الإنتربول

دليل الاستراتيجية الوطنية لمكافحة الجريمة السيبرية

نيسان/أبريل 2021

توطئة

لا تنفك تكنولوجيا المعلومات تزداد تأصلاً في مجتمعاتنا، وقد غدت معها الجريمة السيبرية خطراً شائعاً على الصعيد العالمي. وبوجود أكثر من 4,5 مليارات نسمة على الإنترنت، يغدو نصف سكان العالم معرضاً لخطر الوقوع ضحية للجرائم السيبرية.

وقد أدت جائحة كوفيد-19 إلى تسريع انصهار حيّزَينا المادي والسيبري وإلى زيادة تعويلنا على الاتصال الإلكتروني لدى أدائنا العديد من مهامنا الأساسية في حياتنا الشخصية وحياتنا المهنية على حد سواء.

وبيئة الجريمة السيبرية، إذ تزداد تعقيداً وتقترن بها التحديات الملازمة للتحقيقات عبر الحدود، قد فرضت ضغوطاً إضافية على أجهزة إنفاذ القانون حول العالم.

وفيما يعكف القطاع الخاص على تحويل نفسه، لا يزال القطاع العام يواجه تحديات فرضها الافتقار إلى المعلومات والاستراتيجيات والموارد والبنى التحتية والشراكات.

ومن المهم أن تقر أجهزة إنفاذ القانون بأن التدابير والممارسات والسياسات الحالية قد لا ترقى إلى المستوى الكافي لمواجهة الجريمة السيبرية التي لا تنفك تتغير في عالم اليوم وأن تحدد الخطوات الواجب اتخاذها لتدارك هذا النقص.

وعلى القطاع العام أن يعزز تأهبه وفعاليته وقيادته تحقيقاً للقدرة السيبرية الجماعية على الصمود. فالأمن السيبري لهو مسؤولية مشتركة وهدف مشترك في آنٍ معاً لا بد من أن نصبو باستمرار إلى بلوغه.

وعندما يتكرر استخدام الأساليب والتكتيكات نفسها في الهجمات التي تستهدف مختلف القطاعات حول العالم، إذّاك تتضح بأجلى بيان القيمة الحقيقية للإنتربول بما يمثله من منبر عالمي يساعد المحققين على تبادل المعلومات بشكل مأمون والتحرك بسرعة.

وفي إطار هذه الجهود الرامية إلى دعم البلدان الأعضاء في منظمتنا، من دواعي فخري أن أقدّم لكم **دليل الاستراتيجية الوطنية لمكافحة الجريمة السيبرية من إعداد الإنتربول**.

عالمنا يزداد ترابطاً يوماً بعد يوم ولن ينكفئ الإنتربول عن الاضطلاع بدور مركزي وفريد بوصفه طرفاً في الأسرة العالمية لأجهزة إنفاذ القانون في كفاحنا المشترك ضد الجريمة السيبرية.

يورغن شتوك
الأمين العام للإنتربول

مقدمة

لقد دخلنا مرحلة ينصهر فيها الحيّزان السيبري والمادي، فيما زاد التحول الرقمي من تعويلنا على الاتصال الإلكتروني.

وشهدت أجهزة إنفاذ القانون في كافة أنحاء العالم بالتجربة المباشرة الجوانب الإجرامية الفريدة التي تمخضت عن جائحة كوفيد-19، وأبرزها الأثر المتنامي والمتشعب للجريمة السيبرية. وقد دفعتنا هذه الظاهرة إلى إعادة التفكير في استجابتنا العالمية وإلى استخدام شبكتنا العالمية الزاخرة بأجهزة إنفاذ القانون تحقيقاً لمساعٍ أخرى.

وفي شهر آب/أغسطس 2020، أصدر الإنتربول تقريراً تناول فيه أثر جائحة فيروس كورونا في البيئة العالمية للتهديدات السيبرية، وسلّط التقرير الضوء على الاستراتيجيات الوطنية لمكافحة الجريمة السيبرية باعتبارها وسيلة لبناء قدرة البنى التحتية والخدمات الوطنية على الصمود، بما يساعد البلدان على مواجهة التهديدات السيبرية بشكل فعال وحماية مجتمعاتها من الهجمات السيبرية خلال الجائحة وبعدها.

وفي إطار الولاية المتمثلة في "التخفيف من تبعات الجريمة السيبرية على الصعيد العالمي وحماية المجتمعات المحلية منها وجعل العالم أكثر أماناً"، تتولى إدارة مكافحة الجريمة السيبرية في الإنتربول توفير القدرات الشرطية اللازمة للتصدي للجريمة السيبرية. وأحد أبرز أهداف الإدارة هو تمتين وتعزيز قدرات البلدان الأعضاء بهدف منع الجريمة السيبرية وكشفها والتحقيق فيها.

ويوفر هذا الدليل للبلدان الأعضاء في الإنتربول مرجعاً قيّماً لوضع أو تحديث استراتيجياتها الوطنية لمكافحة الجريمة السيبرية. ويساعد الدليل البلدان أيضاً على تكوين رؤية متعمقة عن استجابتها الحالية للجريمة السيبرية، ويوفر لها وسيلة لتصميم استراتيجية وبرنامج أكثر متانة للتغلب على التحديات التي تعيقها عن التصدي بفعالية أكبر للجريمة السيبرية.

وإني لأوصي البلدان الأعضاء في منظمتنا بالاطلاع على هذا الدليل لما فيه من محتوى يعزز قدرة البلدان على الصمود والتكيف في هذا العالم شديد الرقمية لمكافحة الجريمة السيبرية مكافحة فعالة.

كريغ جونز

مدير إدارة مكافحة الجريمة السيبرية

(ترجم هذا النص وراجعه مترجم خارجي معتمد من الإنتربول)

المحتويات

1. مقدمة 8
2. الجريمة السيبرية والأمن السيبري 9
1.2 صعوبة التعريف بالجريمة السيبرية 9
2.2 مقارنة بين جريمة يعتمد ارتكابها على الإنترنت وجريمة يسهّل الإنترنت ارتكابها 11
3.2 الأمن السيبري والجريمة السيبرية 11
3. عوامل تسهّل ارتكاب الجريمة السيبرية 13
1.3 الاتصال الإلكتروني: أعداد متزايدة من الأفراد المتصلين بالإنترنت وعيهم بالأمن الرقمي متدنٍ 13
2.3 حراك الموظفين: مؤسسات تجارية لديها موظفون يعملون عن بُعد عبر شبكات أقل أماناً 14
3.3 الترابط الإلكتروني: انتقال المدن والمساكن إلى الإنترنت، ما أوجد أشكال ضعف جديدة 14
4.3 الحنكة: للجهات الفاعلة مصدر التهديد مهارات وتكتيكات متطورة 15
5.3 نقص في التبليغ: الإحجام عن التبليغ عن الجرائم السيبرية 16
6.3 التشريعات والولاية القضائية: الافتقار إلى تجريم الجرائم الإلكترونية والتعقيدات لدى تداخل الولايات القضائية 17
4. المنهجية: وضع استراتيجية لمكافحة الجريمة السيبرية 18
1.4 تهيئة الساحة للاستراتيجية 18
2.4 صياغة الاستراتيجية 22
3.4 اعتماد الاستراتيجية 29
4.4 تنفيذ الاستراتيجية 29
5.4 متابعة الاستراتيجية وتقييمها 30
6.4 إدخال التعديلات على الاستراتيجية والابتكار 30
5. اتفاقية بودابست 32
1.5 معلومات عن الاتفاقية 32
2.5 مزايا الاتفاقية 33
3.5 الانضمام إلى الاتفاقية 33
6. نموذج استراتيجية مكافحة الجريمة السيبرية 34
1.6 المقدمة 34
2.6 البيئة الحالية للجريمة السيبرية 35
3.6 الرؤية 36
4.6 مجالات التركيز والأهداف الاستراتيجية الفرعية والإجراءات 37
التذييل ألف: الجريمة السيبرية والأمن السيبرية: الاستراتيجيات والأنظمة الوطنية 43

المختصرات

ASEAN - رابطة بلدان جنوب شرق آسيا

ACCDP - مشروع إنماء القدرات السيبرية في بلدان رابطة أمم جنوب شرق آسيا

CERT - فريق التصدي للطوارئ الحاسوبية

CSIRT - فريق التحرك إزاء الحوادث المتصلة بأمن الحاسوب

DDoS - هجمات تعطيل الخدمة

يوروبول - وكالة الاتحاد الأوروبي للتعاون بين أجهزة إنفاذ القانون

ICT - تكنولوجيا المعلومات والاتصالات

IoT - إنترنت الأشياء

IP - بروتوكول الإنترنت

ITU - الاتحاد الدولي للاتصالات

MLAT - معاهدة المساعدة القانونية المتبادلة

SMART - محددة، وقابلة للقياس، ويمكن تحقيقها، ومرتبطة بالنشاط، ومحددة زمنياً

UNODC - مكتب الأمم المتحدة المعني بالمخدرات والجريمة

الكتّاب

شاين كروس وسايمون هيرل – الإنتربول

ماي آن ليم – شركة TRPC Pte Ltd

شكر وتقدير

تسنى نشر هذا الدليل بفضل الجهود التي بذلها كثيرون خلال مختلف مراحل إعداده. وقد تم عقد العديد من الاستشارات وحلقات العمل وعمليات المراجعة من جانب الأقران والاجتماعات التي وفرت الإسهامات، ويهم مشروع إنماء القدرات السيبرية في بلدان رابطة أمم جنوب شرق آسيا أن يتوجه بخالص الشكر إلى الأشخاص الذين ترد في ما يلي أسماؤهم على إسهاماتهم في مختلف مراحل إعداد الدليل:

- ستيف هونيس – الشركة الاستشارية Aardwolf Consulting Ltd
- بنجامين أنغ – مدرسة س. راجارتنام للدراسات الدولية، جامعة نانيانغ التكنولوجية، سنغافورة
- كلير بلاكروز
- أنتوني تيلوكسينغ – وزارة العدل في الولايات المتحدة
- عائشة أحمد بن حاجي – وزارة الداخلية – مملكة البحرين
- جيني تسانغ وآخرون – شرطة هونغ كونغ
- د. كريستوس فيلاسكو
- يويتشي كوموتا – المركز الوطني لتتأهب للحوادث واستراتيجية الأمن السيبري، اليابان
- إسماموراديي عبد القادر – وكالة الأمن السيبري في ماليزيا
- ممثلو بلدان رابطة ASEAN في حلقة العمل الاستهلالية لمشروع ACCDP
- دونغ أوك كيم، بي لينغ لي، وي تشان تي، الإنتربول

إشعار قانوني

يحتوي دليل الاستراتيجية الوطنية لمكافحة الجريمة السيبرية ("الدليل") على معلومات وإرشادات عامة حول كيفية فهم الجريمة السيبرية والتعامل معها من منظور استراتيجي، وذلك بهدف وضع استراتيجية وطنية لمكافحة الجريمة السيبرية أو تعزيز الاستراتيجية المعتمَدة. وترد المعلومات المذكورة في الدليل من البلدان الأعضاء وشركاء من القطاع الخاص والمصادر المفتوحة. وتستند الخبرات والإرشادات الواردة في هذا الدليل إلى هذه المعلومات، وهي معروضة ليطّلع عليها القارئ بناء على حسن تقديره.

ويُقصد بالأمثلة والأوصاف والمناقشات الواردة في هذا الدليل أن تكون خيارات يمكن النظر فيها، لا توصيات أو دعوات تحفيزية أو مقترحات نهائية. ولدى اتخاذ أي إجراءات أو مقترحات أو تدابير أو سياسات جرى وضعها انطلاقاً من هذا الدليل، لا بد من الركون إلى القوانين السارية التي يتحقق منها ويختبرها القرّاء المعنيون في الولايات القضائية ذات الصلة.

ولا ترد الروابط للمنشورات أو المواقع الإلكترونية المضمّنة في هذا الدليل إلا كمراجع حصراً، ولا تُعد تزكية من جانب الإنتربول لتلك المنشورات أو محتوياتها. والمستخدم مسؤول عن تقييم المحتوى ومدى فائدة المعلومات المستمدة من منشورات/مواقع إلكترونية أخرى.

ولا ترد أوصاف أحكام بعض الصكوك القانونية المضمّنة في هذه الوثيقة إلا كمناقشات، وهي ليست بمثابة مقترحات بشأن التفسيرات السارية في ما يتعلق بأي من هذه الصكوك القانونية، ولا يجوز تفسيرها على أنها كذلك.

ولا يرد نموذج استراتيجية مكافحة الجريمة السيبرية في هذا الدليل إلا لأغراض تعليمية وكمثال/مقترَح يمكن النظر فيه، وهو ليس ملزماً ولا يزكيه الإنتربول باعتباره استراتيجية فعالة بأي شكل من الأشكال، وأمر اعتماده متروك لحسن تقدير القارئ، ولا بد من اعتباره خاضعاً للسياسات والقوانين والظروف السارية في البلد المعني. ولا يتحمل الإنتربول المسؤولية عن أي ضرر أو أذية ناجمين عن اعتماد الدليل في أي ولاية قضائية.

إشعار بحقوق التأليف والنشر

1. مقدمة

الخلفية

أُعد هذا الدليل في إطار المرحلة الثانية من مشروع إنماء القدرات السيبرية في بلدان رابطة أمم جنوب شرق آسيا (ACCDP II)، ويحظى مشروع ACCDP بتمويل من صندوق التكامل المشترك بين اليابان ورابطة أمم جنوب شرق آسيا (JAIF 2.0)، عن طريق سكرتارية ASEAN ووزارة الداخلية في سنغافورة بصفتهما الجهتين المقترحتين للمشروع، بينما يتولى الإنتربول مسؤولية تنفيذ المشروع.

ويرمي هذا المشروع إلى تعزيز قدرات البلدان على مكافحة الجريمة السيبرية وعلى التعاون في ما بينها كمنطقة وعلى الصعيد الدولي. ويتطرق مشروع ACCDP على وجه التحديد إلى حاجة سلطات العدالة الجنائية إلى بناء مهاراتها السيبرية ومعارفها وشراكاتها الإقليمية من خلال أنشطة ومنتجات مصممة خصيصاً لها.

ويندرج مشروع ACCDP في إطار تصدي الإنتربول على المستوى العالمي للجريمة السيبرية، وهو يدعم تنفيذ استراتيجيته العالمية لمكافحة الجريمة السيبرية. ويدعم الإنتربول الجهود الوطنية في مكافحة الجريمة السيبرية ويعتبرها أحد مجالات التركيز العالمية إلى جانب الإرهاب والجريمة المنظمة.

المنهجية والنهج المتبعان في إعداد الدليل

كشفت النتائج الموحدة لعمليات التقييم القطرية (استعراض وضع الجريمة السيبرية في البلدان الأعضاء) التي أجريت في المرحلة الأولى من مشروع ACCDP وجود حاجة واضحة إلى استراتيجية لمكافحة الجريمة السيبرية لدى العديد من البلدان الأعضاء في رابطة ASEAN. ولهذا جرى إعداد هذا الدليل في المرحلة الثانية من مشروع ACCDP.

وبدأ العمل على إعداد الدليل بحلقة عمل امتدت على أسبوع واحد وشارك فيها ممثلون عن أجهزة إنفاذ القانون والأجهزة السيبرية الوطنية ومستشارون خارجيون، وأُلحق ذلك بمداخلات قدمها مختلف الخبراء من الإنتربول والبلدان الأعضاء فيه.

وليست المعلومات الواردة في هذا الدليل مخصصة لأي منطقة بالتحديد، بل هي تفصّل الممارسات الجيدة المعتمَدة دولياً.

الغرض من الدليل

أُعد هذا الدليل لكيما يستخدمه أي بلد يتطلع إلى وضع استراتيجية وطنية لمكافحة الجريمة السيبرية أو إلى مراجعة الاستراتيجية المعتمَدة أو تحسينها.

لاحظ المشروع وجود تفاوت كبير بين مختلف المبادرات والقوانين والعمليات المتبعة في البلدان الأعضاء في الإنتربول، وأكد على أهمية مواءمتها بشكل أوثق مع الممارسات الدولية الجيدة.

وقد أُعد هذا الدليل لتوفير نهج منهجي لدى إعداد أو تحديث استراتيجية مكافحة الجريمة السيبرية، لما قد تطرحه هذه المهمة من تحديات.

2. الجريمة السيبرية والأمن السيبري

1.2 صعوبة التعريف بالجريمة السيبرية

ما من تعريف مقبول عموماً للجريمة السيبرية، والنهج الأكثر شيوعاً يقضي بتعريف أبرز المصطلحات المستخدمة في التحقيقات في الجرائم السيبرية. وتسمح لنا دراسة المصطلحات الشائع استخدامها بتحديد أبرز المفاهيم واستخدام هذه التعريفات باتساق في استراتيجية البلد لمكافحة الجريمة السيبرية.

ومن الأمثلة على هذا النهج القانون النموذجي الصادر في عام 2017 عن رابطة الكومنولث بشأن الحواسيب والجرائم المتصلة بها ("القانون النموذجي للكومنولث)[1]. يبدأ القانون بتعريف بعض أبرز المصطلحات، ومنها "البيانات الحاسوبية"، و"وسيط تخزين البيانات الحاسوبية" و"مقدم الخدمة" و"بيانات المرور". وبعد التعريف بأبرز المصطلحات، ينتقل القانون النموذجي للكومنولث إلى تحديد الجرائم الأساسية التي يعتبر أنها تندرج في خانة الجريمة السيبرية، وهي – (1) النفاذ غير المشروع، (2) التدخل في البيانات، (3) التدخل في النظم الحاسوبية، (4) الاعتراض غير المشروع لحركة البيانات، (5) الأجهزة غير القانونية، (6) استغلال الأطفال في مواد إباحية.

وهذا النهج مشابه للغاية للاتفاقية المتعلقة بالجريمة الإلكترونية الصادرة عن مجلس أوروبا (اتفاقية بودابست)[2]، فالأخيرة تحتوي على تعريفات أولية لـــ "النظام الحاسوبي"، و"البيانات الحاسوبية"، و"مقدم الخدمة"، و"بيانات المرور". ثم تنتقل الاتفاقية إلى تحديد أربع فئات من الجرائم المرتكبة بواسطة النظم الحاسوبية وتكنولوجيا المعلومات، وهي:

- الفئة الأولى: جرائم تستهدف السرية وسلامة وتوفر البيانات والنظم المعلوماتية – أي النفاذ غير المشروع، والاعتراض غير المشروع، والتدخل في البيانات، والتدخل في النظم، وإساءة استخدام الأجهزة؛
- الفئة الثانية: الجرائم المرتبطة بالحواسيب – التزوير المرتبط بالحاسوب والاحتيال المرتبط بالحاسوب؛
- الفئة الثالثة: الجرائم المرتبطة بالمحتوى – استغلال الأطفال في مواد إباحية؛
- الفئة الرابعة: جرائم انتهاك حقوق التأليف والنشر والحقوق ذات الصلة؛
- الفئة الخامسة: المسؤوليات الإضافية والعقوبات – المحاولة، والمساعدة أو التحريض، ومسؤولية الشركات.

[1] https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf

[2] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

الجدول 1: مقارنة بين أبرز المصطلحات في مجال الجريمة السيبرية

المصطلح المعرَّف	القانون النموذجي للكومنولث	اتفاقية بودابست
البيانات الحاسوبية (بيانات الكومبيوتر)	يُقصد بـــ "بيانات الكومبيوتر" أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر، بما في ذلك برنامج مناسب يساعد نظام كومبيوتر في أداء وظيفة معين.	يُقصد بـــ "بيانات الكومبيوتر" أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر، بما في ذلك برنامج مناسب يساعد نظام كومبيوتر في أداء وظيفة معين.
وسيط تخزين البيانات الحاسوبية	يُقصد بـــ "وسيط تخزين البيانات الحاسوبية" أي وسيلة أو أداة (قرص مثلاً) يمكن إعادة إنتاج المعلومات منها، مع أو بدون مساعدة أي وسيلة أو جهاز آخر.	(لا تعرّف هذا المصطلح)
نظام حاسوبي (منظومة الكومبيوتر)	يُقصد بـــ " منظومة الكومبيوتر " أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، بما فيها ذلك الإنترنت، والتي يقوم واحد منها أو أكثر، وفقاً لبرنامج، بالمعالجة الآلية للبيانات أو أي وظيفة أخرى.	يُقصد بـــ " منظومة الكومبيوتر " أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر، وفقاً لبرنامج، بالمعالجة الآلية للبيانات.
مقدم خدمات	يُقصد بـــ "مقدم الخدمة": (1) أي كيان عام أو خاص يقدم لمستخدمي الخدمة التي يوفرها القدرة على الاتصال عن طريق نظام الكومبيوتر، و(2) أي كيان آخر يقوم بمعالجة بيانات الكومبيوتر أو تخزينها نيابة عن مزود خدمة الاتصالات أو مستخدميها.	يُقصد بـــ "مقدم الخدمة": (1) أي كيان عام أو خاص يقدم لمستخدمي الخدمة التي يوفرها القدرة على الاتصال عن طريق نظام الكومبيوتر، و (2) أي كيان آخر يقوم بمعالجة بيانات الكومبيوتر أو تخزينها نيابة عن مزود خدمة الاتصالات أو مستخدمي هذه الخدمة.
بيانات المرور (بيانات حركة الاتصالات)	يُقصد بـــ "بيانات المرور" أي بيانات كمبيوتر: (أ) تتعلق باتصال عن طريق نظام كمبيوتر؛ و(ب) تنشأ عن نظام كمبيوتر يشكل جزءاً من سلسلة الاتصالات؛ و(ج) تشير إلى مصدر الاتصال ووجهته ومساره ووقته وتاريخه وحجمه ومدته أو نوع الخدمات الأساسية.	يُقصد بـــ "بيانات المرور" أي بيانات كمبيوتر تتعلق باتصال عن طريق نظام كمبيوتر، وتنشأ عن نظام كمبيوتر يشكل جزءاً في سلسلة الاتصالات، وتشير إلى مصدر الاتصال ووجهته ومساره ووقته وتاريخه وحجمه ومدته أو نوع الخدمة الأساسية.

يمكن أن تكون النتائج الإيجابية للتحقيقات في الجرائم السيبرية رهناً بالنجاح في جمع الأدلة الرقمية وتحليلها وإثباتها. ويُستخدم مصطلح 'الأدلة الرقمية' بالتبادل مع مصطلح الأدلة الإلكترونية ويشير إلى المعلومات والبيانات التي يتم تخزينها أو استلامها أو إرسالها بواسطة جهاز إلكتروني، وهو ما يشمل الأدلة المستقاة من الأجهزة الرقمية أو السجلات الواردة من مقدمي الخدمات عبر الإنترنت.

2.2 مقارنة بين جريمة يعتمد ارتكابها على الإنترنت وجريمة يسهّل الإنترنت ارتكابها

بالإضافة إلى تحديد أبرز المصطلحات المتعلقة بالجريمة السيبرية – وهي التي بدورها يمكن أن تكون مصطلحاً فضفاضاً ينطوي على جملة من الجرائم – لا بد من التمييز بين 'جريمة يعتمد ارتكابها على الإنترنت' من جهة ويُشار إليها أيضاً بمصطلح 'جريمة سيبرية محضة'، و'جريمة يسهّل الإنترنت ارتكابها' من جهة أخرى. وقد أصدرت وزارة الداخلية في المملكة المتحدة سلسلة من الوثائق البحثية والتحليلية بعنوان "الجريمة السيبرية: مراجعة للأدلة"[3]، وهي تشكل مرجعاً مفيداً وتميّز في متنها بين هذه المفهومين:

- 'الجرائم التي يعتمد ارتكابها على الإنترنت' (أو 'الجرائم السيبرية المحضة') هي جرائم لا يمكن ارتكابها إلا باستخدام الحاسوب أو الشبكات المعلوماتية أو أشكال أخرى من تكنولوجيا المعلومات والاتصالات. ومن هذه الأفعال نشر الفيروسات أو غيرها من البرمجيات الخبيثة والاختراق وهجمات تعطيل الخدمة (DDoS). وهي بمثابة أنشطة تستهدف أساساً الحواسيب أو الموارد الشبكية، علماً بأنه قد تنجم أيضاً عن الهجمات مجموعة من النتائج الثانوية. وعلى سبيل المثال، قد يُصار إلى استخدام البيانات التي تم جمعها عبر اختراق حسابات البريد الإلكتروني لاحقاً لارتكاب عمليات احتيال[4].

- الجرائم التي يسهّل الإنترنت ارتكابها هي جرائم عادية يمكن توسيع نطاقها أو مدى وصولها من خلال استخدام الحواسيب أو الشبكات المعلوماتية أو أشكال أخرى من تكنولوجيا المعلومات والاتصالات. وبخلاف الجرائم التي يعتمد ارتكابها على الإنترنت وعلى تكنولوجيا المعلومات والاتصالات حصراً، يمكن ارتكاب الجرائم الأساسية المندرجة في خانة الجرائم التي يسهّل الإنترنت ارتكابها من دون استخدام تكنولوجيا المعلومات والاتصالات. ويُعتبر الاحتيال والسرقة اثنين من أكثر أنواع الجرائم التي يسهّل الإنترنت ارتكابها انتشاراً[5]. ومن الأمثلة على ذلك رسائل البريد الإلكتروني الاحتيالية التي تحاول الإيقاع بمستلميها حتى يحوّلوا الأموال إلى مرسل غير معروف.

3.2 الأمن السيبري والجريمة السيبرية

ولئن كان 'الأمن السيبري' و'الجريمة السيبرية' مفهومين مترابطين غالباً ما تتقاطع مجالات اهتمامهما، إلا أن معانيهما ليسا على تطابق، ونطاق ما يندرج في إطار 'الأمن السيبري' و'الجريمة السيبرية' يختلف باختلاف وجهات النظر الفنية والقانونية والسياسية.

ويسلط الجدول أدناه بعض الضوء على نطاق كل مجال تنظيمي:

---

[3] https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

الجدول 2: تعريف الأمن السيبري والجريمة السيبرية

الجريمة السيبرية	الأمن السيبري
	التعريف
تُعرّف الجريمة السيبرية بأنها الجرائم التي تستهدف البيانات الحاسوبية ووسائط تخزينها والنظم الحاسوبية ومقدمي الخدمات. ويتناول المفهوم عادة جملة من فئات الجرائم، ومنها مثلاً النفاذ غير المشروع، والتدخل في البيانات والنظم الحاسوبية، والاحتيال والتزوير، واستغلال الأطفال، والتعدي على الملكية الفكرية.	يُعرّف الأمن السيبري عادة بأنه حماية سرية وسلامة وتوفر البيانات والنظم الحاسوبية بهدف تعزيز أمن تكنولوجيا المعلومات والاتصالات وقدرتها على الصمود ومصداقيتها والثقة فيها. ويتناول المفهوم عادة الجوانب السياسية (المصالح الوطنية والأمن) والفنية والإدارية.
	التركيز على الجانب التنظيمي
تركز الأنظمة في مجال الجريمة السيبرية على تحديد ما يعتبره البلد جرائم يعتمد ارتكابها على الإنترنت وجرائم يسهّل الإنترنت ارتكابها، فتزوّد البلد بالأدوات التي تتيح له تجريم الانتهاكات والتفويض بفتح التحقيقات والملاحقة القضائية للانتهاكات في إطار الجريمة السيبرية. وتركز الأنظمة في مجال الجريمة السيبرية على القانون الموضوعي، أي مثلاً إساءة استخدام الأجهزة، والقانون الإجرائي، أي مثلاً الحفاظ على البيانات، وغير ذلك من الأحكام القانونية ومنها مثلاً معاهدات المساعدة القانونية المتبادلة وجمع الأدلة. ووُضعت هذه الأنظمة لحماية المواطنين عبر تحديد هوية المسؤولين عن ارتكاب الجرائم وإحباط عملياتهم وسوقهم كأفراد/جماعات إجرامية منظمة إلى العدالة.	تركز الأنظمة في مجال الأمن السيبري على حماية البنية التحتية الوطنية والقطاعين العام والخاص من الهجمات السيبرية. والوضع المتين في مجال الأمن السيبري إنما يعني حماية النظم الحاسوبية من الدخول غير المصرح إليها أو إلحاق الأضرار بها أو تعطيل إمكانية الدخول إليها. ويهدف الأمن السيبري إلى الحد من مخاطر الهجمات السيبرية ويحمي النظم والشبكات والتقنيات من الاستغلال غير المصرح، وذلك باستخدام مجموعة من التقنيات والعمليات والضوابط على المستويات التقنية والإجرائية والمؤسسية. ويركز الأمن السيبري على السياسة العامة والإجراءات اللازمة لتأمين النظم والأصول وحمايتها.
	التسلسل الزمني للحوادث
تحدد عموماً الأنظمة في مجال الجريمة السيبرية الأنشطة الإجرامية في الحيز السيبري وتكشفها بعد أن تكون قد وقعت، وهي تزود أجهزة إنفاذ القانون بالصلاحيات اللازمة للتحقيق في الأنشطة بعد وقوعها بهدف سوق المجرمين إلى العدالة.	تعمل عادة الأنظمة في مجال الأمن السيبري على منع الهجمات قبل وقوعها، فالأمن عبارة عن دورة مستمرة تشمل التصدي للحوادث ومراجعة العمليات التي تجري بعد كشف الانتهاك.

ينبغي، بل ويجب على استراتيجية مكافحة الجريمة السيبرية أن تعمل باتساق وثيق مع استراتيجية الأمن السيبري. ففي بعض الحوادث السيبرية، قد لا يكون واضحاً في البداية ما إذا كانت المسألة حادثاً في مجال الأمن السيبري يطال البنية التحتية الشخصية أو المؤسسية أو الوطنية، أو حادثاً في مجال الجريمة السيبرية أي ما يعني ارتكاب جريمة فعلية، أو حادثاً يشمل المجالين.

- في حال وقوع حادث في مجال الجريمة السيبرية، على أجهزة إنفاذ القانون ومنظومة العدالة الجنائية أن تستجيب لها، أي مثلاً الجهاز المسؤول عن التحقيق في الجرائم السيبرية.
- وفي حال وقوع حادث في مجال الأمن السيبري، ينبغي إيفاد الجهاز أو الكيان ذي الصلة المسؤول عن الأمن السيبري، أي مثلاً فريق التصدي للطوارئ الحاسوبية (CERT) أو أفرقة التحرك إزاء الحوادث المتصلة بأمن الحاسوب (CSIRT).

وأصدرت الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA) تقريراً في عام 2017 بعنوان "الأدوات والمنهجيات لدعم التعاون بين أفرقة CSIRTs وأجهزة إنفاذ القانون[6]، وأكد التقرير على أن أفرقة CSIRTs وأجهزة إنفاذ القانون غالباً ما تتبادل المعلومات لدى التعامل مع الحوادث/التحقيق فيها، سواء بشكل رسمي أو غير رسمي. واعتُبرت الثقة عاملاً أساسياً لضمان التعاون المثمر. وشدد التقرير على أنه، ولئن كانت لدى أفرقة CSIRTs وأجهزة إنفاذ القانون أهداف وأساليب مختلفة لجمع المعلومات ومعاملتها، إلا أن الطرفين بات لديهما فهم متبادل آخذ بالازدياد لاحتياجات الآخر[7].

وفي حال لم يضع بلد ما بعد *استراتيجية للأمن السيبري* وينفذها، فإن الوثيقة الصادرة عن وكالة ENISA بعنوان "دليل الممارسات الجيدة لوضع استراتيجية وطنية للأمن السيبري" مفيدة ويمكن أن تساعد في هذا المسعى[8].

3. عوامل تسهّل ارتكاب الجريمة السيبرية

ساهم عدد من العوامل في إيجاد بيئة مربحة للمجرمين السيبريين وعدد لا يُستهان به من ضحاياهم المحتملين. ومن هذه العوامل على سبيل المثال لا الحصر:

1.3 الاتصال الإلكتروني: أعداد متزايدة من الأفراد المتصلين بالإنترنت وعيهم بالأمن الرقمي متدنٍ

يزداد سريعاً عدد مستخدمي الإنترنت، وهو ما يُترجم مباشرة إلى ما يرتبط بذلك من زيادة في استخدام الأجهزة المحمولة وانتشار التجارة الإلكترونية والمعاملات الإلكترونية والاتصالات الإلكترونية. وضعف الوعي عموماً بالأمن السيبري وتدابير الوقائية السيبرية، لا سيما لدى المستخدمين من الفئات الهشة مثل كبار السن، **قد أدى إلى طفرة حادة في أعداد ضحايا الجرائم السيبرية.**

- كشفت دراسة أجرتها جامعة بحثية أمريكية في عام 2018 أن السواد الأعظم من مستخدمي الإنترنت في منازلهم يفتقرون إلى بالأمن السيبري، أي أنهم مثلاً لا يدرون ما هو الفرق بين برمجيات مكافحة الفيروسات والجدران النارية، وأن تدابير الوقاية السيبرية لديهم إنما هي دون المستوى، فـــ 67 بالمئة من المشاركين في الاستطلاع لم تكن برمجياتهم لمكافحة الفيروسات محدَّثة، بل و لم تكن هذه البرمجيات مثبّتة

[6] https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement
[7] https://www.enisa.europa.eu/publications/csirts-le-cooperation/at_download/fullReport
[8] https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

أصلاً في بعض الحالات. ويشارك أيضاً مستخدمون كثر الآخرين كلمات السر الخاصة بهم بكل طيب خاطر ويسارعون إلى تشاطر المعلومات الخاصة عبر شبكات التواصل الاجتماعي[9].

2.3 حراك الموظفين: مؤسسات تجارية لديها موظفون يعملون عن بُعد عبر شبكات أقل أماناً

أدى ازدياد حراك الموظفين والوصول الأوسع إلى الشبكة إلى ارتفاع حاد في عدد الموظفين العاملين عن بُعد، بما في ذلك من منازلهم. وهو ما تُرجم مباشرة إلى زيادة في المعاملات والاتصالات التجارية والرسمية عبر شبكات ونظم حاسوبية عامة أو منزلية أقل أماناً (أي مثلاً الموظفون العاملون من المقاهي)، **مما فاقم من هشاشة شبكات الشركات ووسّع رقعة الهجمات التي يشنها المجرمون السيبريون.**

- كشفت دراسة صادرة عن الإنتربول في آب/أغسطس 2020 أن التصيد الاحتيالي والاحتيال عبر الإنترنت وغير ذلك من التهديدات السيبرية زادت بنسبة 59 بالمئة بعد تفشي جائحة كوفيد-19[10].
- ومن جملة تهديدات أخرى، أفاد المنتدى الاقتصادي العالمي في آذار/مارس 2020 عن حاجة المؤسسات التجارية الانتقال لاعتماد ترتيبات تتيح العمل من المنزل حرصاً منها على إيجاد سبيل آمن يمكّن الموظفين من الاتصال بالتطبيقات التي لا غنى عنها لتسيير الأعمال. وبرزت كذلك الحاجة إلى ضمان حماية نقطة النهاية لكل الأجهزة التي يستخدمها الموظفون للوصول إلى موارد العمل عبر الإنترنت، فاعتُمدت مثلاً المصادقة متعددة العوامل[11].

3.3 الترابط الإلكتروني: انتقال المدن والمساكن إلى الإنترنت، ما أوجد أشكال ضعف جديدة

المدن الذكية

أدت زيادة إمكانية الوصول إلى مكونات الحواسيب وتصغيرها إلى تسريع تعميم شبكات المدن الذكية وبناها التحتية. ومن الأمثلة على شبكات المدن المترابطة هذه، نذكر شبكة المدن الذكية التابعة لرابطة ASEAN [12] وتقنية المدن الذكية[13] في الهند. وعلى الرغم من أن إنشاء المدن الذكية هدف بارز وضعته اقتصادات كثيرة نصب أعينها، إلا أنه يوسّع أيضاً **رقعة الهجمات المحتملة المتاحة للمجرمين السيبريين الذي يستهدفون الأجهزة الذكية الضعيفة.**

- في عام 2017، بيّنت الهجمات ببرمجيات انتزاع الفدية ومنها مثلاً WannaCry وNotPetya ما يمكن أن يطرحه هذا النوع من الهجمات من تهديد يطال الشبكات المترابطة ويعرّض للخطر عدداً كبيراً من الأجهزة[14].

---

[9] https://par.nsf.gov/servlets/purl/10083310

[10] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[11] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/

[12] https://asean.org/asean/asean-smart-cities-network/

[13] http://smartcities.gov.in/content/innerpage/strategy.php

[14] https://www.wsj.com/articles/how-hackers-could-break-into-the-smart-city-11568776732

المساكن الذكية

ليست المدن الذكية المثال الوحيد على وفرة الأجهزة المتصلة بإنترنت الأشياء، فتزايد وصول العملاء إلى الأجهزة المترلية الذكية يزيد من عدد الأجهزة التي يحتمَل أن تكون معرضة للخطر. ولا يعمد مستخدمون كثر إلى تغيير كلمات السر الافتراضية أو إلى تحديث برمجياتهم بانتظام، وهو ما يجعل منهم أهدافاً تسهل مهاجمتها. وقد أصبحت أدوات مترلية كأقفال الأبواب والثلاجات أجهزة قادرة على الاتصال بالإنترنت وتوفر مجموعة من الخيارات التي يمكن أن يستهدفها المجرمون السيبريون.

- في عام 2019، أشارت شركة Kaspersky إلى أنه في خلال الأشهر الستة الأولى من العام، اكتُشف أكثر من مئة مليون هجوم استهدفت أجهزة ذكية. ويُعد هذا الرقم زيادة حادة مقارنة بعدد الهجمات التي تم اكتشافها قبل ذلك بعام إذ بلغ 12 مليون هجوم[15]. ويضيف التقرير أن المجرمين السيبريين يفضلون الأجهزة المستخدمة في المساكن على تلك المستخدمة في الشركات[16] إذ يسهل عادة استهدافها.
- وفي عام 2020، كشفت مصائد قراصنة الإنترنت التابعة لشركة Kaspersky، وهي عبارة عن شبكات من نسخ افتراضية لعدة أجهزة وتطبيقات متصلة بالإنترنت، وقوع 426 مليون هجوم على أجهزة متصلة بإنترنت الأشياء، وقد وردت هذه الهجمات من 742 ألف عنوان فريد لبروتوكول الإنترنت في خلال الأشهر الستة الأولى من ذاك العام وحده. ويمثّل هذا ارتفاعاً بمقدار أربعة أضعاف في عدد الهجمات، وبمقدار ضعفين ونصف في عدد بروتوكولات الإنترنت بالمقارنة مع الفترة نفسها من العام الماضي.

4.3 الحنكة: للجهات الفاعلة مصدر التهديد مهارات وتكتيكات متطورة

ترتكب الجهات الفاعلة مصدر التهديد الجرائم السيبرية ولها عدة دوافع، منها ما يلي:

- المقرصنون لدوافع سياسية أو اجتماعية الذين يستخدمون الإنترنت كوسيلة للاحتجاج
- المجرمون، ومنهم:
  - المبتدئون الانتهازيون أو الفضوليون الراغبون باختبار مهاراتهم
  - مرتكبو الاعتداء الجنسي على الأطفال عبر الإنترنت
  - الجماعات الإجرامية المنظمة رغبةً منها في كسب الأموال
- جماعات التهديدات المستمرة المتقدمة التي ترعاها دول أمم والتي تتجسس أو تجمع الأموال أو تهاجم بنى تحتية حيوية.

15 https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019

16 https://securelist.com/iot-a-malware-story/94451/

الصورة 1: نطاق التهديدات السيبرية

المصدر: مجهول

شهدت السنوات الأخيرة تطور ما يُعرف بالجريمة السيبرية كخدمة، حيث جعلت 'خصخصة الجريمة الإلكترونية' الخدمات الإجرامية السيبرية في متناول أي شخص مستعد للدفع. وتتم مثل هذه المعاملات عادة على الشبكة الخفية، وهو الجانب المستتر من الإنترنت الذي لا يمكن الدخول إليه إلا من خلال متصفحات خاصة. ويستفيد المجرمون السيبريون من عامل عدم الكشف عن الهوية في الأسواق ومنتديات الحوار على الشبكة الخفية لمراكمة مهاراتهم وأدواتهم.

ومن الأمثلة على الجريمة السيبرية كخدمة نذكر البرمجية الخبيثة Satan التي تنتمي إلى عائلة برمجيات انتزاع الفدية Gen:Trojan.Heur2.FU. وقد أتيحت برمجية Satan الخبيثة لعموم الناس من خلال منصة لبرمجيات انتزاع الفدية كخدمة[17].

ويزداد كذلك شيوع العمليات واسعة النطاق لبرمجيات انتزاع الفدية التي تفضي إلى تعطيل البنية التحتية للأفراد والمؤسسات والبلدان وإلحاق أضرار جسيمة بها:

- في عام 2020، تعرضت شركة Garmin التي تصنّع أجهزة تعقب اللياقة البدنية باستخدام برمجية انتزاع الفدية WastedLocker. وبحسب الأنباء الواردة، اضطرت الشركة إلى دفع 10 ملايين دولار فدية للمجرمين حتى تتمكن من استعادة نظمها ومنع نشر بيانات المستخدمين علناً[18]؛
- في تشرين الأول/ أكتوبر 2020، نشرت الوكالة الأمريكية للأمن السيبري وأمن البنى التحتية تنبيهاً حذرت فيه من تنامي الأنشطة باستخدام برمجيات انتزاع الفدية التي تستهدف قطاع الرعاية الصحية والصحة العامة[19]

5.3 نقص في التبليغ: الإحجام عن التبليغ عن الجرائم السيبرية

[17] https://www.zdnet.com/article/satan-ransomware-as-a-service-starts-trading-in-the-dark-web/
[18] https://www.wired.com/story/garmin-ransomware-hack-warning/
[19] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

في حالات كثيرة، لا يعمد الأفراد والشركات من ضحايا الجرائم السيبرية إلى إبلاغ الأجهزة بالحوادث. **وهذا الامتناع عن التبليغ بالجرائم يعني أن ثمة نقصاً في البيانات حول أساليب عمل المجرمين السيبريين والتقنيات المستخدمة لارتكاب جرائمهم**. وللأسف، هذه ظاهرة منتشرة للغاية[20].

- غالباً ما يجهل الضحايا من الأفراد أين ينبغي أن يبلّغوا عن الجريمة السيبرية وكيف، أو أنهم يعتبرون أنها لا تستحق الإبلاغ عنها، أو أن الخجل يعتريهم لوقوعهم ضحية عملية احتيال[21]. وفي حالات كثيرة لا يؤدي الحادث إلى خسارة في الأرواح أو الممتلكات المادية (المعلومات أو البيانات الشخصية مثلاً)، ولذا لا يكون الضحايا مدركين أو متأكدين ما إذا وقعوا ضحية جريمة، وبالتالي لا يعمدون إلى إبلاغ الأجهزة بها.
- أما الضحايا من الشركات، فغالباً ما تحجم عن التبليغ عن الجرائم السيبرية إذ إن نشر الأخبار على الملأ مضر بسير الأعمال وقد يؤدي إلى تآكل ثقة المستثمرين أو السوق في الشركة[22]. وفي بلدان كثيرة، تغطي أنظمة حماية البيانات هذه المسألة وهي تنص على إلزامية التبليغ عن الحوادث السيبرية.
- في بعض الحالات، قد يجد ضحايا الجرائم السيبرية أن عملية التبليغ عسيرة أو غير واضحة، مما يمنعهم من التبليغ عن الحادث.

6.3 التشريعات والولاية القضائية: الافتقار إلى تجريم الجرائم الإلكترونية والتعقيدات لدى تداخل الولايات القضائية

غالباً ما تنطوي الجريمة السيبرية على تحقيقات عبر الحدود، إذ يمكن أن يتواجد الضحايا والمجرمون والبنى التحتية في بلدان مختلفة. وهو ما يطرح التحديات بالنسبة للمحققين لأنهم غالباً ما يكتشفون أن البلدان الأخرى لم تقم ربما بسنّ القوانين نفسها التي تجرّم المخالفة، أو أن ثمة عناصر مختلفة لازمة لإثبات وقوع الجريمة، أو أن ثمة تفاوتاً في فترات الاحتفاظ ببيانات المشتركين. وقد تفتقر بعض البلدان حتى إلى التشريعات وبالتالي إلى ما يجرّم الجريمة السيبرية، فيصبح البلد إذّاك ملاذاً آمناً للمجرمين السيبريين.

ومن المهم كذلك أن تنص الأطر القانونية للبلدان على إتاحة متسع كاف من الوقت لجمع الأدلة الرقمية وتحليلها والكشف عنها. فالمهل الزمنية القصيرة للغاية قد تؤدي إلى عدم جمع الأدلة الحاسمة أو تحليلها حسب الأصول أو القبول بها في الوقت المناسب، مما يعني عدم محاكمة المجرمين السيبريين.

ويقتضي إجراء التحقيقات الفعالة عبر عدة ولايات قضائية عقد الشراكات مع الأجهزة النظيرة في بلدان أخرى بهدف الدفع قدماً بمجريات التحقيق. وقد يشمل ذلك إجراء التقصيات وضبط الأدلة المادية و/أو الرقمية، أو إصدار التصاريح القضائية، ومنها مثلاً المذكرات المرسلة إلى كيانات في القطاع الخاص كشركات الاتصالات ومقدمي خدمات الإنترنت.

20 https://www.zdnet.com/article/cyber-crime-under-reporting-of-attacks-gives-hackers-a-green-light-say-police/
21 https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html
22 https://www.infosecurity-magazine.com/opinions/organizations-failing-report/

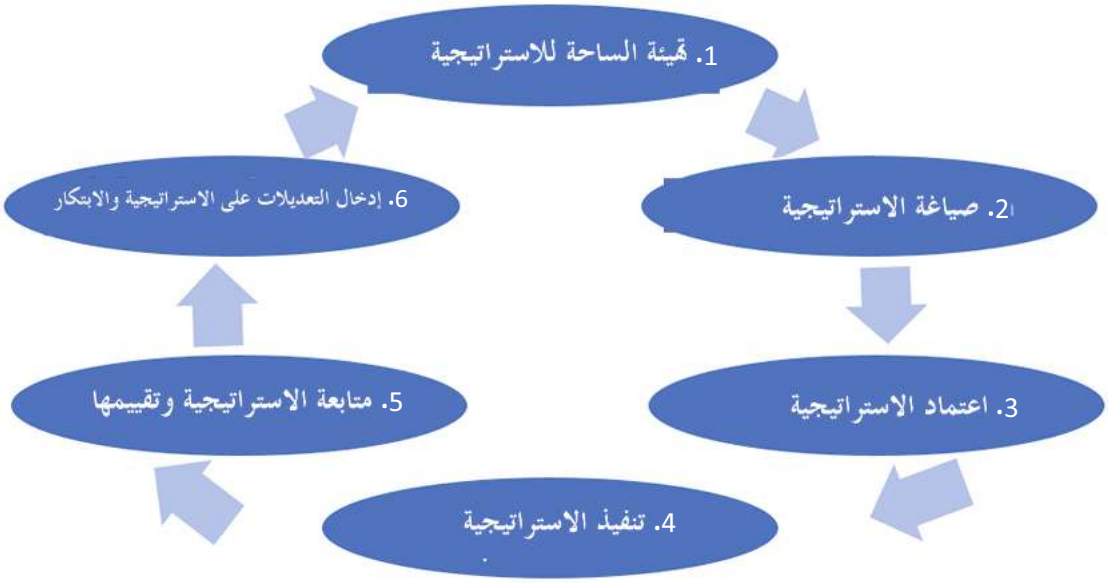
وهذا ليس سوى غيض من فيض صعوبات تعترض إجراء التحقيقات الفعالة عبر عدة ولايات قضائية بهدف ملاحقة مرتكبي الجرائم السيبرية.

4. المنهجية: وضع استراتيجية لمكافحة الجريمة السيبرية

قد تبدو المهمة الأولية بوضع استراتيجية لمكافحة الجريمة السيبرية شاقة للوهلة الأولى، ولذا فإن اتباع عملية تصميم يساعد في صياغة الاستراتيجية.

وثمة نماذج كثيرة تتناول إعداد السياسات، ولكن بشكل عام لا بد من توافر العمليات الآتية:

الصورة 2: مراحل الاستراتيجية



المصدر: شركة TRPC، 2020

1.4 تهيئة الساحة للاستراتيجية

قبل أن تشرع في وضع استراتيجية لمكافحة الجريمة السيبرية، من المهم أن تفهم لماذا تفعل ذلك.

الجريمة السيبرية هي واحدة من أسرع أشكال الجريمة عبر الوطنية التي تواجهها البلدان الأعضاء في الإنتربول تنامياً. وبينما أثمر النمو السريع لتكنولوجيا الاتصالات والمعلومات عن نمو اقتصادي واجتماعي، أسفر ازدياد الاعتماد على الإنترنت عن ارتفاع مستوى المخاطر ومكامن الضعف وعن فتح فرص جديدة لارتكاب الجرائم.

وطبيعة الجريمة السيبرية التي لا تعرف الحدود الجغرافية تضع تحديات في وجه أجهزة إنفاذ القانون تحول دون تحركها بفعالية لمواجهة تلك الجريمة بفعل تعذر إجراء تحقيقات عبر الحدود ووجود مصاعب قانونية وتباين في القدرات بين بلد وآخر.

لا بد إذاً للبلد من استراتيجية واضحة لمواجهة هذه التحديات وحماية مواطنيه بشكل فعال من الجريمة السيبرية.

وثمة أسباب وفوائد عديدة تبرر وضع استراتيجية لمكافحة الجريمة السيبرية، وهو ما سنتطرق إليه في ما يلي:

1.1.4 الجريمة السيبرية مدمرة اقتصادياً

في حزيران/يونيو 2017، استهدف NotPetya، وهو هجوم سيبري عالمي باستخدام برمجية انتزاع الفدية، شركة لتشغيل الخدمات اللوجستية العالمية وعملائها. وقد بلغت تكاليف التي تكبدتها شركة Maersk لتغيير المسارات في اللحظات الأخيرة والتعويض على المتضررين والاستمرار بسير عمل سلسلة الإمداد العالمية 300 مليون دولار[23]. و لم يقتصر الضرر على الشركة، بل كان للحادث تأثير بالغ في عملائها. وعلى سبيل الذكر لا الحصر، خسرت شركة Merck للإمدادات الطبية 870 مليون دولار وشركة TNT Express التابعة لشركة FedEx 400 مليون دولار وشركة Cadbury لإنتاج الشوكولاتة 188 مليون دولار.

وتمظهر بنفس القدر من الوضوح تأثير الدومينو هذا للجريمة السيبرية عندما استهدف هجوم DDoS باستخدام برمجيات 'البوتنت' الخبيثة من نوع Mirai اسم نطاق Dyn في عام 2016، مما شلّ أعمال العديد من العملاء البالغ عددهم 178 ألفاً الذين تستضيف الشركة نطاق الإنترنت الخاص بهم[24]. وتسلط هذه الحوادث الضوء على التعقيد والاستشراء المتناميين لأساليب الجريمة السيبرية الجديدة التي تطورت مقارنة بالأشكال الأقدم من حوادث الجرائم السيبرية، ومنها مثلاً Stuxnet، وهو فيروس حاسوبي أصاب ما لا يقل عن أربع شركات للنفط والغاز، وهي: Baker Hughes وConocoPhillips وMarathon وChevron.[25]

ويقدّر تقرير المخاطر العالمية لعام 2020 الصادر عن المنتدى الاقتصادي العالمي أن تكاليف الأضرار الناجمة عن الجريمة السيبرية قد تصل إلى 6 تريليونات دولار في عام 2021[26].

تحدد إذاً استراتيجية مكافحة الجريمة السيبرية الخطوات اللازمة والواجب اتخاذها لإرساء حوكمة رشيدة لبيانات الشركات وتدابير الوقاية السيبرية الشخصية من أجل الحد من آثارها الاقتصادية.

2.1.4 الجريمة السيبرية تسهّل ارتكاب جرائم أخرى

وفقاً لمكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، غالباً تتولى شبكات إجرامية ناشطة عبر الإنترنت ارتكاب الحوادث الإجرامية السيبرية، وهي تستخدم عائدات الفديات وغيرها من 'المكاسب غير المشروعة' لتمويل أشكال أخرى من الجرائم الخطيرة والإرهاب[27].

تدعم استراتيجية مكافحة الجريمة السيبرية الجهود المبذولة لمكافحة الإرهاب وغسل الأموال وتقوّض آليات تمويل الشبكات الإجرامية المنظمة.

---

23 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

24 https://www.corero.com/blog/financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data/

25 https://isssource.com/stuxnet-hit-4-oil-companies/

26 http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

27 https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html

3.1.4 الجريمة السيبرية تشل عمل الحكومات ويمكن أن توقع خسائر في الأرواح

تُشيع الهجمات السيبرية باستخدام برمجيات انتزاع الفدية الخراب في كافة القطاعات الصناعية. وفي كثير من الحالات، تطال آثارها الخدمات الأساسية كالمستشفيات وأجهزة الرعاية الصحية، وهو ما قد يعني خسارة في الأرواح نتيجة تعطيل النظم الحاسوبية. على سبيل المثال، في عام 2017، استهدف هجوم سيبري ببرنامج انتزاع الفدية WannaCry دائرة الصحة الوطنية في المملكة المتحدة، فعطّل في بعض الحالات النظم الطبية، بينما كان أطباء في خضم عمليات جراحية حرجة، ومنها مثلاً عمليات جراحة القلب[28].

وعلى نفس المنوال، في أيلول/سبتمبر 2020 تعرّض مستشفى في دوسلدورف (ألمانيا) لهجوم ببرمجية انتزاع الفدية. وبسبب إغلاق النظم في المستشفى، كان لا بد من نقل مريضة معرضة حياتها للخطر إلى مستشفى آخر، حيث توفيت بسبب التأخير في تأمين العلاج[29].

لا بد من أن تعمل استراتيجية مكافحة الجريمة السيبرية باتساق مع استراتيجية الأمن السيبري حرصاً على عدم تعطيل الخدمات التي لا يُستغنى عنها.

4.1.4 فوائد وضع الاستراتيجية

للاستراتيجية جملة من الفوائد، ومنها ما يلي:

- إبقاء الأطراف القادرة على الإسهام إيجاباً على اطلاع وجني الفوائد
- تكوين فهم أكثر تعمقاً لمكامن الضعف في بلد ما
- تبيان التقدم المحرَز في مواجهة ما تطرحه الجريمة السيبرية من تحديات
- توفير إطار ثابت للوقاية والكشف والاستجابة
- التوعية

5.1.4 متطلبات الاستراتيجية

1.5.1.4 إنشاء هيئة معنية بالمشروع

يتطلب وضع استراتيجية وطنية لمكافحة الجريمة السيبرية التعاون بين مختلف الجهات المعنية، ومن التحديات الشائعة لدى إعداد استراتيجية لمكافحة الجريمة السيبرية تأمين التزام الأطراف المعنية والحفاظ عليه.

من هنا أهمية تحديد 'هيئة معنية بالمشروع' تتألف من مسؤول رفيع المستوى وفريق معني بالمشروع يتوليان مسؤولية وضع استراتيجية مكافحة الجريمة السيبرية وتنفيذها ومراجعتها.

تقع مسؤولية الوثيقة على المسؤول رفيع المستوى الذي عليه أن يحرص على أن:

---

28 https://www.dailymail.co.uk/news/article-4503420/It-s-life-death-NHS-patients-say-cyber-attack.html

29 https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

- يحظى الفريق المعني بالمشروع بالتعاون اللازم من جانب أبرز الجهات المعنية؛
- تتوفر الموارد الكافية لتنفيذ الاستراتيجية.

على سبيل المثال، يمكن أن يؤدي وزير الداخلية دور المسؤول رفيع المستوى ويمكن أن يتألف الفريق المعني بالمشروع من أعضاء في الوحدة الوطنية لمكافحة الجريمة السيبرية. أما الخيار البديل، فيقضي بأن يكون الفريق المعني بالمشروع عبارة عن فرقة عمل مشتركة.

تكون الهيئة المعنية بالمشروع أيضاً عضواً في اللجنة التوجيهية (راجع القسم 1.2.4).

← وجود القائد والفريق المناسبين شرط أساسي لكي يتكلل وضع استراتيجية مكافحة الجريمة السيبرية بالنجاح.

2.5.1.4 تأمين التعاون بين الهيئات الحكومية

لا بد من التعاون بين مختلف الأجهزة حتى تكون عملية وضع الاستراتيجية فعالة، ويمكن أن يطرح ذلك مجموعة من الصعوبات وهو يستلزم قيادة رشيدة وتعاوناً فعالاً وفي غالب الأحيان حلولاً وسطى. والتعاون الفعال بين مختلف الأجهزة شرط لا غنى عنه في كافة مراحل المشروع، بدءاً من صياغة استراتيجية مكافحة الجريمة السيبرية ووصولاً إلى تنفيذها.

وعلى الهيئة المعنية بالمشروع أن تستشير الأجهزة المعنية الشريكة للحصول على آراءها والتماساً لدعمها.

وبعد الحصول على الموافقة على مفهوم المشروع، نوصي بأن تضع الهيئة المعنية بالمشروع آلية تضمن التعاون بين الهيئات الحكومية. ويمكن أن تشتمل آلية التعاون هذه على اجتماعات دورية تشترك فيها جميع الجهات المعنية ومنها مثلاً أعضاء اللجنة التوجيهية (راجع القسم 1.2.4).

← تأكد من حصولك على تأييد الأجهزة الشريكة قبل إطلاق العمل بالمشروع.

3.5.1.4 تأمين ميزانية وموارد كافية

من الشائع أن تُفرض على الهيئات الحكومية قيود مالية ومن حيث الموارد، وهو ما يمكن أن يؤثّر في إمكانية إنجاز المشروع وتنفيذ استراتيجية وطنية لمكافحة الجريمة السيبرية.

ولكي يتكلل المشروع بالنجاح، لا غنى عن التخطيط لكيفية استخدام وتخصيص الموارد الملائمة، وهو ما يشمل الأموال (أي الميزانية المخصصة) والأفراد (طاقم العمل المفروز للمشروع).

ومن الضروري بالمثل تخصيص الموارد البشرية والمالية على نحو كافٍ لتنفيذ استراتيجية مكافحة الجريمة السيبرية (راجع القسم 4.4.)

← تأكد من أن لديك ما يكفي من الموارد قبل إطلاق العمل بالمشروع.

4.5.1.4 وضع أهداف SMART

الصورة 3: أهداف SMART

على المراحل في استراتيجية مكافحة الجريمة السيبرية أن تتبع مبادئ أهداف SMART [30]: أي يجب أن تكون محددة (S)، وقابلة للقياس (M)، ويمكن تحقيقها (A)، ومرتبطة بالنشاط (R) ومحددة زمنياً (T). وينبغي أن يبدأ البرنامج بوضع أهداف محددة يتعين تحقيقها في إطار زمني محدد ولها مؤشرات مرحلية قابلة للقياس ومهل زمنية لإنجازها.

ومن الأمثلة على ذلك تحديد الجهات المعنية في مختلف مراحل استراتيجية مكافحة الجريمة السيبرية في غضون ستة أسابيع.

- ضع في اعتبارك اعتماد هذا النهج لتوضيح أفكارك وتركيز جهود واستغلال وقتك ومواردك بشكل منتج، بما يزيد في نهاية المطاف من فرص تكلل مشروعك واستراتيجية مكافحة الجريمة السيبرية بالنجاح.

2.4 صياغة الاستراتيجية

في هذه المرحلة يتم تصميم استراتيجية مكافحة الجريمة السيبرية وصياغتها للأسباب والفوائد المنصوص عليها في القسم 1.4.

1.2.4 تشكيل اللجنة التوجيهية وتحديد أبرز الجهات المعنية

أظهرت الدراسات أن نجاح السياسات العامة غالباً ما يتوقف إلى حد كبير على مشاركة الجهات المعنية وتدبّرها شؤونها[31]. والاستراتيجيات التي لا تحصل على التزام أو دعم من الجهات المعنية أو لا تتولى فيها الأخيرة أي مسؤولية غالباً ما تفتقر إلى الموارد والاهتمام اللازمين ولا تخصَص لها الأولوية.

ومن المفيد كخطوة أولى إنشاء لجنة توجيهية تضم الهيئة المعنية بالمشروع وسائر المسؤولين رفيعي المستوى وذوي الصلة الذين يجب اختيارهم بناء على قدرتهم على توفير الرقابة والإرشادات الاستراتيجية في مختلف مراحل وضع استراتيجية مكافحة الجريمة السيبرية.

وعلى اللجنة التوجيهية أن تحدد كافة الجهات المعنية التي يتعين إشراكها في صياغة استراتيجية مكافحة الجريمة السيبرية. وعادة ما تأتي هذه الجهات المعنية الاستشارية ("المستشارون") من الهيئات الحكومية والكيانات غير الحكومية.

[30] https://www.achieveit.com/resources/blog/the-history-and-evolution-of-smart-goals

[31] http://www.oecd.org/gov/regulatory-policy/BPPs-for-Public-Consultation.docx

الهيئات الحكومية:

- الوحدة الوطنية لمكافحة الجريمة السيبرية بهدف تبادل الخبرات والمعارف في مجال التحقيق في الجرائم السيبرية؛
- الجهاز الرائد في مجال الأمن السيبري بهدف تبادل الخبرات في مجال مواجهة الحوادث الإجرامية السيبرية وصياغة سياسات *الأمن* السيبري ومنها مثلاً الاستراتيجيات؛
- أجهزة إنفاذ القانون الأخرى بهدف المساعدة على فهم العمليات والقضايا الإقليمية لدى التحقيق في الجرائم السيبرية، ومنها مثلاً عملية جمع الأدلة الرقمية؛
- كبار المسؤولين ذوو الصلة من الوزارات المعنية، لا سيما أولئك القادرين على إضفاء الحجية وتوفير الدعم لدى صياغة أو اعتماد استراتيجية مكافحة الجريمة السيبرية. ويمكن أن يكون المسؤولون من وزارة الخارجية أو وزارة العدل والشؤون القانونية، ومنهم مثلاً:
- المسؤولون المعنيون من الادعاء العام والقضاء لتقديم المشورة بشأن تطبيق القوانين المتصلة بالإنترنت في البلد؛
- آخرون من المسؤولين الحكوميين المعنيين والأفرقة الحكومية المعنية، أي مثلاً المسؤولون العاملون في المكاتب المعنية بالتحقيق في قضايا الاحتيال، أو المسؤولون من وزارات تكنولوجيا المعلومات والاتصالات والسلامة والأمن العام، إلخ.؛

الكيانات غير الحكومية:

- الأكاديميون/المجموعات الفكرية القادرون على توفير المعارف بالقضايا الراهنة وعلى تسخير مهاراتهم في البحث والصياغة؛
- الهيئات التكنولوجية/الصناعية التي تتمتع بموقع مثالي يسمح لها بتحديد أخطر التهديدات التي تعترض المؤسسات التجارية؛
- منظمات المجتمع المدني بهدف المساعدة على رفع مستوى الوعي العام؛
- الهيئات الإقليمية والدولية بهدف تبادل وجهات النظر حول التهديدات الإقليمية في مجال الجريمة السيبرية.

واختيار المستشارين المناسبين يلبي كامل احتياجات الجهات المعنية ويؤمّن أساساً أفضل لصياغة استراتيجية مكافحة الجريمة السيبرية. وقد تتسبب أي جهات لم تتم استشارتها في المراحل الأولى ثم تم إشراكها في وقت لاحق بعرقلة جمع الجهود السابقة بل وتقويضها حتى.

وبعد تحديد المستشارين، يجري اختيار مجموعة أصغر من الأفراد الأنسب للشروع في نشاط الصياغة ("المحررون") حتى ينكبوا لاحقاً على صياغة الاستراتيجية (راجع القسم 3.2.4 الصياغة).

2.2.4 الاستعراض والتقييم والتحليل

من بالغ الأهمية بمكان لأي بلد أن يستعرض العمليات والموارد والمهارات المتاحة لمكافحة الجريمة السيبرية. ويوفر هذا التمرين أيضاً نظرة متعمقة وقيّمة للمجالات التي تتخللها أوجه قصور. ونتيجة لذلك، يرى البلد بصورة

أوضح البيئة الراهنة للجرائم السيبرية، ويمكنه إذّاك أن يشرع في العمل على بناء مستقبله المنشود من حيث تعزيز قدراته العامة لمكافحة الجريمة السيبرية.

وينبغي أن يأخذ التدقيق في عملية الاستعراض في الحسبان الفئات التالية:

1.2.2.4 الموارد البشرية والمعدات

يقيّم التدقيق الموارد البشرية المتاحة أو العاملة في وظائف مرتبطة بالجريمة السيبرية، أي مثلاً الموظفون المعنيون بالأدلة الجنائية الرقمية أو بمكافحة الجريمة السيبرية، والموظفون المسؤولون عن استتباب الأمن السيبري، ومنهم مثلاً أفرقة CERT.

وفي ما يلي أمثلة عن الأجهزة التي يمكن إدراجها:

- جهاز الشرطة الوطنية – الإدارات والوحدات
- الجهاز أو الإدارة الوطنية المعنية بالأمن السيبري (إن وجدت)
  - فريق CSIRT و/أو فريق CERT الوطني
- وزارة العدل أو الشؤون القانونية على مستوى البلد والمنطقة والولاية/المحافظة
  - قضاة مفروزون لقضايا الجرائم السيبرية
  - مدّعون عامون مفروزون لقضايا الجرائم السيبرية
  - فرع التحقيقات
- الهيئة المركزية المعنية بإدارة معاهدات المساعدة القانونية المتبادلة MLATs
- الجهاز الأمني أو الاستخباراتي الوطني
- الأجهزة الوطنية الأخرى المسؤولة عن الجرائم التي يسهّل الإنترنت ارتكابها (مثل الاحتيال والاستغلال وما إلى ذلك)
- أجهزة شرطة أخرى على مستوى الولاية أو المحافظة لديها وحدات نشطة تحقق في الجرائم السيبرية.

وعلى كل واحد من هذه الأجهزة أن يقدّم تقريراً يتناول فيه:

- موجز عن الهيكل التنظيمي للجهاز والواحدة ذات الصلة والتفويض المناط بهما
- شرح لأنواع الجرائم السيبرية التي يغطيها الجهاز
- الإطار القانوني لعمل الجهاز
- المبادرات الراهنة التي وضعها أي من الأجهزة لمكافحة الجرائم السيبرية.

ضع في اعتبارك أيضاً القدرات التكنولوجية المتوفرة لدى مختلف الأجهزة – هل لديها المعدات المناسبة والتدريب اللازم لأداء مهامها؟

2.2.2.4 العملية: تقييم البيئة التشريعية والتنظيمية

نستعرض هنا الآليات التشريعية والتنظيمية الحالية التي تتعامل مع الجريمة السيبرية في البلد، وهي تشمل كافة التشريعات ذات الصلة، واتفاقات التعاون الدولية، وإجراءات ومعايير التشغيل الداخلية، والعادات والممارسات المحلية.

ويمكن أن تندرج المسائل المتعلقة بالعمليات في الفئات التالية:

- **التشريعات الموضوعية**، ومنها مثلاً القوانين التي تتناول حماية البيانات الشخصية، والقوانين التي تجرّم جرائم كالقرصنة وسرقة البيانات، والقوانين التي تجرّم بيع الأدوات أو الخدمات لأغراض القرصنة، والقوانين التي تستهدف التحرش عبر الإنترنت، والقوانين التي تبيّن المتطلبات اللازمة لحماية البنى التحتية الحيوية.
- **التشريعات الإجرائية**، ومنها مثلاً القوانين التي تتناول جمع الأدلة الإلكترونية واستخدامها، وأنظمة المتعلقة بالبحث في الأدلة الإلكترونية وضبطها، والأنظمة المتعلقة بالمراقبة الإلكترونية.
- **اتفاقات التعاون الدولية**، ومنها مثلاً معاهدات MLATs والانضمام إلى اتفاقية بودابست[32] والاستخدام الفعال للعضوية في الإنتربول بهدف الاطلاع على نظم التعاون الدولي.

ويمكن للمستشارين أن يراجعوا التشريعات الحالية ويحددوا الثغرات في الإطار القانوني الساري حالياً في البلد. وفي بعض الحالات، قد تبرز أيضاً الحاجة إلى دمج عدد من القوانين المختلفة. ويمكن أن تشتمل هذه المرحلة أيضاً على تحديث القوانين ليُصار إلى تجريم الجرائم السيبرية بالشكل المناسب وعلى تحديث الأنظمة التي تشرعن وتنص على البحث عن الأدلة الإلكترونية وضبطها ومقبوليتها في التحقيقات الجنائية. وبالإضافة إلى التشريعات التي تتناول الجريمة السيبرية، قد تدعو الحاجة أيضاً إلى مراجعة صلاحيات التحقيق لدى أجهزة إنفاذ القانون، والمسائل المتصلة بالولايات القضائية، وحماية البيانات، والخصوصية، والقانون التجاري في ما يخص مصادرات عائدات الجريمة السيبرية.

3.2.2.4 التقييم الذاتي والتحليل

بعد الانتهاء من التدقيق في عملية الاستعراض، ينبغي إجراء تقييم لتحديد مكامن الضعف ومجالات التحسين. وثمة العديد من الأدلة المتاحة لإجراء عمليات التقييم وقياس القدرات السيبرية للبلد.

ويتولى الاتحاد الدولي للاتصالات (ITU) إجراء تقييم سيبري شامل لكل بلد بشكل دوري، فهو مسؤول عن مراقبة الالتزامات التي تعبّر عنها البلدان في مجال الأمن السيبري ومقارنتها عبر الركون إلى خمس ركائز هي: الجانب القانوني، والجانب الفني، والجانب المؤسساتي، وبناء القدرات، والتعاون. ويأخذ التقييم كذلك بالاعتبار النتائج التي خرجت بها أدوات التقييم الحالية الأخرى، ومنها مثلاً نموذج نضج القدرات (CMM) ومؤشر الجاهزية الإلكترونية الذي وضعه معهد بوتوماك. ويُشار إلى ما ينتج عن ذلك باسم المؤشر العالمي للأمن السيبري[33].

---

32 https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

33 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ومن أدوات التقييم الذاتي المتعمق نذكر الدليل والأداة التقييمية الصادرين عن البنك الدولي في عام 2017 لمكافحة الجريمة السيبرية. ويتضمن هذا المنهل[34] الأداة التقييمية[35]، وهي عبارة عن ملف Excel آلي يمكّن المستخدم من تحديد الثغرات التي تعتري القدرات الحالية على مكافحة الجريمة السيبرية وإبراز المجالات التي يتعين رفدها بالموارد. ويوفر كتيّب الإرشادات المصاحب (المعروف بالدليل[36]) خلفية سياقية للأداة التقييمية. ويتيح استخدام الأداة التقييمية للمرة الأولى رسم خط أساس يمكن بعد ذلك مراقبته دورياً، ولا بد من استخدام الأداة التقييمية بالترادف مع الدليل.

يُصدر الـــ ITU المؤشر العالمي للأمن السيبري عموماً مرة في السنة لكن بوسع البلدان أن تجري تقييماً ذاتياً باستخدام الأداة التقييمية والدليل الصادرين عن البنك الدولي في الوقت الذي يناسبها.

وتسلط نتائج التقييم الذي يجريه البلد الضوء على مكامن الضعف ومجالات التحسين، وهذه جوانب ينبغي أن ينصب عليها تركيز الاستراتيجية كما يبيّن القسم الآتي.

وحسب الأداة التقييمية المستخدمة والنتائج الصادرة عنها، قد يكون من المفيد التفكير في هيكلة النتائج باستخدام أساليب تحليلية أثبتت بالتجربة نجاعتها، ومنها مثلاً:

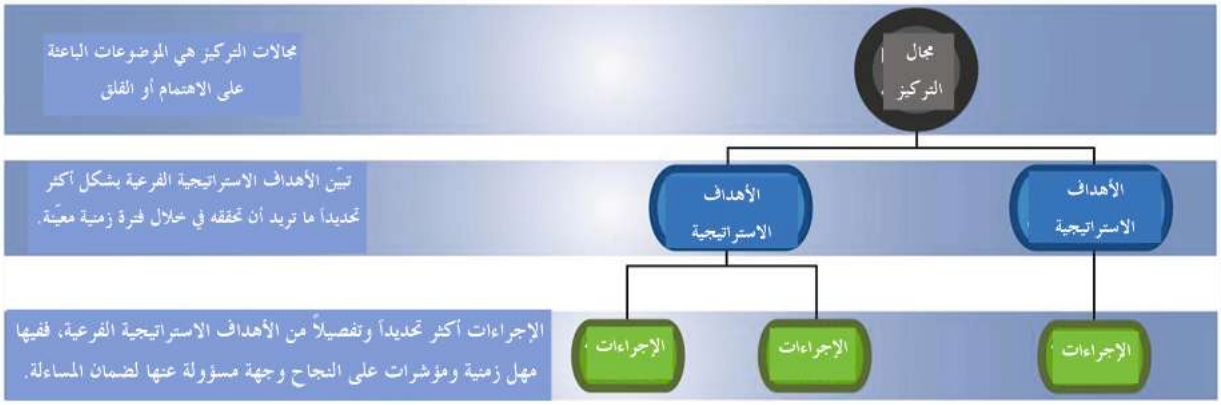
- SWOT – مكامن القوة ومواطن الضعف والفرص والتهديدات
- PESTLE – الأبعاد السياسية والاقتصادية والاجتماعية والتكنولوجية والقانونية والبيئية.

ويسمح الأسلوب المعتمَد لواضعي السياسات بتحديد أي من الثغرات التي كشفها التقييم الذاتي ينبغي تخصيص الأولوية لها عبر اتخاذ إجراءات فورية ومتوسطة وطويلة الأجل.

34 https://www.combattingcybercrime.org/
35 https://www.combattingcybercrime.org/#assessment
36 https://www.combattingcybercrime.org/#toolkit

4.2.2.4 مجالات التركيز والأهداف الاستراتيجية الفرعية والإجراءات

الصورة 4: مجالات التركيز والأهداف الاستراتيجية الفرعية



يحدد البلد مجالات التركيز التي يريد أن يتناولها، ومنها مثلاً الإطار القانوني، من خلال التقييم الذاتي والتحليل (القسم 3.2.2.4)، ثم تُحدد الأهداف الاستراتيجية الفرعية لكل مجال تركيز، أي مثلاً 'اعتماد إطار قانوني أكثر فعالية للتحقيق في الجرائم السيبرية وملاحقة مرتكبيها'. وتفضي هذه الأهداف إلى اعتماد إجراءات يتولى تنفيذها "مسؤولو الإجراءات"، ومنها مثلاً تحديث القوانين الحالية المتعلقة بالجريمة السيبرية وصياغة قوانين جديدة.

مجالات التركيز هي تلك المجالات التي يسعى البلد إلى تحسينها، وهي حجر أساس الاستراتيجية ويحددها البلد بناء على نتائج التقييم الذاتي والتحليل. وهذه هي الخطوة الأولى في إنشاء البنية التي تخوّل البلد أن يكون في وضع أقوى يسمح له بمكافحة الجريمة السيبرية.

مجالات التركيز هي إذاً الخطوط العريضة للاستراتيجية وتمتد على فترة زمنية أطول من الأهداف الاستراتيجية الفرعية والإجراءات.

أما الأهداف الاستراتيجية الفرعية، فهي عبارة عن بيانات محددة بوضوح بالنتائج التي يطمح البلد إلى تحقيقها في خلال إطار زمني محدد.

وتتولى الهيئة المعنية بالمشروع والجهات المعنية ذات الصلة تحديد الإجراءات اللازمة (القسم 1.2.4، "المستشارون") بناء على مدى مناسبتها في المساعدة على بلوغ الأهداف الاستراتيجية الفرعية. وعلى الإجراءات أن تكون على نسق نموذج SMART (القسم 5.1.4) ويجب أن تحاول الإجابة على هذه الأسئلة:

- كيف يمكن بلوغ الهدف الاستراتيجي الفرعي؟
- هل ثمة حالياً أي برامج أو آليات للتعامل مع الهدف الاستراتيجي الفرعي؟
- كيف يمكن تحسين البرامج أو الآليات المعتمَدة حالياً؟
- ما هي البرامج أو الآليات الجديدة التي ينبغي إعدادها أو وضعها؟
- كيف سيجري تنفيذها؟

- ما هي المهلة الزمنية؟
- كيف سيتم قياس نجاحها (المؤشرات على النجاح)؟

وبعد تبيان مجالات التركيز والأهداف الاستراتيجية الفرعية والإجراءات تبياناً واضحاً، يمكن إيجازها في جدول مرجعي بسيط على الشكل الآتي:

الجدول 3: مثال على جدول مرجعي لمجالات التركيز والأهداف الاستراتيجية الفرعية والإجراءات

مجالات التركيز	الأهداف الاستراتيجية الفرعية	الإجراءات
الإطار القانوني	وضع إطار قانوني أكثر فعالية للتحقيق في الجرائم السيبرية وملاحقة مرتكبيها	• صياغة القوانين ذات الصلة بالجريمة السيبرية وتطبيقها في غضون 18 شهراً (الجهة المنفّذة: وزارة الشؤون القانونية) • الانضمام إلى اتفاقية بودابست بشأن الجريمة السيبرية في غضون سنتين (الجهة المنفّذة: فرقة العمل المشتركة بين وزارة الشؤون القانونية ووزارة الخارجية)
بناء القدرات	الحرص على بناء قدرات الموظفين في القطاع العام، لا سيما في أجهزة إنفاذ القانون والادعاء العام والقضاء	• إعداد منهج ودورة تدريبية عن الجريمة السيبرية لأجهزة إنفاذ القانون، على أن يبدأ العمل بهما في غضون 12 شهراً (الجهة المنفّذة: وزارة الداخلية/وزارة الأمن العام أو ما يوازيها) • وضع واعتماد دورات تدريبية تتناول أساسيات الأدلة الرقمية وتكون موجهة للقضاة والمدعين العامين، على أن يبدأ العمل بها في غضون 12 شهراً (الجهة المنفّذة: مكتب النائب العام، وزارة الشؤون القانونية/وزارة العدل).
الشراكات	تعزيز الترتيبات والتفاهمات الوطنية والدولية القاضية بتبادل المعلومات	• اعتماد نظام للتنبيه بالتهديدات السيبرية في غضون تسعة أشهر يشترك فيه القطاعان العام والخاص، مع تخصيص الأولوية للقطاعات الصناعية (الجهة المنفّذة: فرقة العمل المشتركة بين إدارة الجرائم السيبرية ووزارة الصناعة والتجارة، بالعمل مع باقي الوزارات المعنية)

3.2.4 الصياغة

صياغة استراتيجية مكافحة الجريمة السيبرية هي المرحلة التي يُرجَح أن تستغرق معظم الوقت. وللمساعدة في الجهود المبذولة لصياغتها، يرفق هذا الدليل نموذجاً يساعد البلدان. (الفصل 5).

1.3.2.4 التشاور مع الجهات المعنية

ينبغي إطلاق عملية متكررة تُطرح فيها مجالات التركيز للنقاش مع الجهات المعنية ("المستشارين")، وهو ما يتيح للجهات المساهمة في الاستراتيجية فرصة إبداء آراءها في كيفية إحراز تقدم في مجالات التركيز، وبالتالي وضع الأهداف الاستراتيجية الفرعية (راجع الفقرة 4.5).

2.3.2.4 استراتيجية مكافحة الجريمة السيبرية: المسودة الأولى

في هذه المرحلة، يعكف فريق المحررين الذين سبق أن تم اختيارهم (القسم 1.2.4) على صياغة المسودة الأولى من استراتيجية مكافحة الجريمة السيبرية مع مراعاة الأسباب والفوائد المبيّنة في القسم 1.4 ونتائج تمرين الاستعراض المفصَّل في القسم 2.2.4.

ومن الممارسات المعتادة أن تخضع مسودة الاستراتيجية لعدد من المراحل، من الكتابة والتشاور وإبداء الملاحظات إلى المراجعة وإدخال التعديلات. وكلما حصل ذلك بتعمق واستفاضة، زاد احتمال أن تنال الاستراتيجية بصيغتها النهائية إجماع مختلف الجهات المعنية.

ويمكن للمحررين الرجوع إلى نموذج استراتيجية مكافحة الجريمة السيبرية (الفصل 5) للاطلاع على بنية مقترحة للوثيقة.

3.4 اعتماد الاستراتيجية

بعد الانتهاء من عملية صياغة الاستراتيجية، تصبح المسودة النهائية لاستراتيجية مكافحة الجريمة السيبرية جاهزة لعرضها رسمياً ليُصار إلى اعتمادها وتنفيذها.

وتختلف هذه العملية من بلد إلى آخر، ففي بعض البلدان يكون من الضروري التباحث في الاستراتيجية في الجمعية الوطنية أو البرلمان أو أي منتدى آخر للسياسات العامة قبل أن يُصار إلى عرضها للموافقة عليها، أي مثلاً إقرارها في البرلمان/الجمعية الوطنية، أو رفعها إلى رئيس الحكومة/الدولة للموافقة عليها.

4.4 تنفيذ الاستراتيجية

لكي تتكلل استراتيجية مكافحة الجريمة السيبرية بالنجاح، لا بد من نهج منظم لدى تنفيذها. وتنفيذ الاستراتيجية، ولئن اختلف من بلد إلى آخر، إلا أنه يشتمل عموماً على الخطوات الآتية:

- تحديد تفاصيل كيفية بلوغ الأهداف الاستراتيجية الفرعية (القسم 4.2.2.4)
- إعداد خطط تنفيذ منفصلة لكل واحد من الإجراءات
- تخصيص الموارد البشرية والمالية المناسبة.

على الهيئة المعنية بالمشروع والمستشارين أن يضعوا إجراءات وخططاً لتنفيذها دعماً للأهداف الاستراتيجية الفرعية، فضلاً عن ضرورة تحديد موظفين معيّنين أو وحدات معيّنة بوصفهم الجهات المسؤولة ("الجهات المسؤولة عن الإجراءات"). وعلى الجهات المسؤولة أن تتألف من ممثلين عن الأجهزة/الوحدات الأكثر صلة بالإجراء المنوط بها، على أن يتحلوا بأفضل القدرات ليتمكنوا من تنفيذ الإجراءات بنجاح.

وهكذا، يصبح هؤلاء الموظفون أو الوحدات مسؤولين وخاضعين للمساءلة عن تنفيذ الخطة المحددة الموكلة إليهم. وحيث أن خطط التنفيذ معدَّة للمستوى العملي، فمن الضروري أن يُصار إلى تحديدها لكي تفهمها بوضوح الأجهزة المنفِّذة (الجهات المسؤولة عن الإجراءات).

وقد تحتاج الهيئة المعنية بالمشروع إلى تنسيق عملية تنفيذ مختلف الخطط.

أما اللجنة التوجيهية، فقد يتوجب عليها أن تساعد في تأمين ما يكفي من الموارد لتنفيذ مختلف الخطط، وهو ما يضمن ألا تذهب سدى كافة الجهود المبذولة حتى تلك النقطة.

ونوصي بأن تتضمن خطط التنفيذ مقاييس محددة ومؤشرات على النجاح لمتابعة التقدم المحرز في كل واحد من الإجراءات.

5.4 متابعة الاستراتيجية وتقييمها

انطلاقاً من أهداف SMART (القسم 4.5.1.4) من استراتيجية مكافحة الجريمة السيبرية، على الهيئة المعنية بالمشروع والمستشارين أن يخططوا أيضاً لمتابعة الاستراتيجية وتقييمها بانتظام للحفاظ على زخم التقدم المحرز. فبدون متابعة جهود التنفيذ باستمرار، قد تتعرض للخطر لا الإجراءات الفردية وحسب، بل والمشروع برمّته.

ومن شأن الاستمرار في العمل مع الجهات المسؤولة عن الإجراءات وإعدادها للتقارير بشأن المقاييس المحددة مسبقاً أن يساعد في ألا يحيد تنفيذ الاستراتيجية عن مساره. وينبغي أن تركز عملية المتابعة على تفاصيل التقدم المحرز في تنفيذ الأنشطة، وتوافر الموارد، والمسائل والمخاطر التي قد تحول دون تنفيذ الخطة. ولا بد من أن تكون الهيئة المعنية بالمشروع على اطلاع على أي تأخير في الوقت المطلوب حتى يُصار إلى وضع خطط للتخفيف من حدة التأخير. وبالمقابل، ينبغي إطلاع الهيئة المعنية بالمشروع على الإنجازات للإقرار بها.

6.4 إدخال التعديلات على الاستراتيجية والابتكار

كما أن عملية الصياغة الأولية لاستراتيجية مكافحة الجريمة السيبرية اتسمت بالتكرار والتفاعل، هكذا أيضاً ينبغي أن تكون عملية مراجعة الصيغة النهائية بصورة دورية بهدف مواكبة التكنولوجيا ومحاور الهجمات الجديدة والاحتياجات دائمة التغير التي يعبّر عنها البلد.

مثال: تطور استراتيجية نيوزيلندا للأمن السيبري والجريمة السيبرية

يوضح مثال نيوزيلندا في كيفية تطور استراتيجيتها لمكافحة الجريمة السيبرية العملية التي شرعت فيها العديد من البلدان من أجل اعتماد إطار عمل توجيهي يبقى ذا صلة في ضوء الاتجاهات الاقتصادية والمجتمعية المتغيرة. ويبيّن هذا المثال أيضاً ضرورة أن تكون استراتيجية البلد لمكافحة الجريمة السيبرية متوافقة ومتناسبة مع سياق أشمل من السياسات الوطنية، على أن تخضع كلها باستمرار لدورات مراجعة.

وبيّنت استراتيجية الأمن السيبري التي وضعتها نيوزيلندا في عام 2011 كيف استجابت الحكومة للخطر السيبري المتنامي عبر تحديد المجالات والمبادرات ذات الأولوية وتخصيص ما يناسب من الموارد.

وفي عام 2015، نُشرت نسخة محدَّثة (ثانية) عن استراتيجية الأمن السيبري وأُرفقت بها خطة عمل لتحل محل الاستراتيجية المعتمَدة في عام 2011. وقد جرى أيضاً إصدار **خطة وطنية للتصدي للجرائم السيبرية**[37] (شبيهة باستراتيجية مكافحة الجريمة السيبرية) حرصاً من البلد على التصدي بالشكل المناسب للجرائم السيبرية عبر تحديد ما يلي من المجالات ذات الأولوية:

- بناء القدرات اللازمة لمكافحة الجريمة السيبرية
- تكييف الأطر السياساتية والتشريعية في البلد لتواكب العصر الرقمي
- تعزيز التصدي الميداني للجريمة السيبرية
- تسخير العلاقات الدولية لنيوزيلندا بهدف مكافحة الجريمة السيبرية.

وفي عام 2019، أصدرت نيوزيلندا ثالث استراتيجياتها للأمن السيبري[38]، وفيها حدّثت المجالات ذات الأولوية في مضمار الأمن السيبري وأبرز مجالات التركيز في مضمار الجريمة السيبرية.

الصورة 5: خطة العمل الوطنية للتصدي للجرائم السيبرية في نيوزيلندا

الصورة 6: تطور استراتيجية نيوزيلندا للأمن السيبري والجريمة السيبرية

37 https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-cybercrime-plan-december-2015.pdf

38 https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

5. اتفاقية بودابست

ولئن كان الهدف من استراتيجية وطنية لمكافحة الجريمة السيبرية هو تمتين عموم قدرات البلد لمكافحة الجريمة السيبرية على المستوى المحلي، إلا أنه من الضروري إيلاء اعتبار خاص لمواءمة الاستراتيجية مع المعايير والممارسات الدولية. وعلى البلد الذي يضع أو يحدّث الاستراتيجية أن يسعى إلى أن يتوافق إطارها القانوني وسائر الأهداف الاستراتيجية الفرعية مع شروط الانضمام إلى أكثر الاتفاقات الدولية شمولاً واتساقاً بشأن الجريمة السيبرية والأدلة الإلكترونية، أي الاتفاقية المتعلقة بالجريمة الإلكترونية الصادرة عن مجلس أوروبا، والمعروفة باتفاقية بودابست.

5.1 معلومات عن الاتفاقية

تُعد هذه الاتفاقية أول معاهدة دولية بشأن الجرائم المرتكبة عبر الإنترنت وغيره من الشبكات الحاسوبية، وتتناول بشكل خاص الجرائم التي تستهدف وتستخدم البيانات والنظم الحاسوبية، ومن هذه الجرائم النفاذ غير المشروع، والاعتراض غير المشروع، والتدخل في البيانات والنظم، وعمليات الاحتيال المتصلة بالحاسوب، ومواد الاستغلال الجنسي للأطفال، وغيرها من الانتهاكات لأمن الشبكة. وتتضمن الاتفاقية كذلك مجموعة من الصلاحيات والإجراءات الخاصة بالتحقيقات الجنائية وكيفية جمع الأدلة الإلكترونية المتصلة بأي جريمة تكون فيها الأدلة موجودة في نظام حاسوبي، ومن هذه الإجراءات مثلاً التعجيل في حفظ الأدلة والبحث في الشبكات الحاسوبية واعتراض حركة البيانات.

وللاتفاقية هدف رئيسي، ألا وهو اتباع سياسة جنائية مشتركة بهدف حماية المجتمع من الجريمة السيبرية، لا سيما من خلال تبنّي تشريع ملائم ودعم التعاون الدولي.[39] وتهدف الاتفاقية بشكل أساسي إلى:

(1) المواءمة بين بنود الجرائم في القانون الجنائي الموضوعي المحلي والأحكام ذات الصلة في مجال الجريمة السيبرية؛

(2) النص على الصلاحيات المحلية اللازمة في قانون الإجراءات الجنائية للتحقيق في هذا النوع من الجرائم وغيرها من الجرائم المرتكبة عن طريق نظام حاسوبي أو أدلة متعلقة به بشكل إلكتروني وملاحقة مرتكبيها؛ و

(3) استحداث نظام سريع وفعال للتعاون الدولي.[40]

فُتح باب التوقيع على الاتفاقية في بودابست (هنغاريا) في تشرين الثاني/نوفمبر 2001. وفي عام 2003، أُلحق بالاتفاقية بروتوكول بشأن التمييز العنصري وكراهية الأجانب عن طريق النظم الحاسوبية. ومن المتوقع إصدار بروتوكول جديد ثان يعمل على تعزيز التعاون والإفصاح عن الأدلة الإلكترونية، بما في ذلك التعاون المباشر مع مقدمي الخدمات والتعاون في حالات الطوارئ.

39 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

40 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

2.5 مزايا الاتفاقية

يجوز لأي بلد الانتفاع من اتفاقية بودابست باعتبارها مبدأ توجيهياً أو قائمة مرجعية أو قانوناً نموذجياً، إلا أن الانضمام إلى هذه المعاهدة ينطوي على مزايا إضافية:

- توفر الاتفاقية إطاراً قانونياً للتعاون الدولي بشأن الجرائم السيبرية والأدلة الإلكترونية. وترد في الباب الثالث من الاتفاقية أحكام عامة ومحددة تنص على التعاون بين مختلف الأطراف "على أوسع نطاق ممكن" لا في ما يتعلق بالجريمة السيبرية وحسب (الجرائم التي تستهدف أو تستخدم النظم الحاسوبية)، بل وأيضاً في ما يتعلق بأي جريمة تشتمل على أدلة إلكترونية.
- والأطراف الموقّعة أعضاء في اللجنة المعنية باتفاقية الجريمة السيبرية (T-CY)، وهي تتبادل المعلومات والخبرات، وتقيّم تنفيذ أحكام الاتفاقية، وتفسّر الاتفاقية من خلال الملاحظات الإرشادية
- ويمكن للجنة أيضاً أن تعدّ بروتوكولات إضافية إلى هذه المعاهدة. وهكذا، تكون الدول التي لم تشارك في عملية التفاوض بشأن المعاهدة الأصلية قادرة على المشاركة في التفاوض بشأن الصكوك المستقبلية وفي مواصلة تطوير اتفاقية بودابست باعتبارها طرفاً جديداً فيها.
- وتعمل الأطراف في الاتفاقية مع بعضها بعضاً في تعاون موثوق وفعال، وتشير الدلائل إلى أن الكيانات في القطاع الخاص أكثر ترجيحاً للتعاون مع سلطات العدالة الجنائية لدى الأطراف في الاتفاقية بالنظر إلى ضرورة أن تتوفر لدى هذه الأطراف الأطر القانونية المحلية للجرائم السيبرية والأدلة الإلكترونية، بما في ذلك الضمانات المنصوص عليها في المادة 15.
- وقد تصبح الدول التي تطلب الانضمام إلى الاتفاقية أو انضمت إليها بالفعل دولاً تُخصَص لها الأولوية من حيث برامج بناء القدرات. والغرض من هذه المساعدة الفنية هو تيسير تنفيذ أحكام الاتفاقية تنفيذاً كاملاً وتعزيز القدرة على التعاون على الصعيد الدولي.

3.5 الانضمام إلى الاتفاقية

بموجب المادة 37 من الاتفاقية، يجوز لأي دولة أن تنضم إلى المعاهدة وتصبح طرفاً فيها عبر "الانضمام" إليها شريطة أن تكون الدولة مستعدة لتنفيذ الأحكام المنصوص عليها في الاتفاقية. والإجراء المتبع هو التالي:

1. بعد إعداد (مشروع) قانون يشير إلى أن الدولة قد نفذت بالفعل أو من المحتمل أن تنفذ أحكام اتفاقية بودابست في قوانينها الوطنية، يرسل وزير الخارجية (أو أي ممثل آخر جرى تفويضه) خطاباً إلى الأمين العام لمجلس أوروبا يعبّر فيه عن اهتمامه أو اهتمام دولته بالانضمام إلى اتفاقية بودابست.
2. ثم يشاور مجلس أوروبا الأطراف الأخرى، وبعد التوصل إلى إجماع بين الأطراف الحالية في الاتفاقية، توجّه دعوة للدولة للانضمام إليها.
3. تستكمل سلطات تلك الدولة إجراءاتها الداخلية المتبعة لدى التصديق على أي معاهدة دولية قبل إيداعها وثيقة الانضمام في مجلس أوروبا[41].

[41] https://rm.coe.int/cyber-buda-benefits-june2020a-en/16809ebe38

6. نموذج استراتيجية مكافحة الجريمة السيبرية

يتضمن هذا الفصل نموذجاً لتوجيه المحررين في المراحل الأولى لإعداد استراتيجية مكافحة الجريمة السيبرية. ويتناول النموذج النقاط التي تطرقنا إليها في الفصول السابقة ويقدّم بعض الإرشادات الإضافية بشأن بنية الاستراتيجية ومحتوياتها.

ويتضمن هذا النموذج العناصر التي نوصي بها والتي يتكرر ورودها في مختلف استراتيجيات مكافحة الجريمة السيبرية، غير أننا نوصي المحررين أيضاً بأن يضعوا في اعتبارهم السياق والإطار التنظيمي على المستوى المحلي.

ولاستراتيجية مكافحة الجريمة السيبرية أربعة مكونات رئيسية هي:

- المقدمة
- البيئة الحالية للجريمة السيبرية – التقييم والتحليل
- الرؤية
- مجالات التركيز والأهداف الاستراتيجية الفرعية والإجراءات

1.6 المقدمة

يُعد القسم الأول مدخلاً إلى استراتيجية البلد لمكافحة الجريمة السيبرية، وعلى المقدمة أن تتيح للقراء تكوين فهم عن طبيعة الجريمة السيبرية في البلد، ويمكن لها أن تتضمن أقساماً فرعية كما هو مبيّن أدناه.

1.1.6 توطئة

يمكن أن تكون التوطئة عبارة عن رسالة من شخص يؤيد الاستراتيجية ويدفع بها قدماً، أي مثلاً الوزير المختص أو مسؤول سياسي آخر رفيع المستوى. وينبغي أن تبيّن هذه التوطئة سبب أهمية الاستراتيجية وتوضح أنها تحظى بالدعم و"التأييد" من جانب كبار المسؤولين، وأن إنجازها أمر متوقع. وينبغي أيضاً التعريف بالهيئة المعنية بالمشروع.

2.1.6 الغرض من الوثيقة

يصف هذا القسم الغرض المقصود من الاستراتيجية وكيف من شأنها أن تساعد البلد.

3.1.6 معلومات عامة عن سبب أهمية الاستراتيجية

يتضمن هذا القسم لمحة موجزة عن كيفية تطور الاستراتيجيات الرامية إلى التصدي للجرائم السيبرية في البلد (راجع القسم 1.4).

ويمكن هنا الاستشهاد ببعض الإحصاءات (إن وجدت)، ومنها مثلاً عدد الحوادث الإجرامية السيبرية، وعدد المستخدمين المحليين للأجهزة المحمولة و/أو الإنترنت، والأثر المالي الذي يطال البلد والأفراد من الضحايا. فمن شأن هذه الأرقام أن تضع الوضع الراهن للجريمة السيبرية في منظوره الصحيح، ويمكن للإحصاءات المتعلقة

بالإقبال على التكنولوجيات الجديدة أن تكوّن رؤية متعمقة وقيّمة عن محاور الهجمات المتصلة بالجريمة السيبرية التي قد تطرأ في المستقبل، أي مثلاً الأجهزة المعرضة للخطر في مجال إنترنت الأشياء.

وعندما تفتقر البلدان إلى بيانات شاملة عن الجريمة السيبرية، يمكنها استخدام الأرقام العالمية مؤشراً.

2.6 البيئة الحالية للجريمة السيبرية

1.2.6 التعريفات المتصلة بالإنترنت

يقدّم هذا القسم تعريفاً واضحاً لما تعتبره الحكومة جرائم يعتمد ارتكابها على الإنترنت وجرائم يسهّل الإنترنت ارتكابها وللأمن السيبري (القسمان 2.2 و3.2). ويمكن أيضًا الإشارة ههنا إلى مختلف أنواع المجرمين السيبريين أو الجهات الفاعلة مصدر التهديد (القسم 4.34)، والاقتباس من الإحصاءات ذات الصلة المتعلقة بالجريمة السيبرية.

2.2.6 الإحصاءات عن الجريمة السيبرية في البلد

يفصّل هذا القسم الإحصاءات رفيعة المستوى الواردة في القسم 3.1.5 مبيّناً المقاييس ذات الصلة، ومنها مثلاً نوع الجريمة والمنطقة والجانب الديمغرافي وما إلى ذلك. فمن شأن ذلك أن يساعد في تسليط الضوء على جرائم سيبرية محددة وعلى أكثرها شيوعاً في البلد.

ومن الأمثلة على الإحصاءات والاتجاهات التي يمكن إيرادها في هذا القسم نذكر ما يلي:

- عدد الهجمات الإجرامية التي يعتمد ارتكابها على الإنترنت بحسب النوع، أي مثلاً عدد الهجمات ببرمجيات انتزاع الفدية خلال فترة معيّنة؛
- عدد الجرائم التي يسهّل الإنترنت ارتكابها وجرى التبليغ عنها خلال فترة معيّنة؛
- الأنواع الرئيسية للجريمة السيبرية (تشويه المواقع الإلكترونية، التصيد الاحتيالي، مواد الاعتداء الجنسي على الأطفال، التحرش عبر الإنترنت، إلخ.)؛
- تنامي الجريمة السيبرية بمختلف أنواعها بالنسبة المئوية وبالأرقام خلال فترة معيّنة، أي مثلاً على أساس سنوي.

ويحدد دليل إحصاءات العدالة الجنائية بشأن الجريمة السيبرية والأدلة الإلكترونية[42] برنامج جمع الإحصاءات والخطوات الرئيسية لجمع البيانات وتحليلها والتعاون بين العديد من الجهات المعنية.

3.2.6 الأجهزة الحالية المعنية بالجريمة السيبرية

يحدد هذا القسم كافة الأجهزة والهيئات على المستوى الوطني وعلى مستوى الولاية/المحافظة التي تُناط بها مسؤولية التحقيق في الجرائم السيبرية وملاحقة مرتكبيها. ويعرض هذا القسم بالتفصيل أدوارها في منظومة العدالة الجنائية وولاياتها (القسم 1.2.2.4).

[42] https://www.interpol.int/content/download/15731/file/Guide%20for%20Criminal%20Justice%20Statistics%20on%20Cybercrime%20and%20Electronic%20Evidence.pdf

ويهدف ذلك إلى تكوين فهم واضح للمسؤوليات المناطة بكل جهاز وولايته القضائية ومجالات التحقيق والمبادرات لديه والنطاق الذي يغطيه في تصديه للجرائم المتصلة بالإنترنت.

4.2.6 القوانين الحالية

يستعرض هذا القسم من استراتيجية مكافحة الجريمة السيبرية التشريعات التي تم بالفعل سنّها في مجال الجريمة السيبرية (القسم 2.2.2.4).

وقد تشمل ما يلي:

- القانون/التشريع الخاصة بالأمن السيبري
- القانون الخاص بالجرائم الحاسوبية
- القوانين الجنائي الموضوعية
- القوانين الإجرائية، أي توفير المعلومات الأساسية للمسجلين، وبيانات المرور، وبيانات المحتوى
- القوانين و/أو الاتفاقات التي تنص على التعاون الدولي، ومنها مثلاً معاهدات MLATs
- قوانين حماية البيانات، ومنها الأنظمة المتعلقة بالاحتفاظ بالبيانات للجهات المسؤولة عن إيداعها/معاملتها
- أي قانون آخر يمنح صلاحية بدرء الجرائم السيبرية أو التحقيق فيها أو ملاحقة مرتكبيها.

5.2.6 موجز التقييم الذاتي والتحليل

يجب أن يتضمن هذا القسم نتائج عملية التقييم الذاتي والتحليل المبيّنة في القسم 3.2.2.4، وهي تحدد القدرات التي يتحلى بها البلد في مكافحة الجريمة السيبرية وتكشف الثغرات التي ينبغي سدها. ويكون هذا التقييم أساساً لتبيان مجالات التركيز والأهداف الاستراتيجية الفرعية والإجراءات في الاستراتيجية (القسم 4.5).

6.3 الرؤية

يضع هذا القسم رؤية حكومية واضحة لإدارة شؤون الجريمة السيبرية، وهي تكون عادة على شكل موجز بالنجاح الاستراتيجي الذي تنشده الحكومة، وفي ما يلي بعض الأمثلة:

- "تتمثل رؤية خطة العمل بإيجاد بيئة آمنة ومأمونة على الإنترنت في سنغافورة. ولسوف نبلغ هذا الهدف عبر ردع الأنشطة الإجرامية السيبرية وكشفها وإحباطها." – خطة العمل الوطنية لمكافحة الجريمة السيبرية في سنغافورة[43]؛
- "يمكن للمواطنين والشركات والحكومة أن تتمتع بكامل المزايا التي يتيحها حيّز سيبري آمن ومأمون وقادر على الصمود، عاملين معاً، داخل البلاد وخارجها، لفهم المخاطر ومعالجتها، وتقليص الفوائد التي يحققها المجرمون والإرهابيون، واستغلال الفرص في الحيّز السيبري لتعزيز الأمن والقدرة على

[43] https://www.mha.gov.sg/docs/default-source/press-releases/ncap-document.pdf

الصمود بالإجمال في المملكة المتحدة." – استراتيجية مكافحة الجريمة السيبرية الصادرة عن وزارة الداخلية في المملكة المتحدة[44]؛

- "تتمثل رؤية استراتيجية مكافحة الجريمة السيبرية التي وضعتها الشرطة الملكية الكندية بالحد من التهديدات والآثار وأشكال الإيذاء الناجمة عن الجريمة السيبرية في كندا من خلال إجراءات لإنفاذ القانون." – استراتيجية مكافحة الجريمة السيبرية الصادرة عن الشرطة الملكية الكندية[45].

والوضع الأمثل يقضي بأن تحدد الرؤية نهجاً واضحاً يشمل جميع الهيئات الحكومية المعنية وكافة أقطاب المجتمع المعنية لمكافحة الجريمة السيبرية، لا سيما وأنها مسؤولية مشتركة حيث تعمل الحكومة مع المواطنين والشركات والمجتمع المدني لردع الجرائم السيبرية وكشفها وإحباطها. وكلما كانت الرؤية أوضح، سهل على القيادات والجهات المعنية البارزة ضمان اتباع نهج شامل ومتسق ومتماسك.

4.6 مجالات التركيز والأهداف الاستراتيجية الفرعية والإجراءات

يشكل هذا القسم من الوثيقة الجزء الأكبر من استراتيجية مكافحة الجريمة السيبرية وفيه نتابع ما صدر عن عملية التقييم الذاتي والتحليل (القسم 3.2.2.4). وبالاستناد إلى النتائج، تُحدَد مجالات التركيز التي تعتبرها الحكومة بالغة الأهمية في مكافحة الجريمة السيبرية بشكل فعال. ثم تُترجَم هذه المجالات إلى أهداف استراتيجية فرعية وإلى إجراءات (القسم 4.2.2.4) توكَل بعدئذ إلى الأجهزة ذات الصلة (الجهات المسؤولة عن الإجراءات) ويتم تتبعها (القسم 5.4).

1.4.6 مجالات التركيز

كما أوضحنا أعلاه، تتمخض مجالات التركيز عن عملية التقييم الذاتي والتحليل (القسم 3.2.2.4)، على أن يتم بعد ذلك تفصيلها وتقديم التعريفات الواضحة والمبرر لاختيارها.

2.4.6 الأهداف الاستراتيجية الفرعية

يمكن ربط عدة أهداف استراتيجية فرعية بمجال تركيز واحد، وهي تفصّل بدقة أكبر الإجراءات الواجب اتخاذها في غضون فترة زمنية معيّنة.

3.4.6 الإجراءات

الإجراءات أكثر تحديداً وتفصيلاً من الأهداف الاستراتيجية الفرعية، وهي تتضمن المهل الزمنية الفردية والمؤشرات على النجاح وجهة مسؤولة عنها حرصاً على مساءلتها. ويمكن أن تسهم عدة إجراءات في تحقيق هدف من الأهداف الاستراتيجية.

44 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

45 https://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pd

4.4.6 أمثلة على أهداف استراتيجية فرعية وإجراءات موافقة لها

يعرض القسم التالي جملة من الأمثلة للبلدان التي تتطلع إلى وضع الأهداف الاستراتيجية الفرعية من ضمن استراتيجية مكافحة الجريمة السيبرية. راجع أيضاً القسم 4.2.2.4 وتحديداً الجدول 3.

1.4.4.6 الهدف الاستراتيجي الفرعي الأول: وضع إطار قانوني أكثر فعالية للتحقيق في الجرائم السيبرية وملاحقة مرتكبيها

لا يجرّم الإطار القانوني في العديد من البلدان الجرائم السيبرية بشكل فعال، وفي مثل هذه الظروف، سيواصل عدد القضايا المتصلة بالجريمة السيبرية ارتفاعه طالما أن التشريعات لم تواكبها.

ويمكن أن يكون الهدف الاستراتيجي الفرعي هو تحديث الإطار القانوني والاستفادة من الأطر أو الصكوك الدولية لمواجهة التحديات الراهنة في التحقيقات في الجرائم السيبرية ومقاضاة مرتكبيها وإنفاذ القوانين ذات الصلة.

إجراءات لها جداول زمنية وأجهزة تنفذها

- صياغة وإنجاز قانون بشأن الجريمة السيبرية خلال *فترة زمنية محددة* (الأجهزة المنفِّذة المحتملة: وزارة الشؤون القانونية أو إدارة الشؤون الداخلية أو مكتب النائب العام)؛
- الحرص على الانضمام إلى اتفاقية بودابست المتعلقة بالجريمة الإلكترونية في غضون سنتين (الأجهزة المنفِّذة المحتملة: فرقة عمل مشتركة بين وزارة الشؤون القانونية ووزارة الخارجية).

2.4.4.6 الهدف الاستراتيجي الفرعي الثاني: بناء قدرات سلطات العدالة الجنائية

تنامت الجرائم السيبرية كماً وتعقيداً، وهو ما أوجد طلباً متزايداً على التدريب المستمر لسلطات العدالة الجنائية (أفراد الشرطة والمدعون العامون والقضاة مثلاً) التي تتعامل مع هذه الجرائم. وفي الوقت نفسه، تؤدي الأدلة الجنائية دوراً متزايد الأهمية في العديد من أنواع القضايا الجنائية. وغالباً ما يكون الحفاظ على سلامة الأدلة الرقمية منذ جمعها إلى حين عرضها في المحكمة ركيزة أساسية في الملاحقات القضائية الناجحة.

ونظراً لأن الأجهزة الرقمية والأدلة الإلكترونية عناصر في جميع أنواع الجرائم تقريباً، فمن الضروري أن يكوّن موظفو أجهزة إنفاذ القانون "غير المتخصصين" فهماً أساسياً للأدلة الرقمية والطريقة المناسبة في ضبطها.

ويعتمد المدعون العامون والقضاة على الجمع القانوني للأدلة الدقيقة والموثوقة لعرضها والقبول بها في المحاكم، وغالباً ما تتوقف الإدانات على مدى فهم المدعين العامين والقضاة للأدلة الرقمية.

وبالتالي، يمكن أن يكون الهدف الاستراتيجي الفرعي هو بناء القدرات المهمة لدى سلطات العدالة الجنائية الوطنية المسؤولة عن درء الجرائم السيبرية والتحقيق فيها وملاحقة مرتكبيها ومقاضاتهم.

ومن شأن تعزيز قدرات موظفي أجهزة إنفاذ القانون في مجال التحقيقات أن يزيد من فاعليتهم في مكافحة الجرائم السيبرية وأن يبسّط التعاون مع الهيئات الحكومية الأخرى ومع القطاعات الصناعية في القطاع الخاص.

أما بناء قدرات المدعين العامين والقضاة، فيساعدهم على تفسير وعرض/قبول الأدلة الإلكترونية في المحاكم بشكل صحيح.

إجراءات لها جداول زمنية وأجهزة تنفذها

- وضع منهج تدريبي حول الجريمة السيبرية ومراجعته باستمرار في غضون ستة أشهر لتستفيد منه أجهزة إنفاذ القانون (الجهاز المنفِّذ المقترَح: وزارة الداخلية/وزارة الأمن العام أو ما يوازيها)؛
- إجراء ما لا يقل عن خمس دورات تدريبية حول التحقيقات في الجرائم السيبرية سنوياً يستفيد منها موظفو إنفاذ القانون، على أن تبدأ بعد تنفيذ المنهج التدريبي (الجهاز المنفِّذ المقترَح: وزارة الداخلية/وزارة الأمن العام أو ما يوازيها)؛
- إعداد وإجراء دورة تدريبية واحدة على الأقل حول أساسيات التعامل مع الأدلة الرقمية يستفيد منها كافة القضاة والمدعين العامين الذين يتعاملون مع قضايا الجرائم السيبرية (الجهاز المنفِّذ المقترَح: وزارة الشؤون القانونية، مكتب النائب العام).

3.4.4.6 الهدف الاستراتيجي الفرعي الثالث: تعزيز الشراكات لمكافحة الجريمة السيبرية

ولئن يتحمل الموظفون المعنيون بالجريمة السيبرية والأمن السيبري مسؤولية العمل نحو حيّز سيبري أكثر أماناً، إلا أنهم لا يستطيعون النجاح بمفردهم. فيد العون التي تمدها الأجهزة الوطنية والبلدان والقطاعات الأخرى عنصر لا غنى عنه في تعزيز معارف الموظفين وقدراتهم.

التعاون بين الهيئات الحكومية

تميل بعض الأجهزة إلى العمل بمعزل عن بعضها بعضاً، وهكذا أيضاً هو الحال عندما يتعلق الأمر بتبادل المعلومات بين الأجهزة الوطنية. فغالباً ما تكون المعارف وبيانات الاستخبارات والموارد موزَعة على عدة أجهزة تكاد لا تدري بالمعلومات والمبادرات والتحقيقات والقدرات لدى بعضها بعضاً أو تفتقر إلى التنسيق بشأنها.

ويمكن إذاً أن يكون الهدف الاستراتيجي الفرعي تعزيز تبادل المعلومات والموارد بين مختلف الأجهزة بما يمكن أن يفضي إلى اتباع نهج أكثر فعالية على نحو ملموس في مكافحة الجريمة السيبرية.

التعاون الحكومي الدولي

يتواصل الجناة ويعملون عبر الحدود من دون أي قيود، وهو ما يجعلهم في وضع أفضل مقارنة بالأجهزة المكلفة بسوقهم إلى العدالة.

ويمكن إذاً أن يكون أحد الأهداف الاستراتيجية الفرعية للبلد توسيع استخدامه للشبكات الدولية، ويشمل على سبيل المثال المسؤولين في مجال إنفاذ القانون والادعاء العام. وغالباً ما تتبادل هذه الشبكات المعلومات استناداً إلى مبدأ المعاملة بالمثل عن طريق آليات تتفاوت في ما بينها من حيث درجة طابعها الرسمي، وهو ما يزيد من فعالية عملها.

ولأجهزة إنفاذ القانون مجموعة من آليات التعاون تحت تصرفها، ولها إما طابع رسمي – معاهدات MLAT مثلاً –أو طابع غير رسمي بدرجة أكبر بهدف تسريع نقل المعلومات بين الأجهزة. ومن الشبكات التي تعمل على مدار الساعة طيلة أيام الأسبوع، نذكر منظومة الإنتربول العالمية للاتصالات الشرطية I-24/7، وشبكة الجريمة المتصلة بالتكنولوجيا المتقدمة التابعة لمجموعة الدول السبع، وشبكة جهات الاتصال للأطراف في اتفاقية بودابست، وقد أُنشئت هذه الشبكات لتلقّي الطلبات العاجلة بالحصول على أدلة رقمية وتيسير التعاون الدولي.

وثمة أيضاً آليات مخصصة للمدعين العامين المعنيين بالجرائم السيبرية، ومنها مثلاً الشبكة العالمية للنيابات العامة المعنية بمكافحة الجرائم الحاسوبية التابعة للرابطة الدولية للمدعين العامين.

الشراكات مع القطاعين العام والخاص

يتطلب درء الحوادث السيبرية المعقدة والتحقيق فيها مهارات وموارد فنية كثيرة، وقد تكون هذه أيسر توافراً في مؤسسات القطاع الخاص من أجهزة إنفاذ القانون.

ومن شأن تمتين التعاون على مختلف المستويات بين القطاعين العام والخاص أن يقطع شوطاً طويلاً في تعزيز تصدي البلد للجريمة السيبرية، في حين أن الرفع من مستوى وعي عموم الناس يقلل من عدد الضحايا المحتملين.

ويمكن أن يكون أحد الأهداف الاستراتيجية الفرعية عقد شراكات بين القطاعين العام والخاص عبر مختلف القطاعات سعياً إلى منع وقوع الجرائم السيبرية والتحقيق الجنائي فيها. ويمكن لهذه الشراكات مع كيانات مثل مقدمي خدمات الاتصالات والخدمات المالية وشركات الأمن السيبري أن تركز على جوانب مختلفة، ومنها مثلاً زيادة الوعي والتدريب الفني والمساعدة في التحقيقات وعمليات التحليل من خلال تبادل المعلومات وبيانات الاستخبارات. ومن المواضيع التي يمكن تناولها نذكر المعلومات عن التهديدات السيبرية والاتجاهات ومواطن الضعف وكيفية معالجة حوادث محددة.

ويمكن إضافة هدف استراتيجي فرعي آخر هو رفع مستوى الوعي لدى عموم الناس بالتهديدات السيبرية الشائعة. وتوفر مبادرات ينخرط فيها القطاعان العام والخاص، ومنها مثلاً برنامج Get Safe Online [46] في المملكة المتحدة، نصائح عملية لعموم الناس تبيّن لهم كيف يحمون أنفسهم وحواسيبهم وأجهزتهم المحمولة ومؤسساتهم التجارية من خطر الاحتيال وانتحال الهوية والفيروسات ومشاكل أخرى كثيرة يواجهونها عبر الإنترنت.

الشراكات مع المنظمات متعددة الجنسيات

يمكن للشراكات مع المنظمات المناسبة أن تؤثّر مباشرة في قدرة البلد على مكافحة الجريمة السيبرية لأنها تتيح فرصاً لتبادل المعلومات وبيانات الاستخبارات، وهو ما قد يساعد في التحقيقات وفي مجالات أخرى. ويمكن أن ينتج عن الشراكات أثر غير مباشر من خلال التشبيك وتبادل الموارد عن طريق التبرع بالمعدات أو إعارة الموظفين مؤقتاً إلى منظمات شريكة معيّنة. وبالإضافة إلى ما تقدم، يمكن للشركاء الدوليين والإقليميين أن يوفروا سبلاً لبناء القدرات وتبادل أفضل الممارسات، ومن الأمثلة على ذلك هذا الدليل الذي بين يديك.

[46] https://www.getsafeonline.org

ويمكن أن يكون الهدف الاستراتيجي الفرعي عقد الشراكات ذات الصلة على المستويين الدولي والإقليمي وتوطيدها.

فعلى المستوى الدولي، يمكن أن يكون الإنتربول ومكتب الـــ UNODC والاتحاد الدولي للاتصالات والبنك الدولي ومراكز تبادل المعلومات والتحليل شركاء قيّمين.

أما على المستوى الإقليمي، فالشراكات مع منظمات كـــ رابطة ASEAN، ولجنة رؤساء الشرطة التابعة لرابطة ASEAN، واليوروبول، والاتحاد الأفريقي، ومنظمة الدول الأمريكية، ومنظمة التعاون الاقتصادي، والجماعة الكاريبية والوكالة التنفيذية المعنية بالجريمة والأمن، على سبيل المثال والذكر، يمكن أن تعود بفوائد جمة.

إجراءات لها جداول زمنية وأجهزة تنفذها

- استحداث "مركزاً لتبادل المعلومات" بشأن الجريمة السيبرية يكون عبارة عن هيئة مركزية تحرص على تفادي التضارب في عمل مختلف الجهات الوطنية المعنية المشاركة في التحقيق في الحوادث الإجرامية السيبرية وملاحقة مرتكبيها. وينبغي أن يتضمن هذا المركز قناة واحدة للإبلاغ عن الجرائم بهدف منع الازدواجية في التحقيقات، على أن يجري التنفيذ في غضون 12 شهراً مدفوعاً بالوزارات المعنية؛
- الحث على وتحسين استخدام الشبكات ذات الصلة العاملة على مدارة الساعة طيلة أيام الأسبوع على الفور. والأجهزة المنفِّذة هي تلك المسؤولة عن تشغيل منظومة العدالة الجنائية، أي مثلاً وزارة الداخلية/وزارة الأمن العام وإدارة العدل؛
- تسهيل إبرام الاتفاقات الرسمية التي تجيز تبادل بيانات الاستخبارات بين الأجهزة في القطاع العام والكيانات ذات الصلة في القطاع الخاص في غضون ستة أشهر للمساعدة في تبيان التهديدات السيبرية التي تستهدف القطاعات الصناعية الحيوية، مثل منشآت الطاقة والمياه والرعاية الصحية والاتصالات والتمويل والنقل وما إلى ذلك. ويمكن أن تكون الوحدة الوطنية لمكافحة الجريمة السيبرية على الجهاز المنفِّذ؛
- تعزيز تدابير الوقاية السيبرية الجيدة من خلال حملات التوعية العامة، ومنها مثلاً اليوم[47] السنوي للإنترنت الأكثر أماناً في شباط/فبراير. ويمكن للجهاز الوطني المعني بالأمن السيبري والوحدة الوطنية لمكافحة الجريمة السيبرية أن تتولى التنفيذ في غضون ستة أشهر؛
- الاطلاع على والاستفادة بشكل كامل من المعلومات وبيانات الاستخبارات الواردة من منظمات كالإنتربول أو المتاحة من خلالها، ومنها مثلاً فريق خبراء الإنتربول العالمي المعني بمكافحة الجريمة السيبرية والتقارير عن أنشطة الجريمة السيبرية. وتتولى التنفيذ الفوري لذلك الوحدة الوطنية لمكافحة الجريمة السيبرية أو الوزارة المختصة.

[47] https://www.saferinternetday.org/

5.4.6 التذييلات

1.5.4.6 مسرد المصطلحات

قد يكون من المفيد تضمين استراتيجية مكافحة الجريمة السيبرية مسرداً يعرّف بأبرز المصطلحات والمختصرات باختلاف أنواعها.

2.5.4.6 المراجع

روابط إلى المراجع التي قد توفر المزيد من الإرشادات.

التذييل ألف: الجريمة السيبرية والأمن السيبرية: الاستراتيجيات والأنظمة الوطنية

يورد هذا التذييل قائمة بالموارد والمراجع المتاحة للجميع التي يمكن للبلدان أن ترجع إليها لدى صياغة استراتيجيتها الخاصة لمكافحة الجريمة السيبرية. وقد اختارت بعض البلدان عدم الإعلان عن استراتيجيتها لمكافحة الجريمة السيبرية، وهو خيار يمكن اعتماده إذا ساورك القلق بشأن الكشف العلني عن الاستراتيجية.

وفي حالات كثيرة، تُصمَم استراتيجية مكافحة الجريمة السيبرية لتكون استكمالاً لاستراتيجية الأمن السيبري. وفي حالات أخرى، تندرج استراتيجية مكافحة الجريمة السيبرية أصلاً في إطار استراتيجية الأمن السيبري.

أستراليا

- استراتيجية الأمن السيبري (2020)
https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf

كندا

- الاستراتيجية الوطنية للأمن السيبري (2018)
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf
- استراتيجية مكافحة الجريمة السيبرية الصادرة عن الشرطة الملكية الكندية (2014)
http://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf

أوروبا/الاتحاد الأوروبي

- اتفاقية بودابست والمعايير ذات الصلة (2001)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
- الوكالة الأوروبية لأمن الشبكات والمعلومات – دليل الممارسات الجيدة لوضع استراتيجية وطنية للأمن السيبري: إعداد وتنفيذ استراتيجيات وطنية للأمن السيبري (2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

نيوزيلندا

- الخطة الوطنية للتصدي للجرائم السيبرية (2015)
https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-cybercrime-plan-december-2015.pdf
- استراتيجية الأمن السيبري (2019)
https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

سنغافورة

- استراتيجية سنغافورة للأمن السيبري (2016)
https://www.csa.gov.sg/-/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

المملكة المتحدة

- الاستراتيجية الوطنية للأمن السيبري للفترة 2016–2021
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
- استراتيجية مكافحة الجريمة السيبرية (2010)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

الولايات المتحدة الأمريكية (2018)

- الاستراتيجية السيبرية الوطنية للولايات المتحدة الأمريكية
https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

الاتحاد الدولي للاتصالات

- دليل وضع استراتيجية وطنية للأمن السيبري (2018)
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

الإنتربول

نبذة عن الإنتربول

الإنتربول هو أكبر منظمة دولية للشرطة في العالم. ويتمثل دوره في مد يد العون إلى أجهزة إنفاذ القانون في بلدانه الأعضاء الـ 194 لمكافحة الجريمة عبر الوطنية بجميع أشكالها. والبنية التحتية المتطورة للدعم الفني والميداني التي تملكها المنظمة تساعد على مواجهة التحديات الإجرامية المتنامية التي يشهدها القرن الحادي والعشرون. تشمل خدماتنا التدريب المستهدف، وتوفير الخبرات لدعم التحقيقات، وقواعد البيانات المتخصصة، وتأمين قنوات الاتصال بين أجهزة الشرطة.

رؤيتنا: "الوصل بين أجهزة الشرطة لجعل العالم أكثر أمانا"

تتمثل رؤية الإنتربول في إقامة عالم يكون فيه كل موظف من موظفي إنفاذ القانون قادرا، من خلال المنظمة، على التواصل بشكل مأمون وعلى تبادل المعلومات الشرطية الحيوية والوصول إليها كلما وحيثما دعت الحاجة، من أجل ضمان سلامة المواطنين في العالم. ويقدم باستمرار حلولا جديدة ومتطورة لمواجهة التحديات التي تعترض عمل أجهزة الشرطة والأمن على الصعيد العالمي ويشجع على استخدامها