما ينبغي للهيئة الرائدة للمشروع تحديد الآليات التنظيمية الحالية اللينة، مثل الشراكات بين القطاعين العام والخاص، وجرد القدرات التي طورت لمواجهة تحديات الأمن السيبراني، مثل الأفرقة الوطنية للاستجابة للطوارئ الحاسوبية (CERTs). وعلاوة على ذلك، ينبغي استبانة وجرد الأدوار والمسؤوليات التي تضطلع بها الوكالات العامة القائمة التي لها ولاية في مجال الأمن السيبراني، مثل الهيئات التنظيمية أو وكالات حماية البيانات.

وبالإضافة إلى ذلك، ينبغي جمع البيانات ذات الصلة التي يمكنها وصف وضع الأمن السيبراني في البلد. ويمكن أن يشمل ذلك: معلومات عن برامج الأمن السيبراني الوطنية القائمة والمبادرات الدولية ومشاريع

القطاع الخاص وتكنولوجيا المعلومات والاتصالات وبرامج التثقيف السيبراني وتنمية المهارات ومبادرات البحث والتطوير في المجال السيبراني، وبيانات عن تغلغل الإنترنت ومعدلات انتشار الفيروسات، والإقبال على تكنولوجيا المعلومات والاتصالات والتطورات التكنولوجية، واستشراف اتجاهات المستقبل لتكنولوجيا المعلومات والاتصالات وتهديدات الأمن السيبراني.

وينبغي أن يتضمن هذا التحليل أيضاً المعلومات ذات الصلة المستقاة من القطاع الخاص ومؤسسات البحوث وغيرها من جماعات أصحاب المصلحة. وبالنسبة للبلدان النامية، من الأهمية أيضاً جرد المبادرات التعاونية مع شركاء التنمية لتنسيق المساعدة التقنية والاستثمارات.

وأخيراً، ينبغي أن تقوم الهيئة الرائدة للمشروع بتقصي معلومات مماثلة على المستويين الإقليمي والدولي، وأن تنظر في الاستراتيجيات والمبادرات الخاصة بكل قطاع.

2.2.3 تقييم مشهد المخاطر السيبرانية

بناءً على المعلومات التي جمعت في الخطوة السابقة، ينبغي أن تعمد الهيئة الرائدة للمشروع إلى تقييم المخاطر التي تتهدد البلد بسبب التبعية الرقمية. ويمكن تحقيق ذلك من خلال تحديد الأصول الرقمية الوطنية، العامة منها والخاصة، وعلاقات الترابط بينها ومواطن الضعف والتهديدات وتقدير احتمال وقوع حادث سيبراني وأثره المحتمل.

وتشمل هذه الجهود مبدأ إدارة المخاطر والصمود (القسم 6.4) الذي يقر بأن إدارة المخاطر أمر بالغ الأهمية للاستفادة الكاملة من البيئة الرقمية لصالح التنمية الاجتماعية والاقتصادية. وعلاوة على ذلك، يمكن أن يشكل تقييم المخاطر الأولي هذا الأساس لتقييمات المخاطر المقبلة الأكثر تحديداً (ثمة المزيد من المعلومات عن مبدأ إدارة المخاطر والصمود وكيفية تقييم المخاطر في القسم 2.5).

3.3 المرحلة الثالثة: إنتاج الاستراتيجية الوطنية للأمن السيبراني

الغرض من هذه المرحلة هو وضع نص الاستراتيجية بإشراك أصحاب المصلحة الرئيسيين من القطاع العام والقطاع الخاص والمجتمع المدني من خلال سلسلة من المشاورات العمومية وأفرقة العمل. وستكون هذه المجموعة الأوسع من أصحاب المصلحة، التي تنسقها الهيئة الرائدة للمشروع، مسؤولة عن تحديد الرؤية الشاملة ونطاق الاستراتيجية وتحديد الأهداف عالية المستوى وتقييم الوضع الراهن (المفصل في المرحلة الثانية) وتحديد أولويات الأهداف من حيث الأثر على المجتمع والمواطنين والاقتصاد وضمان توفر الموارد المالية اللازمة. وكجزء من هذه المرحلة، ينبغي النظر في جميع المبادئ الشاملة (القسم 4) وفي عناصر الممارسات الجيدة (القسم 5) المفصلة في هذا الدليل.

1.3.3 صوغ الاستراتيجية الوطنية للأمن السيبراني

بعد اكتمال مرحلة الجرد والتحليل، ينبغي أن تبدأ الهيئة الرائدة للمشروع، بالتعاون مع اللجنة التوجيهية، في صوغ الاستراتيجية. ويمكن إنشاء أفرقة عمل مخصصة إما للتركيز على مواضيع محددة أو لصوغ أقسام مختلفة من الاستراتيجية. وينبغي أن تتبع أفرقة العمل العمليات المحددة في مرحلة الاستهلال، مع تعديل هذه العمليات حسب الضرورة.

وينبغي أن توفر الاستراتيجية التوجيه العام للأمن السيبراني للبلد، وأن تعبّر عن رؤية واضحة ونطاق واضح، وأن تحدد الأهداف التي يتعين بلوغها في إطار زمني محدد، وأن تحدد أولويات هذه الأهداف من حيث الأثر على المجتمع والاقتصاد والبنية التحتية. وعلاوة على ذلك، ينبغي لها أن تحدد مسارات العمل الممكنة، وأن تحفز جهود التنفيذ، وأن تدفع تخصيص الموارد اللازمة لدعم جميع هذه الأنشطة. وقد تتضمن الاستراتيجية أيضاً بعض النتائج التي تم التوصل إليها في مرحلة الجرد والتحليل.

وعلى غرار الخطوة المتعلقة بالتخطيط لوضع الاستراتيجية، ينبغي أن تضع الوثيقة إطار عمل واضح للحوكمة (القسم 1.5) يحدد أدوار ومسؤوليات أصحاب المصلحة الرئيسيين. ويشمل ذلك تحديد الهيئة المسؤولة عن إدارة وتقييم الاستراتيجية، إلى جانب هيئة مسؤولة عن إدارتها العامة وتنفيذها، من قبيل سلطة مركزية أو مجلس وطني للأمن السيبراني.

كما يتعين أن تحدد الاستراتيجية أو تؤكد ولاية مختلف الهيئات المسؤولة عن استهلال ووضع سياسات ولوائح الأمن السيبراني داخل البلد. وبالإضافة إلى ذلك، ينبغي أن تحدد مسؤوليات ومهام الهيئات المسؤولة عن جمع معلومات التهديد ومواطن الضعف والتصدي للحوادث السيبرانية (الأفرقة الوطنية للاستجابة للطوارئ الحاسوبية مثلاً) وتعزيز التأهب وإدارة الأزمات. كما ينبغي أيضاً أن تحرص على أن يكون من الواضح كيف تتفاعل كل هذه الكيانات فيما بينها ومع السلطة المركزية.

2.3.3 التشاور مع طائفة واسعة من أصحاب المصلحة

سبق أن ذُكر أعلاه أن إشراك أصحاب المصلحة أمر حاسم الأهمية لنجاح أي استراتيجية. ولضمان استناد الاستراتيجية النهائية إلى رؤية مشتركة ينبغي تعميم مسودة الوثيقة على طائفة واسعة من أصحاب المصلحة لا تقتصر على الأطراف التي شاركت في عملية وضع الاستراتيجية. ويمكن أن يحدث ذلك من خلال مجموعة متنوعة من المشاورات، بما في ذلك التشاور على الخط وورش عمل التحقق وأفرقة العمل الإضافية. ومن المرتقب أن تُستخدم التعليقات والملاحظات الناتجة عن هذه العملية لوضع اللمسات الأخيرة على الاستراتيجية.

3.3.3 التماس الموافقة الرسمية

في الخطوة الأخيرة من وضع الاستراتيجية، ينبغي للهيئة الرائدة للمشروع التأكد من اعتماد الاستراتيجية رسمياً من قبل السلطة التنفيذية. وتختلف عملية الاعتماد الرسمية هذه من بلد لآخر وتعتمد على كيفية تحديد الاستراتيجية في الإطار التشريعي. إذ يمكن اعتمادها مثلاً من خلال إجراء برلماني أو مرسوم حكومي.

وعلاوةً على ذلك، من الأهمية بمكان ألا يقتصر وضع الاستراتيجية على الموافقة من أعلى المستويات الحكومية، بل أن يستمر هذا الالتزام في مرحلة تنفيذ الاستراتيجية. وينبغي أن يخضع القائمون على الاستراتيجية للمساءلة وأن يلقون الدعم من حيث رأس المال السياسي والموارد.

4.3.3 نشر الاستراتيجية

ينبغي أن تكون الاستراتيجية وثيقة عمومية وأن تكون متاحة بسهولة. ومن شأن توفرها على نطاق واسع أن يضمن وعي الجمهور عامةً بأولويات وأهداف الأمن السيبراني لدى الحكومة، وأن يدعم أيضاً أي جهد لإذكاء الوعي بالأمن السيبراني. وفي حال اقتران الاستراتيجية بخطة عمل، ينبغي أن تشير خطة العمل أيضاً إلى فرص إضافية لمزيد من المشاركة والتعاون مع المجتمع المدني والقطاع الخاص.

ثمة المزيد من المراجع في الصفحة 55.

4.3 المرحلة الرابعة: التنفيذ

مرحلة التنفيذ هي أهم عنصر في دورة حياة الاستراتيجية الوطنية للأمن السيبراني. واتباع نهج منظم للتنفيذ، مدعوم بموارد بشرية ومالية كافية، أمر بالغ الأهمية لنجاح الاستراتيجية ويتعين أن يعتبر جزءاً من تطورها. وغالباً ما تتمحور مرحلة التنفيذ حول خطة العمل التي توجه مختلف الأنشطة المتوخاة.

1.4.3 وضع خطة العمل

كما هو الحال في وضع الاستراتيجية، لا يمكن أن يكون تنفيذها هو المسؤولية الوحيدة لهيئة واحدة. وبدلاً من ذلك، يتطلب الأمر المشاركة والتنسيق من جانب طائفة من مختلف أصحاب المصلحة في شتى دوائر الحكومة، فضلاً عن الدعم من جانب المجتمع المدني والقطاع الخاص. ويمكن لخطة العمل، التي وضعت وفقاً لمبدأ القيادة الواضحة والأدوار وتخصيص الموارد (القسم 8.4)، أن تدعم التنفيذ الفعال للاستراتيجية.

ولا يقل وضع خطة العمل أهمية عن الخطة بالذات. إذ ينبغي أن تكون هذه العملية، التي تقوم بتنظيمها الهيئة الرائدة للمشروع، بمثابة آلية لجمع أصحاب المصلحة المعنيين معاً للاتفاق على الأهداف والنواتج، بالإضافة إلى تنسيق الجهود وتجميع الموارد.

2.4.3 تحديد المبادرات التي يتعين تنفيذها

تسلّط الاستراتيجية الوطنية للأمن السيبراني الضوء على أهداف الحكومة والنواتج التي ترغب في تحقيقها عبر مختلف مجالات التركيز المحددة. وفي إطار خطة العمل، ينبغي للهيئة الرائدة للمشروع، بالتنسيق مع أصحاب المصلحة المعنيين، استبانة المبادرات المحددة في كل مجال من مجالات التركيز التي تساعد على تحقيق تلك الأهداف. ويمكن أن تشمل الأمثلة تنظيم تمارين الأمن السيبراني أو إنشاء خطوط أساس أمنية للبنى التحتية الحرجة أو وضع إطار للإبلاغ عن الحوادث، من بين أمور أخرى.

وينبغي إيلاء الأولوية للجدول الزمني والجهود اللازمين لتنفيذ هذه المبادرات وفقاً لأهميتها الحرجة لضمان حسن الاستفادة من الموارد المحدودة. ولهذه الغاية، ربما يمكن النظر في نتائج ونواتج المرحلة الثانية (الجرد والتحليل) على وجه التحديد من منظور "تقييم مشهد المخاطر السيبرانية" (القسم 2.2.3).

3.4.3 تخصيص الموارد البشرية والمالية للتنفيذ

بعد تحديد المبادرات ذات الأولوية، ينبغي للهيئة الرائدة للمشروع أن تحدد هيئات حكومية معينة بمثابة مالكين لكل مبادرة من هذه المبادرات. وفي المقابل، ستكون هذه الهيئات الحكومية مسؤولة عن تنفيذ كل مبادرة محددة مسندة إليها، ويتوقع منها تنسيق جهودها مع الجهات المعنية الأخرى كجزء من عملية التنفيذ.

ولضمان قدرة هذه الكيانات على تحقيق النواتج المتوقعة، ينبغي للهيئة الرائدة للمشروع التحقق مما إذا كانت قد منحت الولاية المناسبة، القانونية أو غير ذلك، المطلوبة للتنفيذ. كما ينبغي أن تعمل الهيئة الرائدة للمشروع مع أصحاب المبادرات المحددة لمعرفة ما هي الموارد المطلوبة لإنجاز العمل. وينبغي أن يتضمن هذا التقييم الموارد البشرية والخبرات والاحتياجات من التمويل. وبعد ذلك ينبغي أن تعمل الهيئة الرائدة للمشروع مع المالكين لمساعدتهم على تحديد وتأمين الموارد المطلوبة وفقاً للأنظمة الإدارية المالية المعمول بها في البلد.

4.4.3 وضع الأطر الزمنية والمقاييس

العنصر الحاسم الأخير في خطة العمل هو وضع مقاييس محددة ومؤشرات أداء رئيسية لتقييم كل من المبادرات المتخذة، من قبيل ما إذا كان البلد قد أجرى حملة توعية بشأن أهمية تبادل المعلومات أو نظّم ونفّذ تمريناً في الأمن السيبراني في قطاع هام في البنية التحتية أو أصدر قانوناً أساسياً للأمن السيبراني. وينبغي أيضاً وضع إطار زمني محدد للتنفيذ.

وينبغي وضع المقاييس ومؤشرات الأداء الرئيسية من قبل الهيئة الرائدة للمشروع بالشراكة مع المالكين المعنيين. وينبغي تشجيع هؤلاء على تحديد مجموعة أكثر تفصيلاً من المقاييس والحفاظ عليها لتسهيل تقييم كفاءة وفعالية المبادرات أثناء تنفيذها وبعد استكمالها.

ثمة المزيد من المراجع في الصفحة 55.

5.3 المرحلة الخامسة: المراقبة والتقييم

ينبغي للسلطة المختصة، أثناء هذه المرحلة، أن تصمم عملية رسمية لمراقبة الاستراتيجية وتقييمها. وفي مرحلة المراقبة، ينبغي أن تضمن الحكومة تنفيذ الاستراتيجية وفقاً لخطة العمل الخاصة بها. وفي مرحلة التقييم، ينبغي للحكومة وسلطتها المختصة تقييم ما إذا كانت الاستراتيجية لا تزال مجدية في ضوء بيئة المخاطر المتغيرة وما إذا كانت لا تزال تعكس أهداف الحكومة وما هي التعديلات الضرورية.

1.5.3 إنشاء عملية رسمية

حرصاً على ضمان المراقبة والتقييم الفعالين لتنفيذ الاستراتيجية، يتعين على الحكومة تحديد هيئة مستقلة مسؤولة عن مراقبة وتقييم التقدم المحرز في التنفيذ وكفاءته. وينبغي أن تشارك الهيئة مثالياً في تحديد مقاييس المراقبة والتقييم المناسبة لتنفيذ الاستراتيجية وخطة العمل والمبادرات المرتبطة بها، والتي ينبغي أن تتم خلال مرحلتي الإنتاج والاستهلال.

وينبغي أن تكون المراقبة وقياس الأداء والتنفيذ الناجح لخطة تنفيذ الاستراتيجية جزءاً من آليات الحوكمة التي يضعها البلد. ويساعد التقييم المستمر لخطة التنفيذ (أي ما يكون وما لا يكون على ما يرام) على حسن سير الاستراتيجية. وفيما يتعلق بتنفيذ الاستراتيجية، ينبغي أيضاً أن تحدد آليات الحوكمة الرشيدة بوضوح المساءلة والمسؤولية لضمان نجاح التنفيذ. ويساعد وضع المقاييس أو مؤشرات الأداء الرئيسية بحسب الأهداف القريبة والمتوسطة والبعيدة على تعزيز آليات الحوكمة والإدارة. وينبغي أن تكون مؤشرات الأداء الرئيسية أو المقاييس:

- محددة – تستهدف مجالاً معيناً للتحسين.
- قابلة للقياس – تحدد مقداراً أو على الأقل تقترح مؤشراً للتقدم.
- قابلة للتحقيق — تحدد ما هي النتائج التي يمكن تحقيقها واقعياً، في حدود الموارد المتاحة.
- مسؤولة – تحدد من سيفعل ماذا.
- مرتبطة بالزمن – تحدد متى يمكن تحقيق النتيجة (النتائج).

ومن شأن وضع مقاييس أساسية تحسين مراقبة الإجراءات وإبراز مجالات التحسين المحتملة. وعلاوة على ذلك، ينبغي أن تتناسب المخصصات في الميزانية مع مستويات الطموح والتعقيد في الأثر المتوخى.

2.5.3 مراقبة التقدم المُحرز في تنفيذ الاستراتيجية

ينبغي أن تقوم الهيئة المسؤولة عن مراقبة التقدم المحرز في تنفيذ الاستراتيجية بأعمالها بموجب جدول زمني متفق عليه طوال دورة حياة الاستراتيجية بأكملها. وينبغي أن تشير نتيجة أي نشاط مراقبة (في شكل تقرير مثلاً) إلى أي انحرافات عن الجداول الزمنية المتفق عليها وأسباب أي تأخير، من قبيل تعديل الأولويات وعدم كفاية الموظفين أو الموارد، وما شابه ذلك. وينبغي أن يتم ذلك بالإضافة إلى التحديثات الدورية التي يقدمها مالكو مختلف عناصر تنفيذ الاستراتيجية إلى الهيئة الرائدة للمشروع.

ومن شأن هذا النهج أن يضمن خضوع أصحاب المصلحة المعنيين للمساءلة عن الالتزامات المحددة، كما يضمن تحديد أي تحديات تواجه التنفيذ في وقت مبكر. وهذا بدوره يمكن الحكومة إما من تصحيح الوضع أو تكييف خططها وفقاً لذلك استناداً إلى الدروس المستخلصة في عملية التنفيذ.

3.5.3 تقييم نواتج الاستراتيجية

بالإضافة إلى تقييم التقدم المحرز في جميع المقاييس المتفق عليها، من المهم أيضاً إجراء تقييم دوري للنواتج ومقارنتها بالأهداف المحددة. وهذا أمر بالغ الأهمية لفهم ما إذا كانت أهداف الاستراتيجية تتحقق أم ما إذا كان ينبغي النظر في اتخاذ إجراءات أخرى. وكجزء من هذه العملية، يتعين أيضاً إعادة تقييم بيئة المخاطر الأوسع بانتظام لفهم ما إذا كان ثمة تغييرات خارجية تؤثر على نواتج الاستراتيجية. وعلى صعيد الواقع، تكون هذه العملية بمثابة لمسات مراجعة خفيفة لمواصفة تقييم المخاطر السيبرانية التي تتهدد البلد.

وينبغي تجميع التقييم، مع التوصيات المرتبطة به، في تقرير يرفع إلى الهيئة الرائدة للمشروع، يشتمل على وسائل لتحديث خطة العمل والتأكد من أنها معاصرة ومستجيبة للتغيير في السياسة وبيئة المخاطر.

وفي نهاية المطاف، ينبغي أن تكون التقارير الصادرة طوال دورة حياة الاستراتيجية هي الأساس للاستعراض الشامل للاستراتيجية الوطنية للأمن السيبراني وفقاً للجدول الزمني المحدد أثناء مرحلة الاستهلال. وينبغي ألا تقتصر هذه المراجعة الشاملة على النظر في التقدم المحرز والتغييرات في البيئة الخارجية فحسب بل ينبغي أيضاً أن تعيد تقييم الأولويات والأهداف الخاصة بالحكومة.

ثمة المزيد من المراجع في الصفحة 55.

4 المبادئ الشاملة

يقدم هذا القسم تسعة مبادئ شاملة يمكنها مجتمعةً أن تساعد في وضع استراتيجية وطنية تطلعية وشمولية للأمن السيبراني.

تنطبق هذه المبادئ على جميع مجالات التركيز الرئيسية المحددة في هذه الوثيقة. وينبغي النظر فيها في جميع خطوات عملية وضع الاستراتيجية الوطنية، من صوغ وثيقة الاستراتيجية الوطنية إلى تنفيذها.

ويعكس ترتيب هذه المبادئ السرد المنطقي وليس الترتيب من حيث الأهمية.

1.4 الرؤية

يجب أن تحدد الاستراتيجية رؤية واضحة لكامل الحكومة ولكامل المجتمع.

يزداد احتمال نجاح الاستراتيجية عندما تحدد رؤية تساعد جميع أصحاب المصلحة على فهم ما هو التهديد وما هي الحاجة إلى الاستراتيجية (السياق) وما الذي يجب تحقيقه (الأهداف) وما هو الغرض منها ومن يتأثر بها (النطاق).

وكلما كانت الرؤية أوضح كان من الأسهل على القادة وأصحاب المصلحة الرئيسيين ضمان اتباع نهج أكثر شمولية واتساقاً وتماسكاً. كما تسهّل الرؤية الواضحة التنسيق والتعاون وتنفيذ الاستراتيجية بين أصحاب المصلحة المعنيين. وينبغي صوغها على مستوى عالٍ بما فيه الكفاية والنظر في الطبيعة الدينامية للبيئة الرقمية.

وينبغي أن تتماشى أهداف الاستراتيجية والجدول الزمني لتنفيذها مع هذه الرؤية.

ثمة المزيد من المراجع في الصفحة 56.

2.4 النهج الشامل والأولويات المخصصة

ينبغي أن تنبثق الاستراتيجية من فهم وتحليل شمولي للبيئة الرقمية إجمالاً، ومع ذلك ينبغي تكييفها حسب ظروف البلد وترتيب أولوياته.

إن الأمن السيبراني ليس تحدياً تقنياً فحسب بل قضية معقدة متعددة الأوجه، تمتد جوانبها إلى ما هو أبعد من الازدهار الاقتصادي والاجتماعي، إلى مجالات مثل إنفاذ القانون والأمن الوطني والدولي والعلاقات الدولية والمفاوضات التجارية والتنمية المستدامة، وما إلى ذلك.

ومن المهم فهم جميع جوانب الأمن السيبراني وكيفية ترابطها أو احتمال تكاملها أو التنافس فيما بينها. وبناءً على هذا الفهم وعلى تحليل السياق في كل بلد، يمكن تحديد الأولويات بما يتماشى مع الأهداف والجدول الزمني لتنفيذ الاستراتيجية. وتمكّن الأولويات من وضع أهداف وجداول زمنية محددة ومن تخصيص الموارد اللازمة.

وتختلف الأولويات التي تضمها الاستراتيجية الوطنية للأمن السيبراني من بلد لآخر. إذ يمكن معالجة بعض مواضيع الأمن السيبراني في نفس الوثيقة أو في وثائق استراتيجية منفصلة (يمكن مثلاً معالجة الجوانب الرقمية للأمن القومي والدفاع في إطار استراتيجية الأمن القومي أو استراتيجية الدفاع).

ثمة المزيد من المراجع في الصفحة 56.

3.4 الشمولية

ينبغي وضع الاستراتيجية بمشاركة نشطة من جميع أصحاب المصلحة المعنيين، وينبغي لها أن تلبي احتياجاتهم ومسؤولياتهم.

أصبح للبيئة الرقمية أهمية حرجة بالنسبة للحكومات ومؤسسات الأعمال والأفراد. وتواجه هذه المجموعات مخاطر الأمن السيبراني وتتقاسم درجة من المسؤولية في إدارتها، وذلك تبعاً لدور كل منها. ولئن كانت المهمة صعبة، فإن تحديد جميع أصحاب المصلحة المعنيين وإشراكهم أمر ضروري لوضع الاستراتيجية الوطنية للأمن السيبراني والنجاح في تنفيذها. ويساعد ذلك على فهم احتياجات أصحاب المصلحة ومعارفهم وخبراتهم الفريدة، مما يسهل التعاون من أجل تحقيق أهداف الاستراتيجية.

ولتعزيز الشمولية، ينبغي أن تكون الاستراتيجية وثيقة عمومية.

ثمة المزيد من المراجع في الصفحتين 56 و57.

4.4 الازدهار الاقتصادي والاجتماعي

ينبغي أن تشجع الاستراتيجية الازدهار الاقتصادي والاجتماعي وأن تعزز مساهمة تكنولوجيا المعلومات والاتصالات في التنمية المستدامة والشمولية الاجتماعية.

إن البيئة الرقمية لديها القدرة على دفع عجلة النمو الاقتصادي والتقدم الاجتماعي وتعزيز القيم المجتمعية الرئيسية وتحسين الخدمات العامة وقدراتها وتسهيل التجارة الدولية وتعزيز الحكم الرشيد.

وقد أفضى تزايد الاعتماد على البيئة الرقمية لتلبية مطالب المجتمعات إلى زيادة الاهتمام بالأمن السيبراني. ومع ذلك، فإن الأمن السيبراني ليس هدفاً في حد ذاته، بل ينبغي للاستراتيجية أن تتماشى مع الأهداف الاجتماعية الاقتصادية الأوسع للبلد وأن تؤدي إلى بناء الثقة اللازمة لتحقيق هذه الأهداف وكذلك لحماية البلد من التهديدات السيبرانية.

ثمة المزيد من المراجع في الصفحة 57.

5.4 حقوق الإنسان الأساسية

ينبغي أن تحترم الاستراتيجية القيم الأساسية وأن تكون متسقة معها.

ينبغي أن تعترف الاستراتيجية بأن الحقوق التي يتمتع بها الناس خارج الخط يجب حمايتها أيضاً على الخط. وينبغي لها أن تحترم الحقوق الأساسية المتفق عليها عالمياً، بما في ذلك دون حصر الحقوق المنصوص عليها في الإعلان العالمي لحقوق الإنسان الصادر عن الأمم المتحدة والعهد الدولي الخاص بالحقوق المدنية والسياسية فضلاً عن الأطر القانونية متعددة الأطراف أو الإقليمية ذات الصلة.

وينبغي إيلاء الاهتمام إلى حرية التعبير وخصوصية الاتصالات وحماية البيانات الشخصية. وعلى وجه الخصوص، ينبغي أن تتجنب الاستراتيجية تسهيل ممارسة المراقبة التعسفية أو غير المبررة أو غير القانونية أو اعتراض الاتصالات أو معالجة البيانات الشخصية.

ولدى الموازنة بين احتياجات الدولة واحتياجات الأفراد، ينبغي أن تحرص الاستراتيجية، حسب الاقتضاء، على أن تكون عمليات المراقبة واعتراض الاتصالات وجمع البيانات، التي تجري ضمن سياق تحقيق معين أو قضية قانونية، مرخص بها من قبل السلطة الوطنية المختصة وأن تكون قائمة على أساس إطار قانوني عام ودقيق وشامل وغير تمييزي يمكّن من الإشراف الفعال والضمانات الإجرائية وسبل الانتصاف.

ثمة المزيد من المراجع في الصفحتين 57 و58.

6.4 إدارة المخاطر والصمود

ينبغي أن تمكن الاستراتيجية من إدارة مخاطر الأمن السيبراني بكفاءة ومن تعزيز صمود الأنشطة الاقتصادية والاجتماعية.

لَئِن كانت البيئة الرقمية توفر لأصحاب المصلحة فرصاً اقتصادية واجتماعية فإنها تعرضهم أيضاً لمخاطر تتهدد الأمن السيبراني. فعندما تستخدم المنظمات مثلاً تكنولوجيا المعلومات والاتصالات لتشجيع الابتكار

وزيادة الإنتاجية وتحسين القدرة التنافسية، أو عندما تنشر الحكومات خدماتها على الخط، من الممكن أن تقع حوادث في مجال الأمن السيبراني يحتمل أن تؤدي إلى خسارة مالية وضرر بالسمعة وتعطيل العمليات وعرقلة الابتكار، وما إلى ذلك. وعلى غرار المخاطر الأخرى، لا يمكن القضاء كلياً على المخاطر التي تتهدد الأمن السيبراني ولكن يمكن إدارتها والحد منها.

ولمواجهة هذا التحدي، ينبغي للاستراتيجية أن تشجع الكيانات على تحديد أولويات استثماراتها في الأمن السيبراني وإدارة المخاطر على نحو استباقي. وتبعاً لمدى تعرض الكيان للمخاطر، يتعين الحفاظ على التوازن بين التدابير الأمنية والفوائد المحتملة، مع مراعاة الطبيعة الدينامية للبيئة الرقمية. كما ينبغي أن تدرك الاستراتيجية الحاجة إلى إدارة مستمرة للمخاطر وأن تعمل على تيسير اتباع نهج متماسك عبر الكيانات المترابطة.

ومن شأن التركيز على إدارة المخاطر أن يؤدي أيضاً إلى تأهب أصحاب المصلحة لحوادث أمنية محتملة، بما يضمن صمود النشاط الاقتصادي والاجتماعي في البلد. ومن هذا المنطلق، ينبغي أن تشجع الاستراتيجية اعتماد تدابير لضمان استمرارية أنشطة مؤسسات الأعمال، والتي تشمل إدارة الحوادث والأزمات فضلاً عن خطط الانتعاش.

ثمة المزيد من المراجع في الصفحة 58.

7.4 المجموعة المناسبة من أدوات السياسة

ينبغي أن تستخدم الاستراتيجية أنسب أدوات السياسة المتوفرة لتحقيق كل هدف من أهدافها، مع مراعاة الظروف الخاصة بالبلد.

لن تتحقق أهداف الأمن السيبراني لدى الحكومة إلا إذا حدث تغيير في السلوك لدى جميع أصحاب المصلحة المعنيين. وفي معظم الأحوال، يتوفر لدى الحكومات وسائل وأدوات سياسة مختلفة لتحقيق هذه الغاية. وتشمل هذه الأدوات برامج وآليات التشريعات والأنظمة والتقييس والحوافز وتبادل المعلومات والبرامج التعليمية وتقاسم أفضل الممارسات ووضع معايير السلوك المتوقعة وبناء مجتمعات الثقة، وغيرها. ولكل من هذه الأدوات مواطن قوة ومواطن ضعف خاصة بها وتأتي بتكلفة مختلفة وتحقق نتائج مختلفة.

ويمكن تحقيق أفضل النتائج باختيار أداة السياسة الأكثر ملاءمة لكل هدف في حد ذاته وموازنة استخدام مختلف الأدوات.

ثمة المزيد من المراجع في الصفحة 59.

8.4 القيادة الواضحة والأدوار وتخصيص الموارد

ينبغي أن تقوم بوضع الاستراتيجية هيئة في أعلى مستوى من الحكومة، تكون مسؤولة عن تعيين الأدوار والمسؤوليات ذات الصلة وتخصيص الموارد البشرية والمالية الكافية.

ينبغي الترويج للأمن السيبراني والحفاظ عليه في أعلى المستويات الحكومية. وعلاوة على ذلك، ولضمان المساءلة والتقدم، يتعين تحديد جهات تنسيق لكل من مسارات العمل، وينبغي أن يكون لدى جميع الأطراف المعنية فهم واضح لأدوار ومسؤوليات كل منها.

وينبغي للاستراتيجية أيضاً أن تخصص الموارد البشرية والمالية والمادية اللازمة لتنفيذها. ويتعين أن يوجه هذا المبدأ عملية وضع الاستراتيجية وصوغ خطة العمل من أجلها.

ثمة المزيد من المراجع في الصفحة 59.

9.4 بيئة الثقة

ينبغي أن تساعد الاستراتيجية على بناء بيئة رقمية يمكن أن يثق بها المواطنون ومؤسسات الأعمال.

إن بناء الثقة في النظام البيئي الرقمي الوطني، حيث تتوفر حماية حقوق المستعملين ومصالحهم وضمان أمن البيانات والأنظمة، أمر ضروري لاستغلال الإمكانات الكاملة للفرص الاجتماعية والسياسية والاقتصادية التي يوفرها استخدام تكنولوجيا المعلومات والاتصالات. ويجب أن تمكّن الاستراتيجية السياسات والعمليات والإجراءات على المستوى الوطني من أجل تقديم خدمات حيوية آمنة (بما في ذلك الحوكمة الإلكترونية والتجارة الإلكترونية والمعاملات المالية الرقمية، وغيرها) تدعمها تكنولوجيا المعلومات والاتصالات ويستخدمها المواطنون. ومن شأن هذا النهج أن يغرس مبدأ الثقة لا بين عموم السكان فحسب بل كذلك داخل المنظمات العامة والخاصة التي تقدم للمواطنين خدماتها المتعلقة بتكنولوجيا المعلومات والاتصالات.

ثمة المزيد من المراجع في الصفحة 59.

5 الممارسات الجيدة في الاستراتيجية الوطنية للأمن السيبراني

يؤثر الأمن السيبراني على العديد من مجالات التنمية الاجتماعية الاقتصادية ويتأثر بعدة عوامل ضمن السياق الوطني.

لذلك، يقدم هذا القسم مجموعة من عناصر الممارسات الجيدة التي من شأنها أن تجعل الاستراتيجية شاملة وفعالة، وتسمح في الوقت ذاته بتصميمها بما يلائم السياق الوطني.

وقد جُمعت عناصر الممارسات الجيدة هذه في مجالات تركيز متميزة، وهي في الواقع مواضيع شاملة للاستراتيجية الوطنية للأمن السيبراني. وقد طُرحت هنا مجالات التركيز والعناصر كأمثلة للممارسات الجيدة، ومع ذلك من المهم بشكل خاص أن يُنظر إلى هذه الأخيرة في السياق الوطني، إذ قد لا يكون بعضها ذو صلة بالوضع المحدد للبلد. وينبغي للبلدان تحديد ومتابعة عناصر الممارسات الجيدة التي تدعم أهدافها وأولوياتها بما يتماشى مع الرؤية المحددة في استراتيجيتها (القسم 4). وينبغي ألا يُنظر إلى ترتيب فرادى العناصر أو مجالات التركيز أدناه على أنها تشير إلى مستوى الأهمية أو الأولوية.

1.5 مجال التركيز 1 – الحوكمة

يقدم مجال التركيز هذا عناصر الممارسات الجيدة التي ينبغي النظر فيها لإدراجها في نص الاستراتيجية عند معالجة بنية الحوكمة للأمن السيبراني الوطني. وينبغي أن تحدد الاستراتيجية بوضوح الأهداف والطموحات التي تبتغيها الحكومة في مجال الأمن السيبراني، بالإضافة إلى تحديد الأدوار والمسؤوليات المطلوبة لضمان تنفيذها.

وتحقيقاً لهذه الغاية، ينبغي أن تحدد الاستراتيجية السلطة المختصة وتخولها المسؤولية عن تنفيذ الاستراتيجية، وأن تضع آلية لتحديد وإشراك الهيئات الحكومية المتأثرة بتنفيذ الاستراتيجية أو المسؤولة عنها، وأن تلتزم بوضع أهداف محددة وقابلة للقياس ويمكن تحقيقها وقائمة على النتائج وعلى الوقت في خطة التنفيذ الخاصة بالاستراتيجية، وأن تدرك الحاجة إلى تخصيص الموارد (من قبيل الإرادة السياسية والتمويل والزمن والناس) لتحقيق النواتج المرجوة.

1.1.5 ضمان أعلى مستوى من الدعم

ينبغي أن تحصل الاستراتيجية على التأييد الرسمي على أعلى مستوى من الحكومة. ويخدم هذا التأييد غرضين هامين. فهو، أولاً، يزيد من احتمال تخصيص الموارد الكافية ونجاح جهود التنسيق. وثانياً، يرسل إشارة إلى البيئة الوطنية الأوسع يبين فيها مدى الأهمية التي يعيرها البلد للأمن السيبراني.

2.1.5 إنشاء سلطة مختصة بالأمن السيبراني

ينبغي أن تحدد الاستراتيجية سلطة مختصة بالأمن السيبراني على المستوى الوطني – قائداً (سواء فرداً أو هيئةً) رفيع المستوى وراسخاً على أعلى مستوى من الحكومة لتوفير التوجيه وتنسيق العمل ومراقبة تنفيذ الاستراتيجية.

وينبغي أن تعمل هذه الهيئة الوطنية المختصة بالأمن السيبراني أيضاً بمثابة هيئة إدارة لتحديد وتوضيح الأدوار والمسؤوليات والعمليات وحقوق اتخاذ القرار والمهام المطلوبة لضمان التنفيذ الفعال للاستراتيجية. ويشمل ذلك تحديد أصحاب المصلحة الذين سوف يشرفون على تنفيذ الاستراتيجية وتحديد أهداف الأداء لمختلف الإدارات الوزارية أو الحكومية أو المؤسسات أو الأفراد المسؤولين عن جوانب محددة من الاستراتيجية وخطة العمل اللاحقة. وقد يتطلب هذا النهج سياسات أو هياكل قانونية إضافية لتمكين الأطراف المعنية من أداء مهامها.

وبما أن مجال الأمن السيبراني يتقاطع مع العديد من مجالات القضايا المختلفة، فمن الضروري التأكد من أن الهيئة الوطنية المختصة لديها القدرة على إشراك وتوجيه أصحاب المصلحة المعنيين.

3.1.5 ضمان التعاون داخل الحكومة

ينبغي أن تضع الاستراتيجية آلية لتحديد وإشراك الهيئات الحكومية المتأثرة بالاستراتيجية أو المسؤولة عن تنفيذها. ويعتبر الالتزام والتنسيق والتعاون داخل الحكومة من المهام الأساسية لهذه الهيئات، وهي ضرورية للتأكد من أن آليات الحوكمة (أي القواعد) والموارد تسفر عن النواتج المرجوة من الاستراتيجية.

ويكفل التواصل والتنسيق على نحو فعال أن جميع الوزارات والهيئات الحكومية على علم بالسلطات والبعثات والمهام التي تضطلع بها الجهات الأخرى. ولكن الالتزام يعني دعم سياسات متسقة على مر الزمن للحرص على الوفاء بالوعود التي تتضمنها الاستراتيجية. ومن الأمثلة على آلية التنسيق عقد اجتماعات دورية لجميع أصحاب المصلحة للمشاركة في خطط العمل ذات الصلة التي يتعين استعراضها معاً. ومن الأمثلة على آلية التعاون إنشاء فريق مهام داخل الحكومة لمعالجة مسألة خاصة. ومن أمثلة الالتزام الاتساق بين برامج السياسات الداخلية والخارجية للبلد، بحيث لا تنال وزارة ما من مصداقية وزارة أخرى باتخاذ مواقف مختلفة في مجال سياسة مسألة بعينها.

4.1.5 ضمان التعاون بين القطاعات

ينبغي أن تعكس الاستراتيجية فهم الجوانب التي تعتمد فيها الحكومة على القطاع الخاص وأصحاب المصلحة الوطنيين الآخرين (والعكس) في ضمان الأمن السيبراني. ولهذه الغاية، ينبغي أن توضح الاستراتيجية كيف يمكن للحكومة أن تشرك أصحاب المصلحة وتحدد لهم الأدوار والمسؤوليات. مثال ذلك، ينبغي أن تحدد الاستراتيجية شبكة من نقاط الاتصال الوطنية الموثوقة لدوائر الصناعات الحيوية والضرورية لتشغيل الخدمات والبنى التحتية الأساسية.

5.1.5 تخصيص الميزانية والموارد المخصصة

ينبغي أن تحدد الاستراتيجية الموارد المخصصة والمناسبة لتنفيذها والحفاظ عليها ومراجعتها. ومن شأن التمويل الكافي المتسق والمستمر أن يوفر الأسس لموقف فعال من حيث الأمن السيبراني الوطني. وينبغي أن تحدد الموارد من حيث المال (أي ميزانية مخصصة) والناس والمواد، فضلاً عن العلاقات والشراكات واستمرار الالتزام السياسي والقيادة المطلوبة لنجاح التنفيذ. وينبغي ألا يعتبر توفير الموارد وتحديد الأهداف والمهام في إطار استراتيجية بمثابة مبادرة لمرة واحدة. ويمكن تخصيص الموارد بحسب المهمة أو الهدف أو بحسب الجهة الحكومية.

وقد تنظر الحكومة أيضاً في إنشاء ميزانية مركزية للأمن السيبراني، تديرها آلية حوكمة مركزية للأمن السيبراني. وسواء تعلق الأمر بتجميع مصادر تمويل مختلفة في برنامج متكامل متماسك أم بوضع ميزانية موحدة في إطار الحكومة، ينبغي وضع برنامج شامل يدار ويتّبع بموجب معالم زمنية لضمان النجاح في تنفيذ الاستراتيجية.

6.1.5 وضع خطة للتنفيذ

ينبغي أن تكون الاستراتيجية مصحوبة أو مرتبطة بخطة تنفيذ تحدد بمزيد من التفصيل كيفية تحقيق أهدافها. وتحدد خطط التنفيذ الفعالة الهيئة المسؤولة عن كل مهمة وهدف والموارد اللازمة للتنفيذ على مر الزمن (المدى القريب والمتوسط والطويل) والعمليات التي سوف تستخدم والنواتج المتوقعة (القسم 4.3 استهلال التنفيذ).

ثمة المزيد من المراجع في الصفحتين 60 و61.

2.5 مجال التركيز 2 – إدارة المخاطر في مجال الأمن السيبراني الوطني

يقدم مجال التركيز هذا الممارسات الجيدة لمعالجة الأمن السيبراني من خلال إدارة المخاطر. وكما جاء في مبدأ إدارة المخاطر والتصدي (القسم 2.4) ينبغي اعتماد نهج لإدارة المخاطر، لأن المخاطر السيبرانية لا يمكن القضاء عليها تماماً. ولكن الحرص على أن يكون لدى البلد فهم جيد للمخاطر التي يتعرض لها يمكّنه من إدارة هذه المخاطر على نحو فعال جداً. ومن حيث تقييم المخاطر، ينبغي أن يركز النهج على تحديد التبعيات المتبادلة وكذلك النظر أيضاً في المخاطر الناشئة عن التبعيات عبر الحدود الوطنية. وينبغي أن ينظر نهج إدارة المخاطر في كامل دورة الحياة، من الوضع أو التوريد إلى التشغيل والاستبدال.

ومن المهم أيضاً أن نلاحظ أن تهديدات الأمن السيبراني دينامية للغاية ولا يمكن التنبؤ بها، ولذلك ينبغي أن يعاد النظر بانتظام في أي نهج لإدارة المخاطر. وبناء عليه، ينبغي أن تخطط الاستراتيجية لمراقبة وتقييم أنشطة إدارة المخاطر لضمان التحسين المستمر.

1.2.5 تحديد نهجِ إدارة المخاطر

ينبغي أن تحدد الاستراتيجية نهجاً متماسكاً لإدارة المخاطر يتعين أن تتبعه جميع الهيئات الحكومية ومشغلو البنية التحتية الحرجة المحددون محلياً. وينبغي أن يفضي النهج إلى تحديد الأصول والخدمات الرئيسية ذات الأهمية لسلامة سير المجتمع والاقتصاد وما يرتبط بذلك من التهديدات والمخاطر.

وينبغي أن يهدف النهج إلى وضع سجل وطني للمخاطر، يتم الاحتفاظ به والاطلاع عليه بشكل آمن، لتمكين الإشراف الحكومي على المخاطر والنهج المتبعة لإدارة هذه المخاطر. وينبغي علاوة على ذلك، أن يطور النهج طريقة لتحديد الأولويات استناداً إلى حساب احتمالات المخاطر وأثرها. وينبغي أن يحدد علاوة على ذلك مسؤوليات الهيئات الرئيسية في كل قطاع فيما يتعلق بتقييم المخاطر التي تتهدد الأمن السيبراني على الصعيد الوطني وقبولها ومعالجتها.

2.2.5 تحديد منهجية مشتركة لإدارة المخاطر التي تتهدد الأمن السيبراني

ينبغي أن تحدد الاستراتيجية منهجية مشتركة لإدارة المخاطر التي تتهدد الأمن السيبراني. وهذا من شأنه ضمان الكفاءة والاتساق في جميع المنظمات وتسهيل تبادل المعلومات عن المخاطر عبر الأنظمة المترابطة. وينبغي تفضيل منهجية قائمة على المعايير الدولية لأن من شأنها أن تخفض التكاليف وتؤدي إلى تفاعل أفضل مع القطاع الخاص.

وينبغي أن توفر المنهجية الإرشاد بشأن توزيع الأدوار والمسؤوليات لمختلف جوانب إدارة المخاطر، من قبيل تقييم المخاطر وتقييم الأصول وتنفيذ وصيانة تدابير التخفيف من أثرها، وقبول المخاطر المتبقية. وينبغي أن تتضمن المنهجية برنامج اعتماد للمساعدة في تقييم الامتثال وتحسينه في نهاية المطاف.

ومن المهم، لدى شراء وتطوير البنية التحتية أو الخدمات، أن توفر منهجية إدارة المخاطر علاوة على ذلك الإرشاد بشأن الحد من المخاطر من خلال معمارية وتصميم آمنين، والاعتراف بأن أفضل طريقة لتحقيق هذا الأمن هي عندما يكون جزءاً لا يتجزأ من عملية تصميم المنتج أو العملية أو الخدمة (الأمن بالتصميم).

3.2.5 تطوير جانبيات قطاعية للمخاطر التي تتهدد الأمن السيبراني

ينبغي أن تستدعي الاستراتيجية استخدام جانبيات قطاعية للمخاطر التي تتهدد الأمن السيبراني. وجانبية المخاطر القطاعية هي تحليل كمي لأنواع التهديدات الماثلة. والهدف من جانبية المخاطر هو توفير فهم أكثر موضوعية للمخاطر من خلال تعيين قيم عددية للمتغيرات التي تمثل أنواعاً مختلفة من التهديدات والمخاطر الماثلة. وينبغي أن توصي الاستراتيجية بجانبيات مخاطر للقطاعات التي يعتبرها البلد ذات أهمية حرجة لمجتمعه واقتصاده.

ويوفر استخدام جانبيات المخاطر القطاعية أساساً لمزيد من التقييمات المحددة للمخاطر التي تتهدد فرادى المنظمات، ويدخل التماسك داخل وعبر جميع القطاعات على المستوى الوطني، ويقلل من الموارد اللازمة لتقييم المخاطر على مستوى المنظمات. وينبغي تحديثها بانتظام للتأكد من أنها لا تزال معاصرة.

4.2.5 وضع سياسات الأمن السيبراني

ينبغي أن تشجع الاستراتيجية على وضع سياسات الأمن السيبراني للهيئات الوطنية الحيوية، مثل السلطات الحكومية ومشغلي البنية التحتية الحرجة، من بين هيئات أخرى. وتشمل هذه السياسات، المعتمدة وفقاً لمبدأ المجموعة المناسبة من أدوات السياسة (القسم 7.4)، الحوكمة والمتطلبات التشغيلية والتقنية وترشد أصحاب المصلحة بشأن أدوارهم ومسؤولياتهم، فضلاً عن أنها توجه أو تفرض مناهج محددة لهذه القضايا.

وقد يشمل ذلك مثلاً السياسات التي تعالج الأمن السيبراني في التوريد أو التطوير وتحدد برامج تقاسم المعلومات وتنسق عمليات الكشف عن مواطن الضعف وتضع المعايير الدنيا للرعاية وتحدد خطوط الأساس للأمن وتحدد برامج شهادات الامتثال وتفرض الإبلاغ عن الحوادث السيبرانية.

ومن شأن اتباع نهج منسق على المستوى الوطني أن يؤدي إلى إدارة أكثر فعالية وكفاءة في مجال الأمن السيبراني، من حيث إنه ينسق الممارسات ويسهل التنسيق وقابلية التشغيل البيني.

ثمة المزيد من المراجع في الصفحة 61.

3.5 مجال التركيز 3 – التأهب والصمود

يوفر مجال التركيز هذا لمحة عامة عن الممارسات الجيدة التي تدعم إنشاء واستدامة القدرات الوطنية الفعالة لمنع حوادث الأمن السيبراني الرئيسية والكشف عنها والتخفيف من حدتها والتصدي لها، ولتحسين الصمود السيبراني عموماً في بلد ما.

1.3.5 إنشاء قدرات التصدي للحوادث السيبرانية

ينبغي أن تدعو الاستراتيجية إلى إنشاء قدرات وطنية مناسبة للتصدي للحوادث لمواجهة تحديات الأمن السيبراني التشغيلية. وفي كثير من الأحيان، تشير هذه القدرة إلى إنشاء أفرقة الاستجابة للطوارئ الحاسوبية (CERTs) أو أفرقة الاستجابة لحوادث الأمن الحاسوبي (CSIRTs) أو أفرقة الاستجابة للحوادث الحاسوبية (CIRTs) ذات المسؤولية على المستوى الوطني.

وقد يتغير الشكل التنظيمي المحدد لأي فريق CERT/CSIRT/CIRT (وطني أو حكومي أو قطاعي، وما إلى ذلك)، وقد لا يكون لكل بلد نفس الاحتياجات والموارد، ومع ذلك ينبغي أن توفر هذه الأفرقة المتخصصة والمخصصة مجموعة من الوظائف الاستباقية والتفاعلية، فضلاً عن الخدمات الوقائية والتعليمية. وهكذا، يمكن لهذه الكيانات أن تزيد من قدرة البلد على الاستجابة السريعة والتعافي من الهجمات السيبرانية، فضلاً عن تحسين قدرته على الصمود إزاء التهديدات السيبرانية، مما يقلل من الأثر الاقتصادي والتشغيلي العام المحتمل للهجمات السيبرانية ذات الأهمية على الصعيد الوطني.

وينبغي أن تحدد الاستراتيجية كذلك آليات التعاون وإجراءات الاتصال وتطورها بين أفرقة الاستجابة للحوادث الوطنية والقطاعية (إن وجدت في البلد)، وكذلك مع النظراء الدوليين.

2.3.5 وضع خطط طوارئ لإدارة أزمة الأمن السيبراني

ينبغي أن تدعو الاستراتيجية إلى وضع خطة وطنية لحالات الطوارئ والأزمات المتعلقة بالأمن السيبراني. وينبغي أن تكون الخطة جزءاً من خطة الطوارئ الوطنية الشاملة أو متوافقة معها. وينبغي أيضاً النظر في خطة محددة للبنى التحتية للمعلومات الحرجة.

وينبغي أن تأخذ خطة الطوارئ الوطنية للأمن السيبراني هذه في الاعتبار نتائج تقييمات المخاطر على المستوى الوطني وأي جوانب ترابط عبر القطاعات يمكن أن تؤثر على استمرارية عمليات البنى التحتية الحرجة، فضلاً عن أي آليات للتعافي من الكوارث. وعلاوةً على ذلك، ينبغي أن توفر نظرة عامة على آليات التصدي للحوادث على المستوى الوطني وأن تسلط الضوء كذلك على كيفية تصنيف حوادث الأمن السيبراني، على أساس أثرها على الأصول والخدمات الحرجة.

3.3.5 تعزيز تبادل المعلومات

ينبغي أن تدعو الاستراتيجية إلى إنشاء آليات لتقاسم المعلومات من شأنها تمكين تبادل الاستخبارات القابلة للتنفيذ ومعلومات التهديد بين القطاعين العام والخاص وداخل كل منهما.

ويمكن أن تساعد برامج تقاسم المعلومات الرسمية وغير الرسمية على تعزيز التنسيق الفعال والاتصالات المتسقة والدقيقة والمناسبة أثناء أنشطة الاستجابة للحوادث والتعافي منها، وأن تسهل سرعة تقاسم معلومات التهديدات والاستخبارات بين الأطراف المتأثرة وأصحاب المصلحة الآخرين، وأن تساعد على تحسين فهم كيفية انتقاء القطاعات واستهدافها، وأن تنشر المعلومات عن الأساليب التي يمكن استخدامها للدفاع عن الأصول المتأثرة وتخفيف الضرر الذي تتعرض له، وأن تقلل في نهاية المطاف من مواطن الضعف والتعرض إلى جانب المخاطر المصاحبة لها.

وينبغي أن تحدد الاستراتيجية هيئة أو أكثر من الهيئات المؤسسية (أي السلطات المختصة) المسؤولة عن نقل المعلومات الدقيقة والقابلة للتنفيذ بين أوساط الأمن السيبراني الوطني، بما في ذلك القطاعين العام والخاص.

وينبغي أن يكون تقاسم المعلومات عملية ذات اتجاهين. وإذا كانت الحكومات مستعدة لتقاسم المعلومات التي في حوزتها، فإن تصرفها هذا سوف يبرهن لهيئات القطاع الخاص على أن الحكومة هي حقاً شريك في تقاسم معلومات التهديد، ويساعد على تركيز اهتمام المستجيبين للتهديدات الأساسية والاستعداد على نحو أفضل للتصدي لها.

4.3.5 إجراء تمارين الأمن السيبراني

ينبغي أن تشجع الاستراتيجية على تنظيم وتنسيق تمارين الأمن السيبراني والاستجابة للحوادث على الصعيدين المحلي والدولي. ويمكن أن تتبع هذه التمارين أشكالاً مختلفة (مثل عمليات المحاكاة أو التمارين في الوقت الفعلي) وأن تستهدف الأوساط التقنية وأصحاب القرار.

ومن شأن تمارين الأمن السيبراني وغير ذلك من آليات التخطيط لمواجهة الأزمات أن تساعد البلدان على تطوير القدرة المؤسسية على الاستجابة للحوادث بفعالية واختبار إجراءات إدارة الأزمات وآليات الاتصال والتحقق من القدرة التشغيلية للأفرقة CERTs/CSIRTs/CIRTs للاستجابة تحت الضغط والمساعدة على فهم أي من أوجه الترابط عبر القطاعات.

وكذلك، من شأن تمارين الأمن السيبراني على المستوى الدولي أن تساعد على تعزيز القدرة على الاستجابة للحوادث السيبرانية بين الدول وفهم أوجه الاعتماد المتبادل عبر الحدود وبناء الثقة بين البلدان وتحسين مستويات الصمود والتأهب على المستوى الدولي عموماً.

ثمة المزيد من المراجع في الصفحتين 62 و63.

4.5 مجال التركيز 4 – خدمات البنية التحتية الحرجة والخدمات الأساسية

يبحث مجال التركيز هذا في الممارسات الجيدة المتعلقة بحماية البنى التحتية الحرجة (CIS)، وعلى وجه الخصوص البنى التحتية للمعلومات الحرجة (CIIS). وبينما ليس هنالك من تعاريف معترف بها عالمياً للمصطلحين، وإذ يتعين على الحكومات أن تحدد ما هي الهيئات والخدمات التي يجب تضمينها استناداً إلى تقييم المخاطر الوطني الخاص بها، يعرّف هذان المصطلحان، لأغراض هذا الدليل، على النحو التالي:

- *البنى التحتية الحرجة (CI)* مصطلح يستخدم لوصف الأصول الأساسية لعمل وأمن المجتمع والاقتصاد في بلد ما؛
- *البنية التحتية للمعلومات الحرجة (CII)* هي أنظمة تكنولوجيا المعلومات وتكنولوجيا المعلومات والاتصالات التي تدفع تشغيل الوظائف الرئيسية للبنية التحتية الحرجة في البلد.

وبديلاً من ذلك، يمكن تطبيق مفهوم الخدمات الأساسية، بالإشارة إلى الخدمات، التي تعتبر أساسية للحفاظ على الأنشطة المجتمعية أو الاقتصادية الحرجة.

وفي كلتا الحالتين، تشمل بعض أمثلة هذه الخدمات، دون حصر، ما يلي: الطاقة (الكهرباء والنفط والغاز) والنقل (الجوي والمائي والبري والسكك الحديدية) والتمويل والمصارف (مؤسسات الائتمان ومواقع التبادل التجاري والأطراف المركزية المقابلة) والرعاية الصحية (مؤسسات الرعاية الصحية، بما فيها المستشفيات

والعيادات الخاصة) وإمدادات مياه الشرب وتوزيعها، والخدمات الرقمية والاتصالات (الخدمات الهاتفية الثابتة والمتنقلة، وتوفير البنية التحتية للإنترنت، مثل نقاط تبادل الإنترنت (IXP) وخدمة أسماء الميادين، وغيرها).

1.4.5 وضع نهجٍ لإدارة المخاطر لحماية البنى التحتية والخدمات الحرجة

ينبغي أن تتناول الاستراتيجية حماية البنى التحتية الحرجة (CIs) والبُنى التحتية للمعلومات الحرجة (CIIs) من منظور إدارة المخاطر، وفقاً لمبدأ إدارة المخاطر والصمود (القسم 6.4). وينبغي لتقييم مفصّل للمخاطر أن يوجّه تحديد ماهية البنى التحتية الوطنية الحرجة CIs وCIIs والخدمات الحرجة، التي قد يكون لتعطلها أثر خطير على الصحة أو السلامة أو الأمن أو الرفاهية الاقتصادية للمواطنين، أو على الأداء الفعال للحكومة أو الاقتصاد.

وعلاوة على ذلك، ينبغي اعتماد نهج قائم على المخاطر في تحديد وترتيب أولويات تنفيذ البرامج والسياسات المصممة لحماية البنى التحتية الحرجة CIs وCIIs. ولتسهيل المشاركة مع القطاع الخاص، يمكن أيضاً النظر في نهج إدارة المخاطر المستند إلى المعايير الدولية.

2.4.5 اعتماد نموذج حوكمة ذي مسؤوليات واضحة

ينبغي أن تصف الاستراتيجية على مستوى عالٍ بنية الإدارة والأدوار والمسؤوليات لمختلف أصحاب المصلحة لحماية البنى التحتية الحرجة CI وCII. وكما جاء في مبدأ القيادة الواضحة والأدوار وتخصيص الموارد (القسم 8.4)، يتطلب أي برنامج يتسم بالفعالية والكفاءة لحماية البنية التحتية الحرجة CI أن يكون لدى أصحاب المصلحة أدوار ومسؤوليات محددة بوضوح وأن تُنشأ آلية تنسيق لإدارة القضايا الجارية.

وكثيراً ما لا تملك الحكومة أو لا تتحكم بالبنى التحتية الحرجة CI وCII، وتتجاوز جهود حماية هذه البُنى التحتية عموماً قدرات وولاية أي وكالة بعينها في الحكومة. وهكذا، فإن تعيين منسق عام لأمن البنى التحتية الحرجة (السيبراني)، من قبيل لجنة مشتركة بين الوكالات، يمكن أن يساعد إلى حد كبير في الجهود المبذولة لحماية البنى التحتية الحرجة.

وينبغي أن يشمل نموذج الحوكمة الخاص بحماية البنى التحتية الحرجة CI وCII تحديد الهيئات الحكومية المسؤولة عن قطاعات محددة ومسؤوليات ومساءلة مشغلي البنى التحتية CI وCII، بالإضافة إلى قنوات الاتصال وآليات التعاون بين الوكالات العامة والخاصة لضمان تشغيل الخدمات والبُنى التحتية الحرجة وتعافيها.

3.4.5 تحديد خطوط الأساس الدنيا للأمن السيبراني

ينبغي للاستراتيجية إما أن تسلط الضوء على التشريعات والأطر التنظيمية القائمة أو أن تقترح وضع تشريعات وأطر تنظيمية جديدة تحدد الخطوط الأساسية الدنيا للأمن السيبراني بالنسبة لمشغلي البنى التحتية الحرجة CI وCII وغيرهم. وعند وضع هذه الخطوط الأساسية، ينبغي النظر في المعايير وأفضل الممارسات المعترف بها دولياً لضمان نتائج أمنية أفضل وكفاءات أكبر.

وينبغي أن تركز خطوط الأساس الأمني على النواتج وأن توضح ما ينبغي أن تستهدفه المنظمات (''التحكم في النفاذ المنطقي إلى الموارد الحرجة'' مثلاً)، بدلاً من كيف ينبغي للمنظمات تنفيذ الجوانب الأمنية (''استخدام الاستيقان ثنائي العامل'' مثلاً)، مما يسمح بدوره للحكومة والصناعة بالاستفادة من التحسينات الأمنية المستمرة. وبالإضافة إلى ذلك، فإن اتباع نهج قائم على النواتج في تطوير خطوط الأساس هذه يترك المجال للتنفيذ بحسب القطاع أو الإرشاد بخصوص ''الكيفية''، مما يوفر للشركات المرونة اللازمة لتحديث إرشاداتها بانتظام لتعكس البيئات المتغيرة للتكنولوجيا والتهديدات.

4.4.5 استخدام طائفة واسعة من محركات السوق

ينبغي أن تنظر الاستراتيجية في طائفة واسعة من السياسات لضمان تحفيز جميع المنظمات والأفراد على الوفاء بمسؤوليات كل منها في مجال الأمن السيبراني، بما يتناسب مع المخاطر التي تواجهها، وفقاً لمبدأ النهج الشامل والأولويات المصممة بحسب الحالة (القسم 2.4).

ويمثل تحديد الثغرات بين ما تستطيع الأسواق أن تدفعه أو ما ينبغي لها أن تدفعه وما تتطلبه بيئة المخاطر خطوة حاسمة نحو تحديد موعد وكيفية الاستفادة من جملة الحوافز والمثبطات المتاحة لتحسين الأمن. ولتشجيع استيعاب معايير وممارسات الأمن السيبراني عبر البُنى التحتية الحرجة CIs وCIIs، ينبغي أن تشير الاستراتيجية إلى أن الحكومة سوف تنظر في طائفة من خيارات السياسة ومحركات السوق تحت تصرفها.

5.4.5 إنشاء شراكات بين القطاعين العام والخاص

ينبغي أن تشجع الاستراتيجية على إقامة شراكات رسمية بين القطاعين العام والخاص لتعزيز أمن البنى التحتية الحرجة CIs وCIIs. وتعتبر الشراكات بين القطاعين العام والخاص حجر الزاوية في حماية البنى التحتية الحرجة بشكل فعال وإدارة المخاطر الأمنية على المديين القصير والطويل. وهي ضرورية لتعزيز الثقة فيما بين الصناعة والحكومة.

ومع ذلك، يتطلب إنشاء شراكات مستدامة أن يكون لدى جميع أصحاب المصلحة المشاركين فهمٌ واضحٌ لأهداف الشراكة ومنافع الأمن المتبادلة التي تنبع من العمل المشترك. ويمكن أن تشمل بعض المجالات التوصل إلى اتفاق بشأن الخطوط الأساسية المشتركة للأمن السيبراني وإنشاء هياكل تنسيق فعالة وعمليات تبادل المعلومات والبروتوكولات وبناء الثقة وتحديد وتبادل الأفكار والنُّهُج وأفضل الممارسات لتحسين الأمن، فضلاً عن تحسين التنسيق الدولي.

ثمة المزيد من المراجع في الصفحتين 63 و64.

5.5 مجال التركيز 5 – المقدرة وبناء القدرات وإذكاء الوعي

يمكن أن تهيمن اعتبارات التكنولوجيا والسياسات على مناقشات الأمن السيبراني، بحيث تغفل العنصر البشري الأساسي في جوهره. ويتناول مجال التركيز هذا التحديات المتعلقة بتعزيز بناء الأمن السيبراني وإذكاء الوعي بين الهيئات الحكومية والمواطنين ومؤسسات الأعمال والمنظمات الأخرى، وهو أمر حاسم لتمكين الاقتصاد الرقمي لبلد ما.

وتشمل الممارسات الجيدة في هذا القسم وضع المناهج المخصصة للأمن السيبراني وبرامج التوعية والتوسع في برامج التدريب وبرامج تنمية القوى العاملة واعتماد خطط إصدار الشهادات الدولية وتشجيع الابتكار ومجمّعات البحث والتطوير.

1.5.5 وضع مناهج الأمن السيبراني

ينبغي أن تسهل الاستراتيجية وضع المناهج المدرسية بهدف التعجيل بتنمية مهارات الأمن السيبراني والتوعية به في جميع مراحل نظام التعليم الرسمي. وينبغي أن يشمل ذلك وضع مناهج الأمن السيبراني المخصصة في المدارس الابتدائية والثانوية ودمج دورات الأمن السيبراني في جميع علوم الحاسوب وبرامج تكنولوجيا المعلومات في التعليم العالي واستحداث درجات مخصصة للأمن السيبراني والتلمذة الحكومية.

وبالإضافة إلى ذلك، ينبغي أن تعزز المناهج المدرسية الوعي وتحفز الاهتمام بفرص العمل في مجال الأمن السيبراني. ولتعزيز الجهود في هذا المجال، ينبغي للحكومة أيضاً أن تنظر في وضع مختلف خطط الحوافز، مثل المنح الدراسية لبرامج التعليم الخاص والمنح لأنواع التلمذة ذات الصلة.

2.5.5 تحفيز تنمية المهارات وتدريب القوى العاملة

ينبغي أن تتناول الاستراتيجية وضع برامج التدريب على الأمن السيبراني وخطط تنمية المهارات للخبراء وغير الخبراء في كل من القطاعين العام والخاص. ويمكن أن تشمل الجهود توفير التدريب التنفيذي والتشغيلي، والتدريب الداخلي والتدريب المهني، والشهادات (الوطنية والدولية) لمهنيي الأمن، على أساس الاحتياجات التي تحددها الصناعة والحكومة. وينبغي استكمال التدريب التقني بمبادرات تركز على إدارة المخاطر.

كما ينبغي أن تعزز الاستراتيجية المبادرات التي تهدف إلى تطوير المسارات المهنية المخصصة للأمن السيبراني، لا سيما بالنسبة للقطاع العام، والحوافز لزيادة الإمداد بالمهنيين المؤهلين في مجال الأمن السيبراني. وينبغي إقامة هذه المشاريع بالشراكة مع الأوساط الأكاديمية والقطاع الخاص والمجتمع المدني. ولمعالجة استمرار الفجوة بين الجنسين بالنسبة للخبراء في مجال الأمن السيبراني، ينبغي النظر في نهج متوازن بين الجنسين من شأنه تحفيز وتشجيع وتيسير المزيد من المشاركة من جانب المرأة في جميع الجهود الرامية إلى تنمية المهارات والتدريب، مما يضمن الشمولية في المستقبل.

3.5.5 تنفيذ برنامج منسق للتوعية بالأمن السيبراني

ينبغي أن تسند الاستراتيجية مسؤولية تنسيق حملات وأنشطة التوعية بالأمن السيبراني على المستوى الوطني إلى سلطة مختصة لضمان ترشيد الموارد وحصر المساءلة. وينبغي أن تتعاون السلطة مع أصحاب المصلحة المعنيين لوضع وتنفيذ برامج للتوعية بالأمن السيبراني تركز على نشر المعلومات عن مخاطر وتهديدات الأمن السيبراني، وكذلك عن أفضل الممارسات للتصدي لها.

ويمكن أن يشمل برنامج التوعية بالأمن السيبراني حملات توعية تستهدف عامة الجمهور والأطفال والمعاقين رقمياً وبرامج التعليم التي تركز على المستهلك ومبادرات التوعية بين أمور أخرى، والتي تستهدف المديرين التنفيذيين في شتى دوائر القطاعين العام والخاص.

4.5.5 تشجيع الابتكار في مجال الأمن السيبراني والبحث والتطوير

ينبغي أن تعزز الاستراتيجية بيئةً تحفز البحوث الأساسية والتطبيقية في مجال الأمن السيبراني عبر القطاعات ومختلف مجموعات أصحاب المصلحة. وتشمل هذه المبادرات، على سبيل المثال، ضمان دعم جهود البحوث الوطنية لأهداف الاستراتيجية الوطنية للأمن السيبراني، ووضع برامج البحث والتطوير التي تركز على الأمن السيبراني في منظمات البحوث العامة، والنشر الفعال للنتائج الجديدة والتقنيات الأساسية والأساليب والعمليات والأدوات. وعلاوة على ذلك، وكجزء من الاستراتيجية، ينبغي أن تسعى البلدان أيضاً إلى إقامة علاقات مع المجتمع الدولي للبحوث في المجالات العلمية المتعلقة بالأمن السيبراني، مثل علوم الحاسوب والهندسة الكهربائية والرياضيات التطبيقية وعلم التجفير، بالإضافة إلى المجالات غير التقنية مثل العلوم الاجتماعية والسياسية ودراسات الأعمال والإدارة وعلم النفس، على سبيل المثال لا الحصر.

وينبغي أن تنظر الاستراتيجية في آليات الحوافز المتاحة من قبيل المنح والمشتريات والائتمانات الضريبية والمسابقات وغيرها من المبادرات التي تشجع على تطوير حلول ومنتجات وخدمات مبتكرة للأمن السيبراني.

ثمة المزيد من المراجع في الصفحتين 64 و65.

6.5 مجال التركيز 6 – التشريع والتنظيم

يتناول مجال التركيز هذا وضع إطار قانوني وتنظيمي لحماية المجتمع من الجرائم السيبرانية وتشجيع بيئة سيبرانية آمنة ومأمونة، وفقاً لمبدأي الشمولية وبيئة الثقة (القسمين 3.4 و9.4، على التوالي). ويمكن أن يشمل هذا الإطار اعتماد تشريع يحدد ما يشكل نشاطاً سيبرانياً غير قانوني، والاعتراف القانوني بالحقوق الفردية والحريات المدنية، وإنشاء آليات الامتثال، وبناء القدرة على إنفاذ الإطار، وإضفاء الطابع المؤسسي على الكيانات الحرجة، والتعاون الدولي لمكافحة الجريمة السيبرانية.

1.6.5 وضع تشريعات بشأن الجريمة السيبرانية

ينبغي أن تعزز الاستراتيجية وضع إطار قانوني محلي يحدد بوضوح ما يشكل النشاط السيبراني المحظور، وهو يهدف إلى الحدّ من الجرائم السيبرانية على الخط. وفي معظم الأحيان، تتخذ هذه المقدرة شكل تشريع بخصوص الجريمة السيبرانية، يمكن تحقيقه من خلال سن قوانين جديدة محددة أو تعديل القائم منها (مثل قانون العقوبات والقوانين التي تنظم الصيرفة والاتصالات والقطاعات الأخرى).

وينبغي أن تشجع الاستراتيجية أيضاً استحداث عملية لمراقبة تنفيذ ومراجعة التشريعات وآليات الحوكمة، واستبانة الثغرات وتداخل السلطات، وتوضيح وتحديد المجالات التي تتطلب التحديث وترتيب أولوياتها (القوانين القائمة، مثل قوانين الاتصالات القديمة).

2.6.5 الاعتراف بالحقوق والحريات الفردية وحمايتها

ينبغي للاستراتيجية أن تحمي الحقوق الأساسية في الإجراءات القانونية الواجبة (في حالة التحقيقات الجنائية والادعاء)، وكذلك حقوق حماية البيانات، بما في ذلك حماية خصوصية البيانات الشخصية (ربما من خلال وضع إطار لحماية البيانات والخصوصية) وحرية التعبير، وفقاً لمبدأ حقوق الإنسان الأساسية (القسم 5.4).

3.6.5 استحداث آليات الامتثال

ينبغي أن تشجع الاستراتيجية على وضع آليات امتثال محلية (من أجل الإنفاذ والحوافز على السواء). وينبغي وضع هذه الآليات لمنع ومكافحة وتخفيف الأعمال الموجهة ضد سرية وسلامة وتوفر أنظمة تكنولوجيا المعلومات والاتصالات والبنى التحتية، والتي تهدد البيانات الحاسوبية، وفقاً للإطار القانوني المذكور أعلاه. وينبغي لها، في جملة أمور، أن تشمل خصائص التحقيق الرقمي والاعتراض المشروع للاتصالات واستخدام الأدلة الإلكترونية.

4.6.5 تعزيز بناء القدرات لإنفاذ القانون

ينبغي أن تشجع الاستراتيجية على تطوير القدرات على إنفاذ القانون السيبراني، بما في ذلك التدريب والتعليم لطائفة من أصحاب المصلحة الضالعين في مكافحة الجريمة السيبرانية (مثل القضاة والمدعين العامين والمحامين وموظفي إنفاذ القانون والتحقيق الجنائي وغيرهم من المحققين). وينبغي أن تتلقى أجهزة إنفاذ القانون تدريباً متخصصاً لتفسير وتطبيق قوانين الجرائم السيبرانية المحلية (أي ترجمة القانون إلى مفاهيم تقنية والعكس)، والكشف الفعال عن الجرائم السيبرانية وردعها والتحقيق فيها ومقاضاة مرتكبيها، والتعاون الفعال مع دوائر الصناعة وهيئات إنفاذ القانون الدولية (مثل الإنتربول واليوروبول) للتصدي للجرائم السيبرانية ولتعزيز الأمن السيبراني. وينبغي أن يأخذ هذا العنصر في الاعتبار مجال التركيز 5 الخاص بالمقدرة وبناء القدرات وإذكاء الوعي (القسم 5.5).

5.6.5 إنشاء عمليات مشتركة بين المنظمات

ينبغي أن تحدد الاستراتيجية وتعترف بولايات الوكالات المحلية ذات السلطة الأولية لضمان الامتثال لتشريع الجريمة السيبرانية، والمسؤولين عن حماية البنى التحتية الحرجة، والمسؤولين عن ضمان تلبية جميع المتطلبات الدولية بخصوص الجريمة السيبرانية (من قبيل ضمان توافق القوانين الوطنية مع المعاهدات الدولية) وعبر خطوط الولايات القضائية (مثل التعاون عبر الحدود) (انظر أيضاً الأقسام 3.1.5 و4.1.5 و6.6.5).

وقد يحتاج الأمر، في بعض الأنظمة القانونية، إلى تشريع لإنشاء المؤسسات المعنية بالأمن السيبراني، مثل الأفرقة الوطنية CERTs/CIRTs/CSIRTs، أو لتوضيح سلطة وكالة واحدة لتنسيق السياسة السيبرانية في بلد ما.

6.6.5 دعم التعاون الدولي لمكافحة الجريمة السيبرانية

ينبغي أن تبرهن الاستراتيجية على التزام بحماية المجتمع من الجريمة السيبرانية على مستوى العالم، من خلال التصديق حيثما أمكن ووفقاً لجدول الأعمال الوطني الشامل والاتفاقات الدولية بشأن الجريمة السيبرانية أو الاتفاقات المكافئة لمكافحة الجريمة السيبرانية، ومن خلال تعزيز آليات التنسيق للتصدي للجريمة السيبرانية على المستوى الدولي. وقد يشمل ذلك مواءمة القوانين الوطنية مع المعاهدات الدولية والاتفاقات الثنائية من خلال المساعدة القانونية المتبادلة وتمكين التحقيقات والملاحقات عبر الحدود والتعامل مع الأدلة الرقمية وتسليم المجرمين. وينبغي أن يأخذ هذا العنصر في الاعتبار مجال التركيز 7 الخاص بالتعاون الدولي (القسم 7.5).

ثمة المزيد من المراجع في الصفحتين 65 و66.

7.5 مجال التركيز 7 – التعاون الدولي

يؤكد مجال التركيز هذا على العناصر التي ينبغي أن تشملها الاستراتيجية من حيث التزامات الأمن السيبراني خارج البلد المعني، سواء على المستوى الإقليمي أم الدولي. ويسهم الأمن السيبراني على نحو متزايد في العديد من المجالات المختلفة في العلاقات الدولية، بما في ذلك حقوق الإنسان والتنمية الاقتصادية والتجارة والحد من الأسلحة والأمن والاستقرار والسلم وفض المنازعات.

ولذلك ينبغي أن تعترف الاستراتيجية بالطبيعة غير الحدودية للأمن السيبراني وأن تسلط الضوء على ضرورة التعاون مع أصحاب المصلحة، لا على المستوى الوطني فحسب وإنما على المستوى الدولي أيضاً. والالتزامات الدولية مع أصحاب المصلحة من القطاعين العام والخاص عنصر أساسي في تسهيل الحوار البناء وتطوير آليات الثقة والتعاون وإيجاد حلول مقبولة متبادلة للتحديات المشتركة واستحداث ثقافة عالمية للأمن السيبراني.

ووفقاً لمبدأ النهج الشامل والأولويات المخصصة (القسم 2.4)، ينبغي تعزيز التعاون الإقليمي والدولي بالتواؤم مع البيئة السياسية والاجتماعية والثقافية والاقتصادية للبلد، فضلاً عن أولويات السياسة الخارجية.

1.7.5 لاعتراف بأهمية الأمن السيبراني كأولوية في السياسة الخارجية

ينبغي أن تعبر الاستراتيجية عن التزام بالتعاون الدولي بشأن الأمن السيبراني والاعتراف بالمسائل السيبرانية كعنصر متأصل في السياسة الخارجية للبلد. ولهذه الغاية، من المهم تشجيع تنمية واستخدام الكفاءات والمهارات التي تركز على المسائل السيبرانية (الدبلوماسية السيبرانية) لاستكمال الأساليب والعمليات الدبلوماسية التقليدية. وقد تتضمن الاستراتيجية أيضاً وضع هياكل تنظيمية محددة وإنشاء بعض المكاتب المخصصة أو الموظفين المدربين الذين يكون محور اهتمامهم المشاركة الدبلوماسية في المسائل السيبرانية.

وعلى وجه التحديد، ينبغي أن تحدد الاستراتيجية بوضوح مجالات تركيز الحكومة والأهداف طويلة الأجل للتعاون الدولي، بما في ذلك مشاركة أصحاب المصلحة (من القطاعين العام والخاص وعلى الصعيدين الإقليمي والعالمي). وقد تشمل هذه المجالات الدعم لوضع قواعد الأمن السيبراني الدولية وتدابير بناء الثقة والالتزام ببناء قدرات الأمن السيبراني والمشاركة في وضع معايير الأمن السيبراني الدولية، فضلاً عن الانضمام إلى الصكوك الإقليمية والدولية القائمة.

وقد يتطلب ذلك أيضاً مواءمةً أفضل بين مختلف الأطراف الحكومية (مثل رئاسة الدولة ومجلس الوزراء ووزارة الخارجية ووزارة الاتصالات وتكنولوجيا المعلومات ووزارة الصناعة والتجارة ووزارة العدل ووزارة الدفاع، وغيرها) بحيث يتسم موقف السياسة، الذي تعبر عنه جهة محلية ما على طاولة المفاوضات في مجال الأمن السيبراني الدولي، بالتنسيق والمواءمة بشكل صحيح مع الهيئات الحكومية الأخرى.

2.7.5 المشاركة في المناقشات الدولية

ينبغي أن تحدد الاستراتيجية آليات تعاون ومنتديات دولية معينة يرغب البلد في الانضمام إليها من أجل المشاركة بفعالية دبلوماسياً في المسائل السيبرانية. ويمكن أن تشمل هذه منظمات إقليمية أو عالمية ومناقشات حكومية دولية وتحالفات في القطاع العام و/أو الخاص، وكذلك آليات التعاون التقليدية القائمة التي تشمل مسائل الأمن السيبراني.

وعندما يشرع البلد في الاضطلاع بهذه الالتزامات، من المحتمل أن يتطلب ذلك من الحكومة تنمية كفاءات ومهارات إضافية تركز على الأمن السيبراني وزيادة قدرتها عموماً في مجال الأمن السيبراني. ولذلك من المهم ترتيب أولويات هذه الجهود وتخصيص الموارد الكافية (من الموظفين والأموال) لضمان تحقيق نتائج ملموسة.

3.7.5 تعزيز التعاون الرسمي وغير الرسمي في الفضاء السيبراني

ينبغي أن تشير الاستراتيجية إلى آليات التعاون الدولي التشغيلية التي يرغب البلد في الالتزام بها. وقد يرغب البلد في المشاركة في المساعي الدولية الرسمية وغير الرسمية لتعزيز التعاون في مجالات من قبيل وضع السياسات والتشريعات وإنفاذ القانون والتصدي للحوادث والتهديدات وتبادل المعلومات. إذ من شأن المشاركة في هذه المبادرات أن تدعم تعاوناً أفضل وتبادلاً للمعلومات بين الهيئات المعنية بشأن التهديدات المحتملة ومواطن الضعف.

4.7.5 مواءمة جهود الأمن السيبراني المحلية والدولية

ينبغي أن تنظر الاستراتيجية في مبادرات الأمن السيبراني الإقليمية والدولية القائمة وأن تعزز التنسيق والمواءمة. وهذا من شأنه أن يمكّن البلد من الاستفادة من أفضل الممارسات القائمة، فضلاً عن المساهمة في تماسك وتقارب نُهُج الأمن السيبراني.

ولهذه الغاية، ينبغي أن تبيّن الاستراتيجية التزام البلد بضمان الاتساق بين برامج السياسة المحلية والخارجية بمواءمة الإطار القانوني الوطني والسياسات الوطنية مع التزاماتها الدولية، ومواءمة نُهُج الأمن السيبراني الوطني مع الجهود الدولية.

ومن الأمثلة البارزة على الجهود الدولية الراهنة التي يمكن اعتبارها كجزء من الاستراتيجية، دون حصر، عمل فريق الخبراء الحكوميين التابع للأمم المتحدة (UN GGE) المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، ومنظمة الأمن والتعاون في أوروبا (OSCE) بشأن تدابير بناء الثقة (CBMs) والمعايير الدولية المعمول بها في مجال الفضاء السيبراني، وعمل الفريق الفرعي المعني بجرائم التكنولوجيا الرفيعة في مجموعة البلدان الصناعية G7، واتفاقية بودابست بشأن الجريمة السيبرانية المنبثقة عن مجلس أوروبا، واتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني، والاتفاق بين حكومات الدول الأعضاء في منظمة شنغهاي للتعاون في مجال ضمان أمن المعلومات الدولية، والاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات، وتوجيه الجماعة الاقتصادية لدول غرب إفريقيا (ECOWAS) بشأن مكافحة الجريمة السيبرانية، وكذلك الدعم من مركز التميز المعني بالتعاون في الدفاع السيبراني لدى حلف شمال الأطلسي (NATO CCD COE) من أجل الإصدارين 1.0 و2.0 من دليل Tallinn.

ثمة المزيد من المراجع في الصفحة 66.

6 المواد المرجعية

في سياق وضع هذا الدليل، أجري جردٌ لما هو متوفر من الأدلة وأفضل الممارسات.

وقد أمكن بذلك تحديد المواد المتاحة بالفعل لدعم البلدان في وضع إستراتيجيتها الوطنية للأمن السيبراني. وتوفر القائمة الواردة أدناه مجموعة شاملة من المواد آنفة الذكر، بما في ذلك روابط الويب.

CCI (2017), *Harare Scheme on Mutual Legal Assistance in Criminal Matters*

Carnegie Mellon (2003), *Handbook for Computer Security Incident Response Teams (CSIRTs)*

Commonwealth (2018), *Commonwealth Cyber Declaration*

CTO (2015), *Commonwealth Approach for Developing National Cyber Security Strategies*

Council of Europe (2001), *Budapest Convention on Cybercrime*

Council of the European Union (2017), *Cyber Diplomacy toolbox*

ENISA (2014), *An Evaluation Framework For National Cyber Security Strategies*

ENISA (2011), *CERT Operational Gaps and Overlaps*

ENISA (2011), *Good Practice Guide for Incident Management*

ENISA (2015), *Methodologies for the Identification of Critical Information Infrastructure Assets and Services*

ENISA (2016), *National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies*

ENISA (2012), *National Cyber Security Strategies: Practical Guide on Development and Execution*

ENISA (2012), *National Cyber Security Strategy, Setting the Course for National Efforts to Strengthen Security in Cyberspace*

ENISA (2016), *National Cyber Security Strategies: Training Tool*

ENISA (2016), *Stocktaking, Analysis and Recommendations on the Protection of CIIs*

ENISA (2016), *Strategies for Incident Response and Cyber Crisis Cooperation*

Global Cyber Security Capacity Centre, University of Oxford (2016), *Cybersecurity Capacity Maturity Model for Nations*

ITU (2017), *Securing Information and Communication Networks. Best Practices for Developing a Culture of Cybersecurity*

ITU (2017), *Global Cybersecurity Index*

ITU (2011), *National Cybersecurity Strategy Guide*

ITU (2010), *UNDERSTANDING CYBERCRIME: Phenomena, Challenges and Legal Response*

ITU (2009), *Cybersecurity Guide for Developing Countries*

Microsoft (2013), *Developing a National Strategy for Cybersecurity*

Microsoft (2014), *Critical Infrastructure Protection: Concepts and Continuum*

Microsoft (2014), *Critical Connections: Protecting Infrastructures*

Microsoft (2014), *Hierarchy of Cybersecurity Needs*

Microsoft (2018), *Building an effective national cybersecurity agency*

Microsoft (2018), *Cybersecurity Policy Framework*

Microsoft (2015), *Information Sharing Framework for Cybersecurity*

Microsoft (2017), *Risk Management for Cybersecurity: Security Baselines*

NATO CCD COE (2012), *National Cyber Security Framework Manual*

NATO CCD COE (2013), *National Cyber Security Strategy Guidelines*

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*

OAS (2015), *Best Practice for Establishing a National CSIRT*

OAS (2004), *Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*

OAS (2015), *Cyber Security Awareness Campaign Toolkit*

OAS (2015), *Report Cybersecurity and Critical Infrastructure in the Americas*

OECD (2015), *Companion Document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity*

OECD (2012), *Cybersecurity Policy Making at a Turning Point*

OECD (2015), *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*

OECD (2013), *Recommendation of the Council Concerning Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)*

OECD (2008), *Recommendation of the Council on the Protection of Critical Information Infrastructures*

OECD (2007), *Report on the Development of Policies for the Protection of Critical Information Infrastructures*

Potomac Institute for Policy Studies (2015), *Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and An Index*

United Nations (2015), *Sustainable Development Goals*

United Nations (1976), *International Covenant on Economic, Social and Cultural Rights, International Covenant on Civil and Political Rights and Optional Protocol to the International Covenant on Civil and Political Rights, Resolution 2200 (XXI)*

United Nations (2014), *The Right to Privacy in the Digital Age, Res A/RES/68/167*

United Nations (1948), *Universal Declaration of Human Rights*

UNCTAD (2014), *A Framework for Information and Communications Technology Policy Reviews*

UNCTAD, *Developing E-Commerce Legislation*

UNCTAD (2016), *Study on Data Protection Regulations and International Data Flows*

UNHR (1976), *International Covenant on Civil and Political Rights*

World Bank et al (2017), *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*

فيما يلي أدناه تفصيلٌ وافٍ للمراجع المشيرة إلى فرادى المبادئ والممارسات الجيدة

دورة حياة الاستراتيجية الوطنية للأمن السيبراني

الموضوع الفرعي	المرجع
الاستهلال	ENISA (2016), National Cyber Security Strategies: Training Tool NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3
الجرد والتحليل	ENISA (2016), National Cyber Security Strategies: Training Tool NATO CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 2.1, 2.2, 3.2.1, 3.3.1 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 3.4, 4
إنتاج الاستراتيجية الوطنية	ENISA (2016), National Cyber Security Strategies: Training Tool
التنفيذ	ENISA (2016), National Cyber Security Strategies: Training Tool
المراقبة والتقييم	ENISA (2016), National Cyber Security Strategies: Training Tool NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 3.9 NATO CCD COE (2012): National Cyber Security Framework Manual, section: 2.4

المبادئ الشاملة

الموضوع الفرعي	المرجع
الرؤية	Microsoft (2013), Developing a National Cybersecurity Strategy, p.4 NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3.1 OECD (2015), Recommendation on Digital Security Risk Management for Economic and Social Prosperity Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.1-3
النهج الشامل والأولويات المخصصة	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, p.14 Microsoft (2013), Developing a National Cybersecurity Strategy, p.5
الشمولية	CCI (2013), Checklist p2 CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies 4.5 and 4.6.6 ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services, chapter 3 ENISA (2016), An Evaluation Framework for National Cyber Security Strategies 3.2 ENISA (2016), National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace, p.9 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, p.14 ITU (2011), National Cybersecurity Strategy Guide, chapter 5.3 NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.1.3

الموضوع الفرعي	المرجع
الشمولية (تابع)	NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 3.4, 3.5, 4.3
	OAS (2015), Cyber Security Awareness Campaign Toolkit, p.20
	OAS (2015), Report on Cybersecurity and Critical Infrastructure in the Americas, p.2
	OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, p.14-15
	OECD (2013), Recommendation of the Council Con-cerning Guidelines for the Protection of Privacy and Transborder flows of Personal Data (Privacy Guidelines); Supplementary Explanatory Memoran-dum to the Revised OECD Privacy Guidelines, p.31
	Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.3-6
	UNCTAD (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development
	UNCTAD (2014), A Framework for Information and Communications Technology Policy Reviews
الازدهار الاقتصادي والاجتماعي	Microsoft (2014), Hierarchy of Cybersecurity Needs, chapter 1
	NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 1.5.1, 2.2.1
	Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.1-3
حقوق الإنسان الأساسية	CCI (2013), Checklist 2.6.5.
	CTO (2015), Commonwealth Approach for Develop-ing National Cyber Security Strategies, Principle 4
	ENISA (2014), An Evaluation Framework for Cyber Security Strategies, 3.1.1 Objectives
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, p.39

الموضوع الفرعي	المرجع
حقوق الإنسان الأساسية (تابع)	ITU (2011), National Cybersecurity Strategy Guide, chapter 7.4
	Microsoft (2013), Developing a National Cybersecurity Strategy, p.5
	NATO CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 1.3.1, 1.3.3
	NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 1.5.4, 1.5.5, 5.2.6
	OECD (2015), Companion Document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity, principle 9 and principle 3
	UNCTAD (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development
	United Nations (1948), Universal Declaration of Human Rights
	United Nations (1976), International Covenant on Economic, Social and Cultural Rights, International Covenant on Civil and Political Rights and Option-al Protocol to the International Covenant on Civil and Political Rights
	United Nations (2014), The Right to Privacy in the Digital Age
إدارة المخاطر والصمود	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.15
	Microsoft (2013), Developing a National Cybersecurity Strategy, p.6
	Microsoft (2017), Risk Management for Cybersecurity: Security Baselines
	OECD (2015), Recommendation on Digital Security Risk Management Economic and Social Prosperity and Companion Document

الموضوع الفرعي	المرجع
المجموعة الملائمة من أدوات السياسة	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 3.1 NATO CCD COE (2012): National Cyber Security Framework Manual, section: 1.4
القيادة الواضحة والأدوار وتوزيع الموارد	ENISA (2016), NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies NATO CCD COE (2012): National Cyber Security Framework Manual, section: 4 Microsoft (2018):Building an effective national cybersecurity agency Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, sections: 1-7
بيئة الثقة	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 2.2, p.25 NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3.1 Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 4, 6

الممارسات الجيدة في الاستراتيجية الوطنية للأمن السيبراني

الموضوع الفرعي	المرجع
مجال التركيز 1 – الحوكمة	CCI (2013), Checklist.
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.1, 4.4.4, 4.4.5, 4.4.8, 4.4.9, 4.4.20, 4.4.21, 4.4.34, 4.5
	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.1, 3.2, 3.4, 3.5, 3.17
	ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, sections: 2.2.1, 3.1.1, 3.1.2, 3.1.3
	ENISA (2016), National Cyber Security Strategies: Setting the course for National Efforts to Strengthen Security in Cyberspace, sections: 4, 6
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, 1.5, 1.6, p.14-15
	ITU (2011): National Cybersecurity Strategy Guide, sections: 5.2.1, 5.3, 7.2, 7.3, 11.1, 11.2, 20, 20.2
	Microsoft (2013), Developing a National Cybersecurity Strategy, sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline
	Microsoft (2018) Building an effective national cybersecurity agency
	NATO CCD COE (2013), National Cyber Security Strategy Guidelines, sections: 1.1, 3.3, 3.8
	NATO CCD COE (2012), National Cyber Security Framework Manual, sections: 1.4.2, 2.1.1 2.1.3, 2.2, 2.3, 2.4, 3.1, 3.5, 4, 5.3.1
	OECD (2012), Cybersecurity Policy Making at a Turning Point, Annex IV
	OECD (2013), Recommendation of the Council Concerning Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)
	OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document

الموضوع الفرعي	المرجع
مجال التركيز 1 – الحوكمة (تابع)	OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, section 1
مجال التركيز 2 – إدارة المخاطر في الأمن السيبراني الوطني	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.6, 4.4.15, 4.4.24, 4.4.25, 4.4.26, 4.4.27 ENISA (2016), National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.3 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.14 ITU (2011), National Cybersecurity Strategy Guide, section 10.1.2 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2013), Developing a National Cybersecurity Strategy, chapter on Building a Risk Approach NATO CCD COE (2013), National Cyber Security Strategy Guidelines, section: 3.5 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 2.1.2, 5.3.2 NIST (2015), Framework for Improving Critical Infrastructure Cybersecurity OAS (2018), Managing National Cyber Risk OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, section: 1

الموضوع الفرعي	المرجع
ممجال التركيز 3 – التأهب والصمود	Carnegie Mellon (2003), Handbook for Computer Security Incident Response Teams (CSIRTs)
	CCI (2013), Checklist
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, section: 4.4.3, 4.4.20, 4.4.21, 4.4.22, 4.4.27, 4.4.31
	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.6, 3.7, 3.10, 3.14, 4.1, 4.5, 4.8
	ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, p
	ENISA (2011), CERT Operational Gaps and Overlaps, p.
	ENISA (2011), Good Practice Guide for Incident Management, p.
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.2, p.14
	ITU (2011), National Cybersecurity Strategy Guide: 11.3, 17.3
	Microsoft (2017), Risk Management for Cybersecurity: Security Baselines
	Microsoft (2015), Information Sharing Framework for Cybersecurity
	Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Building Incident Response Capabilities
	NATO CCD COE (2013): National Cyber Security Strategy Guidelines, Section: 3.5
	NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 3.2, 4.2.2
	OAS (2016), Best Practice for Establishing a National CSIRT, p.35
	OAS (2004), Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, pp.3-4

الموضوع الفرعي	المرجع
ممجال التركيز 3 – التأهب والصمود (تابع)	OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, section: 2-B Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 2, 4
مجال التركيز 4 – خدمات البُنى التحتية الحرجة/الخدمات الأساسية	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.12, 4.4.13, 4.4.20, 4.4.25, 4.4.26, 4.4.28, 4.4.32 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, 1.4, p.14; Dimension 5.2, p.49 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.6 ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, section: 4.2 ITU (2011), National Cybersecurity Strategy Guide, sections: 5.1.1, 5.3.3, 11.4 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2014), Critical Infrastructure Protection: Concepts and Continuum, all sections Microsoft (2014), Critical Connections: Protecting Infrastructures, all sections NATO CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 3.4, 3.5 NATO CCD COE (2012), National Cyber Security Framework Manual, section: 4.5.4 OAS (2015), Report Cybersecurity and Critical Infrastructure in the Americas OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity

الموضوع الفرعي	المرجع
مجال التركيز 4 – خدمات البُنى التحتية الحرجة/الخدمات الأساسية (تابع)	OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures: Part I, Part II Potomac Institute for Policy Studies (2015): Cyber Readiness Index 2.0, sections: 2, 4
مجال التركيز 5 – المقدرة وبناء القدرات وإذكاء الوعي	CCI (2013), Checklist; CCI (2005, 2017), Commonwealth Network of Contact Persons Framework; CCI (2011), Harare Scheme on Mutual Legal Assistance in Criminal Matters; CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.11, 4.4.17, 4.4.20, 4.4.34, 4.4.12, 4.4.14, 4.4.16, 4.4.23 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.12, 3.8, 3.11, 3.13, 4.3, 4.6, 4.7, 4.14 ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, section: 2.1 ENISA (2011), CERT Operational Gaps and Overlaps, p.6, 16, 19, 21, 27, 29, 31, 32, 50, 57 ENISA (2010), Good Practice Guide for Incident Management, p.19, 23, 26, 32, 46, 56, 58, 64, 69 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.5, p.15; Dimension 2.1, 2.2., 2.3, p.25; Dimension 3-1, 3-2, 3-3, p. 32; Dimension 5.6, p.49 ITU (2011), National Cybersecurity Strategy Guide, sections: 5.3.7, 5.3.8, 12.4, 12.1, 12.3, 18 Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Driving Research and Technology Investment, Public Awareness, Workforce Training and Education; NATO CCD COE (2013, National Cyber Security Strategy Guidelines, section: 3.5

الموضوع الفرعي	المرجع
مجال التركيز 5 – المقدرة وبناء القدرات وإذكاء الوعي (تابع)	NATO CCD COE (2012), National Cyber Security Strategy Framework Manual, sections: 4.5.5, 4.6.3; OAS (2015), Cyber Security Awareness Campaign Toolkit, all sections; OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, section: 2-B Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 2, 5 UNCTAD (2015), Prgramme on E-Commerce and Law Reform
مجال التركيز 6 – التشريع والتنظيم	CCI (2013), Checklist CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4.9, 4.4.18, 4.4.19, 4.4.20 Council of Europe (2001), Budapest Convention on Cybercrime, article 15 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.15, 3.184.9, 4.12 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, 4.2, 4.3, p.39-40; Dimension 5.7, p.50 UNHR (1976), International Covenant on Civil and Political Rights, article 19 ITU (2011), National Cybersecurity Strategy Guide, sections: 5.3.4, 5.3.5, 9, 11.5, 12.2, 15 ITU (2010), ITU Toolkit for Cybercrime Legislation NATO CCD COE (2013), National Cyber Security Strategy Guidelines, section: 3.2 NATO CCD COE (2012), National Cyber Security Strategy Framework Manual, section: 5 OAS: Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, section: 3

الموضوع الفرعي	المرجع
مجال التركيز 6 – التشريع والتنظيم (تابع)	UN (2015), Sustainable Development Goals, article 16.3 UNCTAD, Global Cyberlaw Tracker World Bank et al., Combatting Cybercrime: Tools and Capacity Building for Emerging Economies
مجال التركيز 7 – التعاون الدولي	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.20, 4.4.21 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.16 and 4.10 ENISA (2016), Guidebook on National Cyber Security Strategies, section: 3.16 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.3, p.40 ITU (2011), National Cybersecurity Strategy Guide, sections: 5.3.9, 10.2.2, 13, 19 Microsoft (2013), Developing a National Strategy for Cybersecurity, section on structuring international engagement NATO CCD COE (2013), National Cyber Security Strategy Guidelines, sections: 1.3, 3.2.1, 3.3.2 NATO CCD COE (2012), National Cyber Security Strategy Framework Manual, sections: 4.7, 5.4.2, 5.4.3 OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures, chapters: 4, 5 OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, p. 13, 48, 58 Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 4, 6

7 المختصرات

المختصر	التعريف
CCI	مبادرة الكومنولث بشأن الجريمة السيبرانية
CERT	فريق الاستجابة للطوارئ الحاسوبية
CBM	تدابير بناء الثقة
CII	البنية التحتية الحرجة للمعلومات
CTO	منظمة اتصالات الكومنولث
ENISA	وكالة الاتحاد الأوروبي المعنية بأمن الشبكات والمعلومات
ICT	تكنولوجيا المعلومات والاتصالات
ITU	الاتحاد الدولي للاتصالات
NATO CCD COE	مركز التميز للدفاع السيبراني التعاوني التابع لمنظمة حلف شمال الأطلسي
NIST	المعهد الوطني للمعايير والتكنولوجيا
OAS	منظمة الدول الأمريكية
OECD	منظمة التعاون والتنمية في الميدان الاقتصادي
UN	الأمم المتحدة
UNCTAD	مؤتمر الأمم المتحدة للتجارة والتنمية

ISBN: 978-92-61-27796-3