الاتحاد الدولي للاتصالات

المسألة 22/1
التقرير النهائي

قطاع تنمية الاتصالات | لجنة الدراسات 1 | فترة الدراسة الرابعة (2006-2010)

المسألة 22/1:

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

لجان الدراسات التابعة لقطاع تنمية الاتصالات (ITU-D)
في الاتحاد الدولي للاتصالات

قرر المؤتمر العالمي لتنمية الاتصالات (WTDC-06) بموجب قراره 2 (الدوحة، 2006) الاحتفاظ بلجنتي دراسات وحدد المسائل التي تدرسها كل منهما. كما اعتمد المؤتمر القرار 1 (الدوحة، 2006) الذي حدد فيه إجراءات العمل التي يتعين على اللجنتين اتباعها. وقد أسندت إلى لجنة الدراسات 1، فيما يتعلق بالفترة 2006-2010، دراسة تسع مسائل في مجال الاستراتيجيات والسياسات ذات الصلة بتنمية الاتصالات. أما لجنة الدراسات 2، فقد أسندت إليها دراسة عشر مسائل في مجال تنمية وإدارة خدمات الاتصال وشبكاتها وتطبيقات تكنولوجيا المعلومات والاتصالات.

يرجى الاتصال بالعنوان التالي للحصول على أي معلومات:

Mr Souheil MARINE/Ms Christine SUND
Telecommunication Development Bureau (BDT)
ITU
Place des Nations
CH-1211 GENEVA 20
Switzerland
Telephone: +41 22 730 5323/ 5203
Fax: +41 22 730 5484
E-mail: souheil.marine@itu.int
christine.sund@itu.int

لطلب منشورات الاتحاد الدولي للاتصالات:

يرجى ملاحظة أن الطلبات لا تقبل عن طريق الهاتف، ولذلك ينبغي إرسالها بالفاكس أو بالبريد الإلكتروني.

ITU
Sales Service
Place des Nations
CH-1211 GENEVA 20
Switzerland
Fax: +41 22 730 5194
E-mail: sales@itu.int

المكتبة الإلكترونية للاتحاد: http://www.itu.int/publications

الاتحـــاد الدولـــي للاتصـــالات

المســـألة 22/1

التقرير النهائي

قطاع تنمية الاتصالات لجنة الدراسات 1 فترة الدراسة الرابعة (2006-2010)

المسألة 22/1:

تأمين شبكات المعلومات والاتصالات:
أفضل الممارسات من أجل بناء
ثقافة الأمن السيبراني

إخلاء مسؤولية

شارك في إعداد هذا التقرير عدة خبراء من إدارات وشركات مختلفة. ولا ينطوي ذكر شركات أو منتجات معينة على أي تأييد أو توصية من جانب الاتحاد الدولي الاتصالات.

جدول المحتويات

الصفحة

مقدمة 1

الجـــزء I – وضع استراتيجية وطنية للأمن السيبراني والحصول على موافقة عليها 6

A.I عرض عام للأهداف في إطار هذا الجزء 7

B.I الخطوات المحددة لتحقيق هذه الأهداف 7

الجـــزء II – إقامة التعاون بين الحكومة الوطنية والقطاع الخاص 10

A.II عرض عام للهدف في إطار هذا الجزء 11

B.II الخطوات المحددة لتحقيق هذا الهدف 11

الجـــزء III – ردع الجريمة السيبرانية 14

A.III عرض عام للهدف في إطار هذا الجزء 14

B.III الخطوات المحددة لتحقيق هذا الهدف 14

الجـــزء IV – إنشاء منظمة وطنية لإدارة الحوادث: المراقبة والإنذار والاستجابة والانتعاش 20

A.IV عرض عام للأهداف في إطار هذا الجزء 20

B.IV الخطوات المحددة لتحقيق هذه الأهداف 20

الجـــزء V – الترويج لثقافة وطنية للأمن السيبراني 23

A.V عرض عام للهدف في إطار هذا الجزء 23

B.V الخطوات المحددة لتحقيق هذه الأهداف 23

التذييـــل 1 – قائمة بالمختصرات 26

التذييـــل 2 – استراتيجية تنفيذ التعاون في مجال الأمن السيبراني وتدابير الفعالية 28

الملحق ألف – لجنة الدراسات: رسائل اقتحامية (Spam) 31

الملحق بـــاء – إدارة الهوية 47

الملحق جيم – روابط ومراجع 57

المسألـــة 22/1

مقدمة

هذا التقرير يزود الإدارات الوطنية باستعراض شامل للعناصر الأساسية اللازمة لمعالجة مسألة الأمن السيبراني على الصعيد الوطني، وتنظيم النهج الذي تتبعه إزاء الأمن السيبراني الوطني[1]. وبالنظر إلى تباين القدرات الوطنية الحالية، واستمرار ظهور المخاطر المتعلقة بهذا الموضوع، فإن هذا التقرير لا يقدم وصفة ناجعة لتأمين الفضاء السيبراني. لكن هذا الإطار، بالأحرى، يبين نهجاً مرناً يمكن تطبيقه لمساعدة الإدارات الوطنية على مراجعة وتحسين مؤسساتها وسياساتها وروابطها الحالية التي تعنى بمسألة الأمن السيبراني. وعلى الرغم من أن هذا التقرير يركز على الأمن السيبراني، فإننا نلاحظ أن حماية الشبكة المادية تشكل أولوية على نفس القدر من الأهمية. ونشير أيضاً إلى أنه يجب حماية الأحكام المتعلقة بالخصوصية وحرية التعبير واحترامهما، على النحو الوارد في الأجزاء المعنية من الإعلان العالمي لحقوق الإنسان ومبادئ إعلان جنيف.[2]

والعناصر الرئيسية لهذا التقرير هي كالتالي:

- وضع استراتيجية وطنية للأمن السيبراني؛
- إقامة تعاون على المستوى الوطني بين الحكومة ودوائر الصناعة؛
- ردع الجريمة السيبرانية؛
- استحداث مقدرة إدارية للتحكم في الحوادث وطنياً؛
- النهوض بثقافة وطنية للأمن السيبراني.

وينبغي لكل عنصر من هذه العناصر أن يشكل جزءاً من منهجية وطنية شاملة إزاء الأمن السيبراني. ولا يشير ترتيب ظهورها إلى تفضيل عنصر ما على عنصر آخر. وقد تكون هناك عناصر أخرى حسب الظروف الوطنية.

ولأغراض هذا التقرير، يُعرَّف ***الأمن السيبراني***، على النحو المحدد في التوصية ITU-T X.1205، بأنه مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ونُهُج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية والمنظمة وأصول المستعملين. وتشمل المنظمة وأصول المستعملين تجهيزات الحواسيب الموصولة، والموظفين، والبنية التحتية، والتطبيقات، والخدمات، وأنظمة الاتصالات، والحصيلة الكلية للمعلومات المرسلة و/أو المخزنة في البيئة السيبرانية. ومن شأن خدمات الأمن السيبراني كفالة تحقيق والحفاظ على الخواص الأمنية للمنظمات وأصول المستعملين إزاء المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتتألف الأهداف العامة للأمن مما يلي:

- التوافر
- السلامة، والتي قد تشمل الأصالة وعدم التنصل
- الموثوقية

ومن المهم تفهم العلاقة بين الأمن السيبراني، والبنية التحتية الحيوية، والبنية التحتية الحيوية للمعلومات، وحماية البنية التحتية الحيوية للمعلومات، والبنية التحتية غير الحيوية. ويصور الشكل 1 هذه العلاقة.

ولئن كان هناك تباين طفيف في التعريفات، فإن ***البنية التحتية الحيوية*** (CI) ينظر إليها عموماً باعتبارها الأنظمة والخدمات والوظائف الرئيسية التي يؤدي تعطيلها أو تدميرها إلى آثار موهنة على الصحة العامة والسلامة أو التجارة أو الأمن القومي أو على أي مجموعة من هذه الأمور في آن واحد. وتتألف البنية التحتية الحيوية من عناصر مادية (مثل المرافق والمباني) وعناصر افتراضية، (مثل الأنظمة والبيانات) (انظر الشكل 1). وقد تتباين الطبيعة "الحيوية" من بلد لآخر، لكنها عادة ما تشمل عناصر تكنولوجيا المعلومات والاتصالات، والطاقة، والأعمال المصرفية، والنقل، والصحة العامة، والزراعة، والأغذية، والمياه، والمواد الكيميائية، والملاحة البحرية،

---

[1] يرجى من القراء المهتمين الرجوع إلى نواتج المنظمة الدولية للتوحيد القياسي من 27001 إلى 27003.

[2] انظر القمة العالمية لمجتمع المعلومات (WSIS): برنامج عمل تونس بشأن مجتمع المعلومات، الفقرة 42.

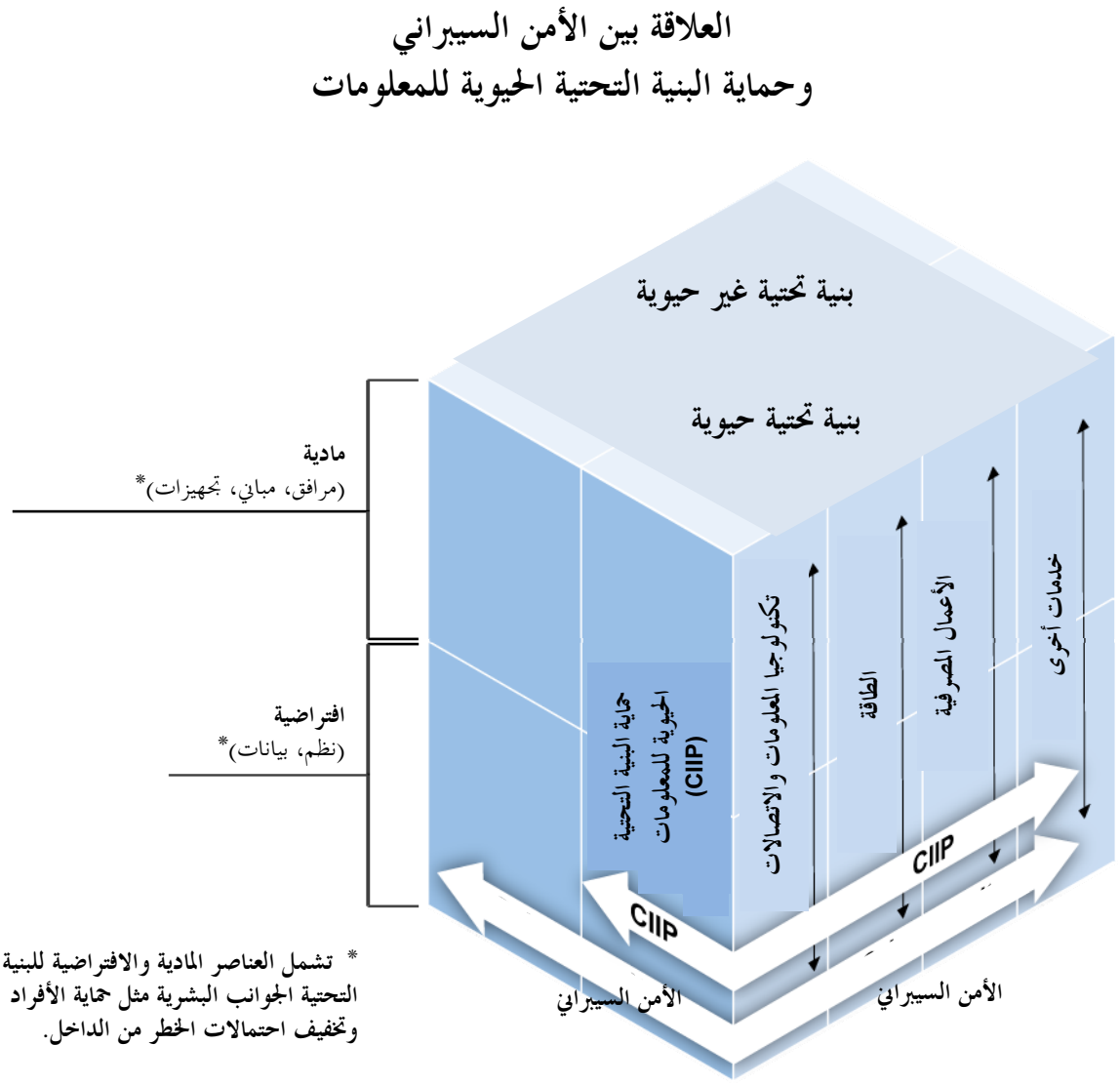
وقطاعات الخدمات الحكومية الأساسية. والبلدان في جميع مراحل التنمية في حاجة إلى تخطيط ووضع سياسات لحماية ما تقرر أنه يشكل لديها البنية التحتية الحيوية (أي بعبارة أخرى، حماية البنية التحتية الحيوية، بما في ذلك الحماية المادية والافتراضية) لتوفير قدر معقول من ضمان المرونة والأمن لدعم المهام الوطنية والاستقرار الاقتصادي.

وكل قطاع من هذه القطاعات الاقتصادية له أصوله المادية الخاصة به، مثل مباني المصارف، ومحطات الطاقة، والقطارات، والمستشفيات، والمكاتب الحكومية. ولكن هذه القطاعات الحيوية في اقتصاد بلد ما تعتمد كل الاعتماد على تكنولوجيات المعلومات والاتصالات. وعلى نحو شامل، فإن هذه القطاعات وأصولها المادية تعتمد اليوم على الأداء الموثوق به لهذه ***البنية التحتية الحيوية للمعلومات*** لتقديم خدماتها وتصريف شؤون أعمالها. وعليه، فإن حدوث أي عطل كبير في البنية التحتية الحيوية للمعلومات من شأنه أن يحدث على الفور أثراً موهناً يتجاوز مداه قطاع تكنولوجيا المعلومات والاتصالات، ويؤثر في قدرة البلد على أداء مهامه الأساسية في قطاعات متعددة. ومن شأن برنامج ***حماية البنية التحتية الحيوية للمعلومات*** أن يوفر الحماية للمكون الافتراضي للبنية التحتية الحيوية للمعلومات.

وكما يشار إليه في الشكل 1، تعتبر حماية البنية التحتية الحيوية للمعلومات (CIIP) مجموعة فرعية من البنية التحتية الحيوية للمعلومات والأمن السيبراني على السواء. ويوفر الأمن السيبراني الحماية من جميع أشكال الحوادث السيبرانية من خلال تعزيز سلامة البنية التحتية الحيوية للمعلومات التي تعتمد عليها القطاعات الحساسة، وتأمين الشبكات والخدمات التي توفر الاحتياجات اليومية للمستعملين. ويمكن للحوادث السيبرانية أن تؤثر على البنية التحتية للمعلومات الحيوية وغير الحيوية، وربما تأخذ أشكالاً كثيرة من أشكال الأنشطة الضارة، مثل استخدام روبوتات النت (botnets) في الهجمات المتعلقة برفض الخدمة ونشر الرسائل الاقتحامية والبرمجيات الضارة (مثل الفيروسات وبرمجيات وورم التخريبية) التي تؤثر في قدرة الشبكات على العمل. وبالإضافة إلى ذلك، قد تشمل الحوادث السيبرانية أنشطة غير مشروعة مثل التصيد الاحتيالي (phishing) والتحايل لسرقة المعلومات الشخصية (pharming)، علاوة على سرقة الهوية. والخطر السيبراني آخذ في الازدياد مع تزايد الأدوات والمنهجيات وتوفرها على نطاق واسع، ومع اتساع نطاق وتطور القدرات التقنية للمجرمين السيبرانيين. وقد تعرضت البلدان على مختلف مراحل تنميتها لهذه المخاطر السيبرانية.

ويشمل أي نهج وطني لتحقيق الأمن السيبراني زيادة الوعي بالمخاطر السيبرانية الحالية، وإنشاء هياكل وطنية لمعالجة مسألة الأمن السيبراني، وإقامة الروابط اللازمة التي يمكن الاستفادة منها في التصدي لما يقع من حوادث. ويشكل أيضاً تقييم الخطر، وتنفيذ تدابير لتخفيف الأثر، وإدارة النتائج جزءاً من أي برنامج وطني للأمن السيبراني. ومن شأن وضع برنامج وطني جيد للأمن السيبراني أن يساعد على حماية اقتصاد البلد من التمزق عن طريق المساهمة في استمرارية التخطيط عبر القطاعات، وحماية المعلومات المخزنة في أنظمة المعلومات، والحفاظ على ثقة الجمهور، وصيانة الأمن القومي، وضمان صحة الناس وسلامتهم.

الشكل 1: تصور للعلاقة بين حماية البنية التحتية الحيوية للمعلومات والأمن السيبراني



لا يمكن أن يقتصر تعزيز الأمن السيبراني على استراتيجية وطنية فحسب رغم أنه أمر هام للغاية، بل ينبغي استكماله باستراتيجيات إقليمية ودولية كما دعت إليه النتائج ذات الصلة بالقمة العالمية لمجتمع المعلومات (WSIS) في مرحلتيها في 2003-2005 ومتابعتها بشأن إجراءات خط العمل جيم5 القائمة على الرقمين 35 و36 من إعلان جنيف للمبادئ والرقم 39 من برنامج عمل تونس، وتنفيذ نتائج القمة العالمية لمجتمع المعلومات عن طريق القرارات والإجراءات والمبادرات ذات الصلة التي اعتمدها الاتحاد ولا سيما:

أ) الهدف 4 الوارد في القرار 71 لمؤتمر المندوبين المفوضين (المراجع في أنطاليا، 2006) "الخطة الاستراتيجية للاتحاد للفترة 2008-2011"؛

ب) القرار 130 لمؤتمر المندوبين المفوضين (المراجع في أنطاليا، 2006) "تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات"؛

ج) الأجزاء المعنية من خطة عمل الدوحة للمؤتمر العالمي لتنمية الاتصالات (WTDC-06)، بما في ذلك البرنامج 3 بشأن الاستراتيجيات الإلكترونية وتطبيقات تكنولوجيا المعلومات والاتصالات الذي يحدد الأمن السيبراني باعتباره أولوية بالنسبة لقطاع تنمية الاتصالات، مصحوباً بأنشطة محددة وخاصة اعتماد القرار 45 (الدوحة، 2006) بعنوان "آليات لتعزيز التعاون

في مجال الأمن السيبراني بما في ذلك مكافحة الرسائل الاقتحامية". ويكلف القرار 45 مدير مكتب تنمية الاتصالات بتنظيم اجتماعات لمناقشة أساليب تعزيز الأمن السيبراني بما في ذلك، ضمن جملة أمور، وضع مذكرة تفاهم لتعزيز الأمن السيبراني ومكافحة الرسائل الاقتحامية بين الدول الأعضاء المهتمة، وأن يقدم تقريراً عن نتائج هذه الاجتماعات إلى مؤتمر المندوبين المفوضين لعام 2006. ويمكن الاطلاع على تقرير مكتب تنمية الاتصالات المقدم إلى مؤتمر المندوبين المفوضين لعام 2006 على الموقع التالي: http://www.itu.int/md/S06-PP-C-0024-en.[3]

د) الأعمال المكثفة التي أجرتها لجنة الدراسات الرئيسية 17 لقطاع تقييس الاتصالات بشأن الأمن السيبراني والأنشطة التكميلية التي قامت بها لجنة الدراسات 13؛

هـ) القرار 58 الذي اعتمدته مؤخراً الجمعية العالمية لتقييس الاتصالات (جوهانسبرغ، 2008) بعنوان "تشجيع إنشاء أفرقة استجابة وطنية في حالات الحوادث المعلوماتية (CIRT)، خاصة للبلدان النامية" الذي اعترف بالأعمال التي اضطلعت بها المسألة 22.1 في قطاع تنمية الاتصالات؛

و) يلخص تقرير رئيس فريق الخبراء رفيع المستوى المعني بالبرنامج العالمي للأمن السيبراني (GCA) الذي أطلقه الأمين العام في 17 مايو 2007 مقترحات الخبراء بشأن الأهداف الاستراتيجية الرئيسية السبعة المتجسدة في هذه المبادرة، مع التركيز على التوصيات ذات الصلة في مجالات العمل الخمس التالية:

- التدابير القانونية
- التدابير التقنية والإجرائية
- الهيكل التنظيمي
- بناء القدرات
- التعاون الدولي

وتركز "التدابير القانونية" ضمن مجالات العمل هذه على كيفية تناول التحديات القانونية التي تثيرها الأنشطة الإجرامية المرتكبة على شبكات تكنولوجيا المعلومات والاتصالات بطريقة متوافقة دولياً. وتركز "التدابير التقنية والإجرائية" على التدابير الرئيسية لتعزيز اعتماد نهج معززة لتحسين الأمن وإدارة المخاطر في الفضاء السيبراني، بما في ذلك مخططات وبروتوكول ومعايير الاعتماد. ويركز "الهيكل التنظيمي" على الوقاية من الهجمات السيبرانية والكشف عنها والاستجابة لها وإدارة الأزمات، بما في ذلك حماية أنظمة البنية التحتية الحيوية للمعلومات. ويركز "بناء القدرات" على وضع استراتيجيات لآليات بناء القدرات لاستثارة الوعي، ونقل المعارف، وتقوية الأمن السيبراني في برنامج السياسة الوطنية. وأخيراً، يركز "التعاون الدولي" على التعاون والحوار والتنسيق الدولي في تناول قضايا الأمن السيبراني.[4] [5]

ز) مشروع الراي 4 الأخير الذي اعتمده المنتدى العالمي لسياسات الاتصالات بشأن "استراتيجيات تعاونية لبناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات"[6]، خاصة فقرتي يدعو الاتحاد الدولي للاتصالات ويدعو الدول الأعضاء.

ح) أنشطة البرنامج 3 (التطبيقات الإلكترونية) في مكتب تنمية الاتصالات عن طريق تقديم المساعدة المباشرة إلى الدول الأعضاء في البلدان النامية، من خلال مشاريع وأدوات بناء القدرات/التقييم الذاتي للأمن السيبراني على الصعيد الوطني/حماية البنية التحتية الحرجة للمعلومات (CITP) ومجموعة أدوات تخفيف آثار البرمجيات الروبوتية الضارة للاتحاد الدولي للاتصالات ومجموعة أدوات بناء القدرات لأفرقة الاستجابة الوطنية لحوادث أمن الحاسوب (CIRT).

---

[3] اصبحت الدول العربية بعد تجربتها خلال السنوات الأربع الماضية أكثر اقتناعاً بأن توقيع مذكرة تفاهم بين الدول الأعضاء لتعزيز الأمن السيبراني ومكافحة الرسائل الاقتحامية هو السبيل الأمثل للوفاء بالاحتياجات العالمية و/أو الإقليمية.

[4] أيد خبراء من الدول العربية جميع التوصيات الواردة في تقرير رئيس فريق الخبراء رفيع المستوى.

[5] يمكن الاطلاع على تفاصيل تقرير رئيس فريق الخبراء رفيع المستوى على الموقع:
http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf.

[6] يمكن الاطلاع على النص الكامل لمشروع الرأي 4 للمنتدى العالمي لسياسات الاتصالات على الموقع:
http://www.itu.int/osg/csd/wtpf/wtpf2009/documents/opinion4.pdf.

ط) أُطلقت مبادرة حماية الأطفال على الخط (COP) في نوفمبر 2008 كشبكة تعاونية دولية للعمل على النهوض بحماية الأطفال والشباب على الخط في جميع أنحاء العالم من خلال تقديم توجيهات بشأن السلوك الآمن على الخط بالاشتراك مع وكالات الأمم المتحدة والشركاء الآخرين. وتتمثل الأهداف الرئيسية لهذه المبادرة في: 1) تحديد المخاطر الرئيسية ومواطن الضعف التي تحيط بالاطفال والشباب في الفضاء السيبراني؛ 2) التوعية بالمخاطر والقضايا من خلال قنوات متعددة؛ 3) وضع أدوات لمساعدة الحكومات والمنظمات والمعلمين على تدنية المخاطر؛ 4) تبادل المعارف والخبرات مع تسهيل إقامة الشراكات الاستراتيجية الدولية لوضع وتنفيذ مبادرات ملموسة.

ي) هيئة التعاون بين الاتحاد الدولي للاتصالات والشراكة الدولية متعددة الأطراف لمواجهة التهديدات السيبرانية (IMPACT) في إطار برنامج العمل العالمي للاتحاد الدولي للاتصالات في مجال الأمن السيبراني، والتي تهدف إلى جمع أصحاب المصلحة الرئيسيين والشركاء من الحكومات وشركات القطاع الخاص والهيئات الأكاديمية لتوفير خبراتهم ومرافقهم ومواردهم للدول الأعضاء بالاتحاد من أجل مواجهة التهديدات السيبرانية بفعالية. والأهداف الرئيسية لهذه الهيئة التعاونية هي: 1) وضع إطار عالمي للمراقبة والإنذار والاستجابة في حالات الحوادث؛ 2) إنشاء الهياكل ووضع السياسات الدولية والإقليمية والمنظماتية، مثل الأفرقة الوطنية للاستجابة للحوادث الحاسوبية (CIRT)؛ 3) تسهيل بناء القدرات البشرية والمؤسسية في جميع القطاعات؛ 4) تسهيل التعاون الدولي بين أصحاب المصلحة المتعددين في جميع أنحاء العالم.

الجـــزء I

وضع استراتيجية وطنية للأمن السيبراني والحصول على موافقة عليها

يقتضي وضع وتنفيذ خطة وطنية للأمن السيبراني وجود استراتيجية شاملة تشمل استعراضاً عاماً أولياً لمدى كفاية الممارسات الوطنية الحالية والنظر في دور جميع أصحاب المصلحة (الهيئات الحكومية، والقطاع الخاص، والمواطنين) في هذه العملية.

ولأسباب تتعلق بالأمن القومي والرفاه الاقتصادي، تحتاج الحكومات إلى المساعدة في عملية حماية البنية التحتية لمعلوماتها الحيوية، وتعزيز هذه الحماية وضمانها. فالبنية التحتية للمعلومات في عصرنا الحالي تشمل جميع قطاعات الصناعة في أي بلد كما أنها تتجاوز حدود البلدان. ومن شأن الطابع الشامل للبنية التحتية الحيوية للمعلومات الذي يجعلها موجودة في كل مكان أن يهيئ فرصاً ومزايا اقتصادية هائلة.

على أن هذه المزايا تقترن أيضاً بالكثير من حالات الاعتماد المتبادل والمخاطر المكلفة. ولخَّصت دراسة جرت بتفويض من مكتب تنمية الاتصالات بالاتحاد هذه التكاليف على النحو التالي[7]:

> إن تكاليف وإيرادات جميع أصحاب المصلحة الضالعين في كامل شبكة القيمة لخدمات المعلومات مثل بائعي البرمجيات ومشغلي الشبكات وموردي خدمات الإنترنت (ISPs) والمستعملين تتأثر بالبرمجيات الخبيثة والرسائل الاقتحامية. وتشمل هذه الآثار، على سبيل المثال لا الحصر، تكاليف التدابير الوقائية وتكاليف العلاج والتكاليف المباشرة لعرض النطاق والتجهيزات وتكاليف فرص الازدحام. ومما يزيد من تعقيد هذا الأمر حقيقة أن البرمجيات الخبيثة والرسائل الاقتحامية تولد تدفقات جديدة للدخل، بعضها شرعي والبعض الآخر غير شرعي. حيث إنها تضفي الشرعية على نماذج للأعمال التجارية (مثل المنتجات المضادة للفيروسات وتلك المضادة للرسائل الاقتحامية والبنية التحتية وعرض النطاق) كما أنها تفسح المجال أمام نماذج إجرامية للأعمال التجارية (تأجير الشبكات الروبوتية وتقاضي عمولات على المبيعات المتولدة عن الرسائل الاقتحامية وخطط التلاعب بالأوراق المالية). وبالتالي تؤدي هذه العوامل إلى حوافز مختلطة وأحياناً متعارضة لدى أصحاب المصلحة تعمل على تعقيد التوصل إلى حلول متسقة لهذه المشكلة.

ولقد ظلت السياسات الوطنية في معظم البلدان، لعدة سنوات، تعامل شبكة الهاتف الوطنية العمومية التبديلية (PSTN) على أنها بنية تحتية أساسية، وتتولى حمايتها على هذا الأساس. وفي كثير من البلدان، تمتلك الشركات التجارية أجزاء كبيرة من البنية التحتية لهذه الشبكات وتعاونت مع الحكومات ومع بعضها بعضاً في هذا الجهد. غير أن التوسع السريع في تكنولوجيات المعلومات والاتصالات الرقمية الأساس في شبكات الاتصال السلكية واللاسلكية ذات الاتصال البيني أدى إلى إحداث تغيير جذري في طابع ومتطلبات أمن الشبكات وربما أصبحت معه سياسات وإجراءات الأمن المعتمد على شبكات الهاتف الوطنية العمومية التبديلية التقليدية غير كافية لتلبية المتطلبات الجديدة لتحقيق هذا الأمن.

وتقتضي التغييرات التي أحدثتها تكنولوجيات المعلومات والاتصالات مزيداً من التركيز على التعاون من جانب الحكومات والأعمال التجارية وغيرهما من المنظمات وفرادى المستعملين الذين يضعون ويملكون ويوردون ويديرون الخدمة، ويستخدمون أنظمة وشبكات المعلومات. وفي حين تواصل الحكومات في كثير من الأحيان الاضطلاع بدور قيادي في أمن الشبكات، فإن مما له أهميته الحاسمة ضمان إدماج أصحاب المصلحة الآخرين المعنيين، بمن فيهم مشغلو البنية التحتية وموزِّدوها، في عملية التخطيط ورسم السياسة بوجه عام. ومن خلال العمل معاً، يمكن لكل من الحكومة والقطاع الخاص أن يعززا من خبراتهما ومن إدارة المخاطر المتصلة بالبنية التحتية الحيوية للمعلومات. ومن شأن هذا الإدماج أن يضاعف من الثقة وأن يكفل تطوير وتطبيق السياسات والتكنولوجيات بالشكل الملائم والأكثر فعالية. وعلى الصعيد الدولي، تقتضي حماية البنية التحتية الحيوية للمعلومات وتعزيز الأمن السيبراني التعاون والتنسيق بين الدول والشركاء على الساحة الدولية.

---

[7] انظر مشروع الدراسة "الجوانب المالية لأمن الشبكات: البرمجيات الخبيثة والرسائل الاقتحامية"، ITU-D 1/144 (6 مايو 2008).

A.I عرض عام للأهداف في إطار هذا الجزء

1.A.I استثارة الوعي على مستوى السياسات الوطنية بقضايا حماية الأمن السيبراني والهياكل الأساسية الحيوية للمعلومات، وبالحاجة إلى الإجراء الوطني والتعاون الدولي.

2.A.I وضع استراتيجية وطنية لحماية الهياكل الأساسية الحيوية للمعلومات والفضاء السيبراني من الهجمات السيبرانية والمادية.

3.A.I المشاركة في الجهود الدولية الرامية إلى تنسيق الأنشطة الوطنية ذات الصلة بالوقاية من الحوادث والاستعداد والتصدي لها، والتعافي منها.

B.I الخطوات المحددة لتحقيق هذه الأهداف

الأهداف السابقة مشتركة بين جميع البلدان؛ بيد أن الخطوات المحددة التي تتخذ لتنفيذها تتباين بحسب الاحتياجات والظروف التي ينفرد بها كل بلد. وسوف تتولى الحكومات الوطنية، في كثير من البلدان، الاضطلاع بهذه الخطوات.

1.B.I إقناع المسؤولين الرئيسيين في الحكومات بالحاجة إلى إجراء وطني للتصدي للأخطار ومواطن الضعف في البنية التحتية السيبرانية الوطنية من خلال المناقشات على مستوى السياسات.

1. بالنسبة لأي دولة تسعى إلى تعزيز الأمن السيبراني وتأمين البنية التحتية لمعلوماتها الحيوية، تتمثل الخطوة الأولى في ترسيخ الأمن السيبراني باعتباره سياسة وطنية. وعلى وجه العموم، فإن أي بيان لسياسة وطنية للأمن السيبراني (1) يعترف بأهمية البنية التحتية الحيوية للمعلومات بالنسبة إلى البلد، (2) يحدد المخاطر التي تواجهه (في نهج يتناول عادةً جميع المخاطر[8])، (3) يحدد هدف سياسة الأمن السيبراني، (4) يحدد بوجه عام كيفية تنفيذ هذه السياسة، بما في ذلك عن طريق التعاون مع أصحاب المصلحة المعنيين.

وما أن يتم تحديد سياسة عامة واضحة للأمن السيبراني، فإن هذه السياسة يمكن التوسع فيها عن طريق استراتيجية وطنية تحدد الأدوار والمسؤوليات، وتضع الأولويات، وتقرر الأطر الزمنية والقياسات المتعلقة بالتنفيذ. وبالإضافة إلى ذلك، فإن السياسة والاستراتيجية قد يضعان أيضاً الجهود الوطنية في سياق الأنشطة الدولية الأخرى المضطلع بها في مجال الأمن السيبراني. ومن أجل وضع سياسة عامة للأمن السيبراني، قد يكون من الضروري زيادة الوعي بالمسائل التي ينطوي عليها الأمر فيما بين كبار المسؤولين عن اتخاذ القرارات. ويتعين على هؤلاء المسؤولين أن يدركوا أن بلوغ الأهداف المتفق عليها للأمن السيبراني قد يستغرق فترة طويلة.

2. لا ينبغي لأي إطار وطني للأمن السيبراني أن يتألف من سياسات لا يمكن تغييرها. وبدلا من ذلك، ينبغي أن يتوخى في وضع الإطار والسياسات التحلي بالمرونة والقدرة على الاستجابة لبيئة المخاطر الدينامية. وينبغي للإطار أن يحدد أهداف السياسة العامة. ومن خلال تحديد أهداف السياسة العامة، يمكن للوكالات الحكومية والكيانات غير الحكومية أن تعمل معاً من أجل بلوغ الأهداف المقررة على النحو الأكثر كفاءة وفعالية.

3. ينبغي وضع هذه السياسة الوطنية بصورة تعاونية من خلال عملية تشاور مع ممثلي فئات المشاركين المعنيين، بما في ذلك الوكالات الحكومية، والقطاع الخاص والأوساط الأكاديمية والرابطات المعنية. وينبغي نشر هذه السياسة على المستوى الوطني، ويفضل أن يكون ذلك من خلال رئيس الحكومة.

---

[8] النهج المتعلق *بجميع المخاطر* أو *النهج المتعدد المخاطر* والذي يتبع في إدارة المخاطر يشمل النظر في جميع المخاطر الطبيعية والتكنولوجية المحتملة؛ ويشمل ذلك حالات الكوارث الطبيعية والتي من صنع الإنسان (العرضية أو العمدية).

2.B.I تحديد شخص رئيسي ومؤسسة رائدة لتولي الاضطلاع بالجهد الشامل على المستوى الوطني؛ وتحديد المكان الحكومي الذي ينبغي أن ينشأ في إطاره فريق استجابة لحوادث أمن الحاسوب[9]، توكل إليه المسؤولية الوطنية في هذا المجال[10]؛ وتحديد المؤسسات الرائدة لكل جانب من جوانب الاستراتيجية الوطنية.

1) يتطلب الشروع في مبادرة تتعلق بالأمن السيبراني تحديد شخص يتولى، في المرحلة الأولية، قيادة الجهد الوطني المتعلق بهذا الأمن على المستوى الوطني، وهو شخص من العاملين بالحكومة على مستوى السياسات، وعلى إدراك بالمسائل المتعلقة بالأمن السيبراني، ويستطيع أن يوجه وينسق جهود المؤسسات الحكومية، وأن يتفاعل مع القطاع الخاص. وينبغي من الناحية المثالية أن يكون لهذا الشخص مكانة سياسية مرموقة وممن يحظون بإمكانية النفاذ إلى رئيس الحكومة. وهذه السلطة الرفيعة المستوى ضرورية لضمان التنسيق فيما بين الكيانات التي تحتاج إلى التفاعل بين بعضها البعض. وسوف يوفر ذلك في الوقت المناسب أساساً مؤسسياً يمكن أن يرتكز عليه القادة والمنظمات التقنية للأمن السيبراني في البلد.

2) بمجرد أن يشرع البلد في مبادرة تتعلق بالأمن السيبراني، قد لا تظل الحاجة قائمة إلى أن يضطلع بهذا الدور الشخص أو المؤسسة اللذين شرعا في هذا الجهد.

3) يتعين تحديد المؤسسات الأخرى المسؤولة عن وضع وتنفيذ أجزاء مختلفة من الاستراتيجية الوطنية للأمن.

3.B.I تحديد الخبراء وواضعي السياسات الملائمين داخل الوزارات الحكومية، والسلطات الحكومية والقطاع الخاص وأدوارهم.

1) تتطلب الإجراءات الوطنية الفعالة إدراج "ثقافة الأمن السيبراني" بين جميع المشاركين. وعلى جميع الأفراد والمؤسسات داخل الحكومة وخارجها، الذين يضعون أنظمة وشبكات المعلومات ويمتلكونها ويورِّدونها ويديرونها ويقومون بصيانتها ويستعملونها، تفهم الدور الذي يتعين أن يضطلعوا به والإجراءات التي ينبغي اتخاذها. ويجب على كبار صانعي السياسات وقادة القطاع الخاص تحديد الأهداف والأولويات داخل مؤسساتهم. ويتعين على كبار الخبراء الفنيين توفير الخطوط التوجيهية والأطر اللازمة لاتخاذ الإجراءات المطلوبة.

4.B.I تحديد الترتيبات التعاونية لجميع المشاركين وفيما بينهم.

1) ينبغي للحكومات الوطنية أن تعزز، على السواء، من الترتيبات التعاونية الرسمية وغير الرسمية التي تتيح وتشجع الاتصال وتبادل المعلومات فيما بين القطاع الخاص والحكومة. وسوف ينفذ الأمن السيبراني على المستوى التقني أو التشغيلي بواسطة طائفة عريضة من المؤسسات الحكومية وغير الحكومية. وينبغي أيضاً تنسيق هذه الجهود وإدراج آلية لتقاسم المعلومات.

5.B.I إقامة آليات للتعاون فيما بين الحكومات وكيانات القطاع الخاص على المستوى الوطني.

1) ينبغي وضع السياسات وبلورة وتنفيذ الخطط الوطنية من خلال عملية مفتوحة وشفافة. وينبغي أن تراعي هذه الجهود آراء ومصالح جميع المشاركين.

6.B.I تحديد النظراء الدوليين على المستوى المحلي للمشاركين المحليين، وتعزيز الجهود الدولية لمعالجة قضايا الأمن السيبراني، بما في ذلك تقاسم المعلومات وجهود المساعدة، على أن تؤخذ في الاعتبار نتائج المشروع المتعلق بتنفيذ القرار 45 الصادر عن المؤتمر العالمي لتنمية الاتصالات لعام 2006 (WTDC-06).

1) سيحصل الجهد الرامي إلى تحسين الأمن السيبراني الوطني على المساعدة من خلال المشاركة في المنتديات الإقليمية أو الدولية التي يمكن أن توفر التعليم والتدريب، في شكل مؤتمرات وورش عمل في أغلب الأحيان. وتقوم هذه المنتديات باستثارة الوعي بالقضايا، وتوفير عروض الخبراء، وإتاحة الفرصة للبلدان لتقاسم أفكارها وخبراتها ومنظوراتها. كما يمكن

---

[9] "فريق الاستجابة لحوادث أمن الحاسوب" هو فريق يتألف من خبراء أمن المعلومات، ويتمثل عمله الرئيسي في الاستجابة لحوادث أمن الحاسوب. ويوفر الفريق الخدمات اللازمة لمعالجة هذه الحوادث ومساعدة العناصر المتأثرة بها على التعافي من أي اختلالات (*A Step-by-Step Approach on How to Set Up a CSIRT* *على الموقع* http://www.enisa.europa.eu/act/cert. ويطلق على هذه الأفرقة أيضاً اسم أفرقة الاستجابة لحالات الطوارئ الحاسوبية أو أفرقة التأهب لحالات الطوارئ الحاسوبية (CERTs)، ويؤدي كلا النوعين من الأفرقة نفس المهام. ومصطلح "الحاسوب" في عبارة فريق استجابة لحوادث أمن الحاسوب يستعمل بصورة شاملة في هذا التقرير بحيث يغطي، على سبيل المثال، أجهزة المسيِّرات، والمخدمات، والأجهزة المتنقلة التي تعمل ببروتوكول الإنترنت، والتطبيقات المتصلة بها.

[10] لأغراض هذا التقرير، سيشار إلى الأفرقة الوطنية للاستجابة لحوادث أمن الحاسوب، اختصاراً، بالمختصر "N-CSIRT".

أن تساعد في هذا الجهد المشاركة و/أو العضوية في المنظمات الإقليمية والدولية العاملة نحو تحقيق أهداف مماثلة. وهذا هو أحد أهداف المشروع المتعلق بتنفيذ القرار 45.

2) المشاركة في البرامج والأنشطة المتاحة للمنظمات المتعددة الأطراف التي تسعى إلى تحسين أو تعزيز الأمن السيبراني العالمي هي طريقة أخرى من طرق تعزيز التعاون الدولي. ومن أمثلة المنظمات المتعددة الأطراف الاتحاد الدولي للاتصالات (خط العمل جيم5 للقمة العالمية لمجتمع المعلومات)، ومنظمة التعاون والتنمية في الميدان الاقتصادي، ومنظمة الدول الأمريكية، ومنظمة التعاون الاقتصادي لآسيا والمحيط الهادئ وغيرها. وبالإضافة إلى ذلك، هناك مؤتمرات أخرى يمكن للحكومات أن تتقاسم فيها المعلومات بشأن المسائل المتصلة بالأمن السيبراني، مثل مؤتمر الميريديان.

3) وبالإضافة إلى ذلك، ينبغي أيضاً النظر في مشاركة الجهود التي يقودها القطاع الخاص، مثل فريق العمل المعني بمكافحة الاحتيال الحاسوبي والجهود الدولية الأخرى المماثلة.

7.B.I إنشاء عملية إدارة متكاملة للمخاطر لغرض تحديد الجهود الوقائية المتعلقة بالأمن السيبراني ووضع الأولويات المتعلقة بها.

1) إن إدراك المخاطر هو السبيل الوحيد أمام الحكومات ومالكي البنى التحتية ومشغليها (بما في ذلك الموردون الذين يدعمونهم) لبدء تعاون بين القطاع العام والقطاع الخاص والناس من أجل تحديد الوظائف والعناصر الرئيسية للحماية ووضع الأولويات المتعلقة بها. وحال تحديد هذه الوظائف والعناصر، يمكن وضع الأولويات المتعلقة بوظائف البنية التحتية الحيوية للمعلومات أو ترتيبها من حيث الأهمية. ومن المهم ألا يغيب عن البال أن مفهوم الطابع "الحيوي" للبنية التحتية الحيوية للمعلومات أمر مرهون بالحالة المعنية، وما يمكن اعتباره حيوياً في حالة ما قد لا يكون حيوياً في حالة أخرى. وينبغي أن تضع الدول في اعتبارها، وهي تحدد ماهية الوظائف الحيوية وتضع الأولويات المتعلقة بها، أن الطابع الحيوي من شأنه أن يتغير بفعل التكنولوجيا، والبنية التحتية، وتحسين العمليات.

2) ويعد تحقيق الحماية للبنية التحتية الحيوية للمعلومات والفضاء السيبراني من الأمور التي تشكل تحدياً بالغاً. ذلك أن حماية البنية التحتية الحيوية للمعلومات والفضاء السيبراني والوظائف الحيوية التي تنطوي عليها هذه العملية إنما يقتضي التطبيق المستمر لمجموعة من الممارسات الخاصة بإدارة المخاطر (مثل تقييم المخاطر ومواطن الضعف والعواقب، وتحديد الضوابط وسبل التخفيف من الأثر، وضوابط التنفيذ، وقياس الفاعلية) بما يمكن المشغلين من إدارة المخاطر وكفالة توقي الصدمات عبر مراحل الاضطلاع بمهامهم الأساسية. وتتوفر عموماً لدى فرادى موفري البنية التحتية للمعلومات منهجيات وممارسات متقدمة لإدارة المخاطر بالنظر إلى طابع الوقت الفعلي للخدمات التي يقدمونها. بيد أن سمات التوصيلية، والترابط، والتعقيد التقني للبنية التحتية للمعلومات يحد من القدرة على القيام بسهولة بتقييم الخطر أو التأهب له. ونتيجة لذلك، تتحقق منافع كثيرة نتيجة لتعزيز التعاون بين القطاعين العام والخاص في مجال تقييم أوجه الترابط المشتركة والمخاطر التي تتعرض لها البنية التحتية (من كوارث طبيعية، وأعطال تكنولوجية، وهجمات إرهابية، وغيرها).

8.B.I تقييم الحالة الراهنة للأمن السيبراني وإعادة تقييمه دورياً ووضع أولويات البرامج.

1) ينبغي أن تتضمن الاستراتيجية الوطنية للأمن السيبراني مسحاً وطنياً لأغراض التقييم، يمكن استخدامه في عمليات التقييم الذاتي للتقدم الذي يجري إحرازه كجزء من التدريب أو جهد التقييم المدعم. ويمكن للبلدان، باستخدام أداة تقييم مشتركة، أن تحدد مواطن القوة والثغرات الممكنة في إطارها الوطني وأن تنشئ عملية لغرض تحقيق الاتساق مع الأهداف المرجوة. (أنشأ مكتب تنمية الاتصالات أدوات للتقييم الذاتي للأمن السيبراني على الصعيد الوطني/حماية البنى التحتية الحرجة للمعلومات (CIIP) لكي تكون مصاحبة لهذه الوثيقة المتعلقة بأفضل الممارسات).

9.B.I تحديد متطلبات التدريب وكيفية تحقيقها.

1) قد يجد أحد البلدان، كنتيجة لمقارنة أفضل الممارسات الموصى بها الواردة في هذا التقرير مع ممارساته الحالية بشأن الأمن السيبراني (أي إجراء تحليل للثغرات)، أن هناك جوانب في برنامجه معنية بالأمن السيبراني تحتاج إلى تحسين. وقد يكون الحل تقنياً (مثل الأجهزة أو البرمجيات الجديدة) أو قانونياً (مثل صياغة قوانين أو لوائح جديدة لمعالجة السلوك السيبراني غير الملائم) أو تنظيمياً. وقد يكشف تحليل الثغرات أيضاً عن الأماكن التي تحتاج إلى مزيد من بناء القدرات البشرية (التدريب).

الجـــزء II

إقامة التعاون بين الحكومة الوطنية والقطاع الخاص

تعد حماية البنية التحتية الحيوية للمعلومات والفضاء السيبراني مسؤولية مشتركة يمكن إنجازها على أفضل وجه عن طريق التعاون بين الحكومات على جميع المستويات والقطاع الخاص، الذي يمتلك ويدير جانباً كبيراً من البنية التحتية. وبالطبع، يجب أن يكون للحكومة الكلمة الأخيرة في أي قرارات وطنية تتخذ. ومن الأهمية بمكان الاعتراف بأنه على الرغم من أن الأنظمة العالمية لأمن المعلومات أصبحت إلى حد كبير قابلة للتشغيل البيني ومتصلة ببعضها البعض توصيلاً بينياً، فإن هيكل هذه الشبكات قد يتباين تبايناً كبيراً من بلد لآخر. ولذلك، فإن التعاون بين مالكي هذه الأنظمة ومشغليها من شأنه أن يعزز وجود نظام للأمن يتسم بالفعالية والاستدامة.

ولكل من الحكومة والقطاع الخاص مصلحة دائمة في ضمان مرونة البنية التحتية وقدرتها على توقي الصدمات. وبناءً على ذلك، فإن الشراكة بين القطاعين العام والخاص أمر أساسي لتعزيز الأمن السيبراني لأنه لا يمكن لكيان واحد أن يوفر الحماية للبنية التحتية بكاملها. وبالنظر إلى أن معظم مرافق البنية التحتية السيبرانية في بلدان كثيرة مملوكة و/أو يقوم بتشغيلها القطاع الخاص، فمن المحبذ أن تقوم الحكومة والصناعة، كل في مجال الدور المنوط به، بالعمل معاً بطريقة هادفة. ويقتضي نجاح التعاون بين القطاعين العام والخاص توفر ثلاثة عناصر هامة: (1) عرض واضح بقيمة هذا التعاون؛ (2) وصف واضح للأدوار والمسؤوليات؛ (3) الثقة.

عرض القيمة

يتوقف نجاح المشاركة على تحديد المنافع المتبادلة بين الشركاء من الحكومة والقطاع الخاص. وتتمثل المنافع التي تحققها الحكومة في قيام موردي البنية التحتية ومشغليها بتوفير القدرات التي تقع عادةً خارج نطاق الاختصاصات الأساسية للحكومة، من قبيل:

- ملكية وإدارة معظم البنية التحتية الحيوية في قطاعات كثيرة، وفي كثير من البلدان؛
- تفهم الأصول، والشبكات، والأنظمة، والمرافق، والمهام، وغيرها من القدرات؛
- الخبرة أو الدراية في مجال الاستجابة للحوادث؛
- القدرة على ابتكار وتوفير منتجات وخدمات وتكنولوجيات جديدة تركز سريعاً على الاحتياجات؛
- تصميم شبكة الإنترنت العالمية ونشرها وتشغيلها وإدارتها وصيانتها.

وفيما يتعلق بتقييم عرض القيمة بالنسبة إلى القطاع الخاص، فإن هناك منفعة واضحة في العمل مع الحكومة لتعزيز حماية البنية التحتية الحيوية للمعلومات والأمن السيبراني. ويمكن للحكومات أن تعزز من قيمة هذه العلاقة التعاونية بعدد من السبل، من بينها:

- تزويد الملاك والمشغلين بالمعلومات التحليلية والدقيقة والمجمعة والمفيدة، في الوقت المناسب، بشأن المخاطر التي تواجه البنية التحتية الحيوية؛
- إشراك القطاع الخاص منذ البداية في وضع المبادرات والسياسات المتعلقة بحماية البنية التحتية الحيوية؛
- أن توضح لقادة المؤسسات، عن طريق المحافل العمومية وبالاتصال المباشر، المنافع المحققة سواءً على مستوى الأعمال أو مستوى الأمن القومي عن طريق الاستثمار في تدابير أمنية تتجاوز مجرد استراتيجيات الأعمال التجارية الخاصة بهم؛
- تهيئة بيئة لتشجيع ودعم الحوافز للشركات لكي تقوم طواعية باعتماد الممارسات الأمنية السليمة والمقبولة على نطاق واسع، والقيام، حسب الاقتضاء، بتحديث وتحسين عملياتها وممارساتها الأمنية خارج نطاق ما تتطلبه مصالحها التجارية المحدودة؛
- العمل مع القطاع الخاص لتحديد مهام رئيسية لها وتحديد الأولويات الخاصة بها والمساعدة على حمايتها و/أو إصلاحها؛
- توفير الدعم للبحوث اللازمة لتعزيز مستقبل الجهود المبذولة في مجال حماية المعلومات الحيوية؛
- تحديد الموارد اللازمة للمشاركة في الاضطلاع بدراسات شاملة مشتركة بين القطاعات، عن طريق التدريبات والندوات والدورات التدريبية والنمذجة الحاسوبية مما يسفر عن دعم توجيه القرارات من أجل التخطيط لمواصلة الأعمال؛

- إتاحة تقاسم المعلومات ذات الحساسية الزمنية وتوفير الدعم المتعلق بالإصلاح والإنعاش لمرافق البنية التحتية والخدمات ذات الأولوية خلال أوقات الحوادث.

الأدوار والمسؤوليات

يمكن للحكومة والقطاع الخاص أن تضعا سوياً تفاهماً مشتركاً لأدوار ومسؤوليات كل منهما فيما يتعلق بالأمن السيبراني. ويمكن للحكومة أن توفر التنسيق والقيادة لجهود الحماية. وعلى سبيل المثال، فإن استمرار الحكومة يتطلب ضمان الأمن وتوافر البنية التحتية المادية للأنشطة السيبرانية الحكومية لدعم مهامها وخدماتها الأساسية. وبالإضافة إلى ذلك، يمكن للحكومة أن تقوم بدور تنسيقي في حالة وقوع كارثة أو يمكنها المساعدة في الحالات التي يفتقر فيها القطاع الخاص إلى الموارد الكافية للاستجابة لحادث معين. ويمكن للحكومة أن تعزز تشجيع الجهود الطوعية للقطاع الخاص من أجل تحسين الأمن، بما في ذلك وضع سياسات وبروتوكول لتقاسم المعلومات التحليلية والمفيدة وحسنة التوقيت بشأن المخاطر، وتوفير الحوافز للقطاع الخاص من أجل تعزيز الأمن خارج النطاق الذي تتطلبه حدود مصالح المؤسسات. وأخيراً، يمكن للحكومة أن تشرف على عمليات إجراء دراسات والقيام بالبحث والتطوير وتمويل هذه العمليات من أجل تحسين عمليات الأمن وأدواتها.

الثقـــة

الثقة هي عنصر أساسي لنجاح التعاون بين الحكومة والصناعة. كما أن الثقة لازمة لإيجاد وتطوير وتعزيز العلاقات المتبادلة بين الحكومة والقطاع الخاص. ومن شأن التعاون القوي وتبادل المعلومات بين القطاع الخاص والحكومة أن يعززا من الوعي بالحالات وتيسير التعاون بشأن المسائل الاستراتيجية، والمساعدة على إدارة المخاطر السيبرانية ودعم أنشطة الاستجابة والإنعاش. ومن خلال تحسين تقاسم المعلومات وتحليلها، ستكون الحكومة والقطاع الخاص أفضل إعداداً لتحديد المخاطر ومواطن الضعف، وتبادل التكتيكات والموارد التخفيفية والوقائية.

وتدرج أدناه الأهداف العامة التي ينبغي أن تضعها الحكومات في الاعتبار لدى تعاونها مع القطاع الخاص.

A.II عرض عام للهدف في إطار هذا الجزء

1.A.II إقامة الروابط التعاونية بين الحكومة والقطاع الخاص التي من شأنها أن تؤدي بشكل فعال إلى إدارة المخاطر السيبرانية وحماية الفضاء السيبراني.

2.A.II توفير آلية للجمع بين مجموعة متنوعة من المنظورات والأصول والمعارف لغرض التوصل إلى توافق في الآراء والمضي قدماً معاً من أجل تحسين الأمن على المستوى الوطني.

B.II الخطوات المحددة لتحقيق هذا الهدف

1.B.II إدراج المنظورات المتعلقة بالقطاع الخاص في المراحل المبكرة لوضع وتنفيذ سياسة الأمن والجهود المتصلة بها.

1) في بلدان عديدة، تكون معظم البنى التحتية الحيوية، والعناصر السيبرانية التي تعتمد عليها، مملوكة ملكية خاصة ويجري تشغيلها عن طريق القطاع الخاص. وبفضل ابتكارات القطاع الخاص يطرأ تطور سريع على التكنولوجيات التي تشكل الفضاء السيبراني وتدعمه. ولذلك، فإنه لا يمكن للحكومات بمفردها أن توفر الأمن الكافي للفضاء السيبراني. ومما له قيمته البالغة بالنسبة لجهود الأمن السيبراني التي تبذلها الحكومات لوضع وتنفيذ سياسة للأمن السيبراني وأطر لإدارة المخاطر، إدراك وجهات نظر القطاع الخاص وإدماج الملاك والمشغلين الرئيسيين للبنية التحتية الحيوية في هذه الجهود. ويمكن للحكومات أن تطلع على آراء القطاع الخاص في هذا الشأن عن طريق المشاركة في الأفرقة العاملة المشتركة بين الحكومات والقطاع الخاص، والتماس التعليقات من القطاع الخاص بشأن وضع سياسات واستراتيجيات الأمن السيبراني، وتنسيق الجهود مع منظمات القطاع الخاص عن طريق آليات تقاسم المعلومات. وينبغي للحكومة أن تكفل مشاركة القطاع الخاص في المراحل الأولية لوضع المبادرات والسياسات وتنفيذها ومواصلة العمل بها.

2) ينبغي أن تتعاون الحكومات والقطاع الخاص على اعتماد نهج لإدارة المخاطر يتيح للحكومة والقطاع الخاص تحديد البنية التحتية السيبرانية وتحليل المخاطر، وتقييم مواطن الضعف، وتقييم الآثار الناجمة عن المخاطر، وتحديد سبل التخفيف من هذه الآثار.

3) ينبغي أن تتعاون الحكومات والقطاع الخاص على متابعة أنشطة البحث والتطوير التي تستهدف إدارة المخاطر السيبرانية. ومن شأن وضوح الرؤية فيما يتعلق بأولويات البحث والتطوير والمبادرات التي يضطلع بها كل من القطاع الخاص والحكومة أن يكفل تخصيص الموارد واستخدامها على نحو فعال، ووضع مبادرات البحث والتطوير على أساس ملائم من حيث التوقيت، وأن تصبح النواتج والخدمات قيد الإعداد في نهاية المطاف في وقت ملائم من أجل تعزيز الأمن السيبراني الوطني.

2.B.II التشجيع على إنشاء أفرقة للقطاع الخاص من مختلف صناعات البنية التحتية الحيوية لمعالجة الاهتمامات الأمنية المشتركة بالتعاون مع الحكومة.

1) يمكن للمعلومات المستمدة من هذه الأفرقة، مثل رابطات الأعمال التجارية، في مختلف قطاعات البنية التحتية، أن تساعد على مواجهة الاحتياجات المشتركة في مجال الأمن السيبراني. ويمكن لهذه الأفرقة أن تركز على المسائل الاستراتيجية و/أو التشغيلية وإدارة الشواغل الأمنية المتصلة بالقطاع الخاص ككل. ويمكن أن تشمل هذه المسائل إدارة المخاطر، والتوعية ووضع السياسات وتنفيذها، ومسائل أخرى جمَّة. وتوفر أفرقة القطاع الخاص هذه عملية مؤسسية للمشاركة مع الحكومات ويمكن الاستعانة بها كمنتدى لإجراء الحوارات الحساسة بشأن المسائل المتصلة بالأمن السيبراني.

2) وفي بعض البلدان، قام العديد من قطاعات البنية التحتية الحيوية بإنشاء هذه الأفرقة للجمع بين ممثلي القطاعات لتقاسم المعلومات بشأن المخاطر الأمنية، ومواطن الضعف، والآثار الناجمة. وفي أحيانٍ كثيرة، تقوم هذه الأفرقة أيضاً بتوفير التنبيهات والإنذارات في الوقت الفعلي للأعضاء لتيسير الجهود المبذولة للتخفيف من آثار الحوادث التي تتعرض لها البنية التحتية الحيوية والاستجابة لهذه الحوادث والتعافي منها.

3) وينبغي لهذه الأفرقة أن تنظر في اعتماد ممارسات تتيح التعاون وتبادل المعلومات بين الأعضاء (أي الحكومات والقطاع الخاص) في منتدى موثوق به. وقد تشمل بعض هذه الممارسات توفير ما يلي: عدم الإفصاح عن هوية الأعضاء؛ النفاذ إلى المعلومات الحكومية والشاملة لعدة قطاعات؛ النفاذ إلى النواتج الحساسة المتعلقة بالمخاطر ومواطن الضعف والنواتج التحليلية؛ وخبرة في مجال الموضوع بشأن تنسيق الاستجابة في حالات الطوارئ، والممارسات التشغيلية والتمرينات. ومع النظر في هذه الممارسات من أجل إتاحة التعاون، من المهم إدماج سبل حماية المعلومات التي تخضع لحقوق الملكية والمعلومات الحساسة تجارياً.

3.B.II الجمع بين أفرقة القطاع الخاص والحكومة في منتديات موثوق بها لمناقشة التحديات المشتركة في مجال الأمن السيبراني.

1) هناك عدة شروط ضرورية لبناء ثقة وتعزيز التعاون الناجح بين الحكومة والقطاع الخاص. ويوصى بوضع اتفاق مكتوب يوفر التوجيهات بشأن التعاون والتبادل بين الحكومة والقطاع الخاص. ويحتاج المشاركون إلى تقاسم الرؤية والهدف. وتقوم القيادات الفردية أو التنظيمية القوية بتحديد الأولويات، وتخصيص الموارد، وتحديد الالتزامات المطلوبة لمواصلة التعاون بين القطاعين العام والخاص ويلزم أيضاً وجود قواعد للمشاركة لتوجيه السلوك الفردي والتنظيمي في إطار علاقة التعاون.

2) ويجب أن يتوصل المشاركون إلى نتائج ملموسة وقابلة للقياس. ويعد وضع عرض بقيمة التعاون بين الأفراد والمنظمات، والتحديد الواضح لهذه القيمة، أمراً أساسياً لتطوير ومواصلة الروابط التعاونية بين القطاعين العام والخاص.

4.B.II تشجيع التعاون بين الأفرقة من الصناعات المترابطة.

1) يمكن للحوادث التي تنطوي على نوع واحد من البنية التحتية أن تكون لها آثار تعاقبية وتؤدي إلى وقوع حوادث في أنواع أخرى من البنية التحتية. وعلى سبيل المثال، فإن انقطاع الطاقة ربما يؤدي إلى تعطيل الخدمات الهاتفية وخدمة الإنترنت. وعلاوة على ذلك، فرغم أن بعض الناس ربما يخططون لحالات الطوارئ في إطار قطاعاتهم الخاصة، ينبغي لهم أيضاً أن يأخذوا في الاعتبار ما يمكن أن يكون لهذه الحوادث من آثار على قطاعات أخرى. ويمكن لتقاسم المعلومات عبر مختلف البنى التحتية أن يساعد الجهود الرامية للاستجابة إلى الحوادث على نحو يشمل عدة قطاعات لها أهميتها على الصعيد الوطني.

5.B.II وضع ترتيبات تعاونية بين الحكومات والقطاع الخاص لإدارة الحوادث.

1) يمكن في حالات كثيرة التقليل من الأضرار الناجمة عن الحوادث السيبرانية من خلال التعرف السريع عليها، وتبادل المعلومات بشأنها، ومعالجتها. وعلى المستوى الوطني يلزم التعاون بين الحكومة والقطاعين العام والخاص لإجراء التحليلات وإصدار الإنذارات وتنسيق جهود الاستجابة.

2) ينبغي أن تتعاون الحكومات والصناعة في وضع إطار للتنسيق الاستراتيجي والتشغيلي والتثقيفي من أجل تحسين إدارة الحوادث. وينبغي أن يتضمن هذا الإطار شكلاً رسمياً لتقاسم المعلومات يضم جهات تنسيق للمسائل المتصلة بالسياسات وتبادل المعلومات التشغيلية. وينبغي أن يشمل الإطار أيضاً السياسات والإجراءات المتعلقة بتقاسم المعلومات بشأن الحوادث وتقديم تقارير عنها، وحماية ونشر المعلومات مسجلة الملكية (الخاصة بالحكومة والقطاع الخاص)، وآليات لنقل هذه المعلومات ونشرها. وغالباً ما تتضمن معلومات القطاع الخاص معلومات ذات ملكية مسجلة للشركات يمكن أن يؤدي نشرها إلى خسارة حصص في الأسواق أو إلى دعاية مناوئة، أو إلى أي آثار سلبية أخرى. وبالمثل، فإن المعلومات الحكومية قد تكون سرية أو حساسة وليست للنشر لعامة الجمهور. ومن ثم ينبغي وضع السياسات والتدابير التقنية اللازمة لحماية المعلومات مع القيام في الوقت ذاته بتحقيق التوازن فيما يتعلق بحق الجمهور في المعرفة. ويمكن للحكومات أن تواصل بناء الثقة من خلال تعزيز سياسات تقاسم المعلومات وإقامة الروابط مع القطاع الخاص عن طريق مواصلة سياسات التقييم. ويمكن أيضاً للتمرينات السيبرانية أن تختبر إمكانات الاتصال والتنسيق بين الحكومة والقطاع الخاص فيما يتصل بالاستجابة للحوادث السيبرانية وجهود التعافي منها عن طريق نشر آليات للتمرين في وقت الأزمات الفعلية.

الجـــزء III

ردع الجريمة السيبرانية

يمكن تحسين الأمن السيبراني، ضمن جملة أمور أخرى، عن طريق إنشاء وتحديث القوانين والإجراءات والسياسات الجنائية الداعمة لمنع الجريمة السيبرانية وردعها والرد عليها وتقديم مرتكبيها إلى المحاكمة.

A.III عرض عام للهدف في إطار هذا الجزء

1.A.III سن وإنفاذ مجموعة شاملة من القوانين ذات الصلة بالأمن السيبراني والجرائم السيبرانية.

يحتاج كل بلد لقوانين تعالج الجرائم السيبرانية في حد ذاتها، وإجراءات التحقيقات الإلكترونية وتقديم المساعدات للبلدان الأخرى. وقد تكون القوانين، أو لا تكون، في مكان واحد في النظام القضائي. ولأغراض تبسيط الأمور، تفترض هذه الوثيقة أنه سيكون لدى كل بلد قانون لمكافحة الجرائم السيبرانية بالإضافة إلى مجموعة من القوانين الإجرائية ونصوص قانونية تتعلق بالمساعدة المتبادلة ذات الصلة. وبطبيعة الحال، سوف تستخدم البلدان البنية التي تفضلها.

B.III الخطوات المحددة لتحقيق هذا الهدف

1.B.III تقييم السلطات القانونية الحالية للتأكد من كفايتها. ويتعين على البلد أن يستعرض قانونه الجنائي الحالي، بما في ذلك الإجراءات ذات الصلة لتحديد ما إذا كان كافياً لمعالجة المشاكل في الحاضر (والمستقبل). ويقترح اتخاذ الخطوات التالية:

1) القيام، حسب الاقتضاء، بوضع التشريعات اللازمة ذات الصلة، على أن تراعى، على وجه الخصوص، المبادرات الإقليمية، التي تشمل، ليس على سبيل الحصر، اتفاقية مجلس أوروبا المعنية بالجريمة السيبرانية (2001). وينبغي لهذه التشريعات أن تتناول، في جملة مسائل أخرى، الإضرار بالبيانات الحاسوبية أو إتلافها؛ والآليات الإجرائية التي تدعم التحقيقات، بما في ذلك القدرة على تتبع مصدر رسائل البريد الإلكتروني، وما إلى ذلك؛ وإدراج التعاون القانوني الدولي الممكن (من قبيل الحصول على الأدلة، وغير ذلك).

2) ينبغي لأي بلد أن ينظر فيما إذا كانت قوانينه تستند إلى توقعات تكنولوجية فات أوانها. وعلى سبيل المثال، فربما يكون هناك قانون يناقش تتبع إرسالات الصوت فقط. وقد يحتاج الأمر تغيير مثل هذا القانون بحيث يشمل إرسال البيانات أيضاً.

3) ينبغي لقانون الجريمة السيبرانية لأي بلد أن يخضع لتقييم جميع السلطات الحكومية والهيئات التشريعية المعنية التي قد تكون لها مصلحة في هذا القانون، حتى ولو لم تكن لها صلة بموضوع العدالة الجنائية، حتى لا تهدر أي فكرة مفيدة. وربما يلاحظ أحد مسؤولي تكنولوجيا المعلومات، على سبيل المثال، أن قانون الجريمة السيبرانية غير كاف للتطرق إلى تكنولوجيا جديدة استعمالها آخذ في التزايد لكنها ليست معروفة بعد على نطاق واسع لدى واضعي القوانين في ذلك البلد.

4) وبالإضافة إلى ذلك، يوصى أيضاً بأن يخضع القانون الجنائي المعمول به في أي بلد لعملية تقييم مماثلة من جانب بعض أو جميع الجهات التالية: القطاع الخاص المحلي، وأي فرع محلي لقطاع خاص دولي، والمنظمات غير الحكومية المحلية، والدوائر الأكاديمية، والخبراء المعترف بهم، وفئات المواطنين.

5) يمكن لأي بلد أن يلتمس المشورة بشأن هذه المسائل من بلدان أخرى.

2.B.III صياغة واعتماد القوانين الفنية والإجرائية والخاصة بالمساعدات المتبادلة لمعالجة الجريمة السيبرانية.

1) يوصى بأن تقوم البلدان بالمشاركة الفعالة، حسب الاقتضاء، في وضع التشريعات اللازمة، آخذة في الاعتبار على وجه الخصوص المبادرات الإقليمية، بما في ذلك، ليس على سبيل الحصر، اتفاقية مجلس أوروبا المعنية بالجريمة السيبرانية. ويوصى بأن تشارك البلدان في التعاون الإقليمي والدولي لأغراض مكافحة الجريمة السيبرانية وتعزيز الأمن السيبراني، وأن تضع آليات لتحسين التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية والبرمجيات الضارة وروبوتات الحاسوب، وغيرها.

2) ينبغي أن يخضع مشروع قانون الجريمة السيبرانية في أي بلد لتقييم جميع السلطات الحكومية والهيئات التشريعية. وينبغي أن يتاح هذا المشروع أيضاً للجمهور للتعليق عليه بغرض التطرق إلى أي تكنولوجيات أو اختلالات أو أي مسائل أخرى محتملة لم تتم تغطيتها أصلاً.

3) وينبغي أن يتناول أي قانون خاص بالجرائم السيبرانية لا الجرائم السيبرانية التقليدية فحسب، مثل الجرائم الحاسوبية وعمليات الاقتحام الحاسوبية، ولكن أيضاً حماية الأدلة الإلكترونية على الشبكات فيما يتعلق بالجرائم الأخرى.

4) ينبغي عدم توسيع أو تفسير قوانين حماية البيانات التي وضعت لخدمة الحياة المدنية والتجارة مما يعيق بصورة غير ملائمة من تدفق الأدلة الجنائية فيما بين البلدان.

5) يتعين على البلدان التي تقرر الاستعانة بخبراء استشاريين للقيام بعمليات الصياغة، أن تدرس مؤهلاتهم والإشراف على أعمالهم طوال عملية الصياغة. وقد لا يدرج الأشخاص الذين لم يحصلوا على التدريب بصورة محددة في إطار قانون البلد جميع الأحكام اللازمة بصورة كافية، وخاصة الأقسام المتعلقة بالنواحي الإجرائية والمساعدة القانونية المتبادلة. وعلاوة على ذلك، فإن من المستبعد أن ينظر الأشخاص الذين لا يمتلكون الخبرات القضائية بصورة كافية إلى التفاصيل الدقيقة لإثبات إحدى الحالات. وهناك بعض الخبراء الاستشاريين المؤهلين لصياغة القوانين التجارية إلا أنهم ليسوا كذلك بالنسبة للقوانين الجنائية.

6) ويجوز التشاور مع البلدان الأخرى للحصول على اقتراحات تتجاوز ما تحتويه الاتفاقية. فعلى سبيل المثال، قد تطلب البلدان من موردي خدمات الإنترنت الاحتفاظ ببعض البيانات التي تُنقل عبر أنظمتها لبعض الوقت، لمدة ستة أشهر في أغلب الأحيان، أو قد تحتاج إلى إبلاغ السلطات الحكومية ببعض حوادث الحاسوب ذات الأهمية المعينة؛ أو قد تتطلب إثبات الهوية بشكل ملائم من أي شخص قبل أن يستخدم مقهى سيبرانياً.

7) ويجوز لأي بلد أن يلتمس، إذا سمح الوقت، تعليقات على مشروع قانون الجرائم السيبرانية (أو تعديلات) من البلدان الأخرى والمنظمات المتعددة الأطراف. ويمكن الحصول على هذه التعليقات بصفة شخصية، وسيكون من المفيد، كما أشير أعلاه، الحصول على وجهات نظر العديد من البلدان استناداً إلى خبراتها.

8) ويتعين على البلد أن يطلب كذلك في أبكر مرحلة ممكنة (بما يتفق والإجراءات الوطنية)، تعليقات من الجهات المعنية ذات الاهتمام المعترف به بالموضوع: القطاع الخاص المحلي وأي فرع محلي لقطاع خاص دولي والمنظمات غير الحكومية المحلية والدوائر الأكاديمية والمواطنين المهتمين غير المنتسبين وغيرهم.

3.B.III إنشاء أو تحديد وحدات وطنية معنية بالجرائم السيبرانية.

1) من المهم أن يكون لدى كل بلد، بصرف النظر عن مستوى التنمية التي وصل إليها، قدرة أساسية على الأقل على التحري عن الجرائم السيبرانية. فعلى سبيل المثال، فإن استخدام الهواتف الخلوية قد اتسع بقوة حتى في البلدان النامية، ويمكن أن تستخدم هذه الهواتف الخلوية في ارتكاب أعمال الاحتيال وتحويل الأموال والتآمر وإرسال الفيروسات إلى الشبكات الإلكترونية وإشعال المتفجرات، وما إلى ذلك.

2) ويتعين على كل بلد أن يختار أو أن يوفر التدريب لوحدة للتحقيق في الجرائم السيبرانية تختص بالتحريات عن الجرائم السيبرانية على المستوى الوطني. وسيكون من الواضح في بعض الأحيان تحديد دائرة أو دوائر إنفاذ القانون التي يتعين أن تضطلع بذلك. وقد تختلف بعض وكالات إنفاذ القانون المتنافسة في الرأي في بعض الأحيان على هذا الاختيار، وسوف يتعين على السلطات العليا أن تتخذ قرارات صعبة. وحتى إذا تبين أنه لا يوجد في هذا البلد أي شخص في الوقت الحاضر يتمتع بالمهارات اللازمة، فإن من الصحيح القول أيضاً بأن هناك واحداً من موظفي إنفاذ القانون في مكان ما مهتماً بالتكنولوجيا الإلكترونية ولديه طموح على تعلم المزيد والمضي قدماً في هذا المجال.

3) وتحتاج وحدات التحقيقات في الجرائم السيبرانية إلى الدعم، حتى إذا كانت تتكون من عدد محدود من المحققين. فهي تحتاج إلى معدات حديثة وتوصيلات يعتمد عليها بصورة معقولة بالشبكات واستمرار التدريب. وقد يأتي هذا الدعم من جانب حكومة البلد أو من المنظمة الدولية أو من البلدان الأخرى أو من المنح التي يقدمها القطاع الخاص.

4) ومن المستصوب حيثما يكون ممكناً أن يكون لدى الوحدات قدرة أساسية، على الأقل، في مجال الطب الشرعي الحاسوبي. وسوف تتطلب هذه القدرة توافر أدوات برامجية وتدريبات إضافية. (وإذا رُئي أنه من المتعذر توفير هذه القدرة في مجال الطب الشرعي، يتعين على البلدان أن تقبل مسبقاً احتمال ضياع أدلة حاسمة حتى في قضايا حاسمة). وفي بعض الظروف،

قد تتوافر مساعدة قضائية من بلدان أخرى في قضايا معينة. وعلاوة على ذلك، فإن التدريب على التحقيقات الشرعية السيبرانية قد يتاح من بلدان أخرى أو من المنظمات المعنية. وعلى سبيل المثال، يقدم مركز تنسيق فريق الاستجابة لحالات الطوارئ الحاسوبية في جامعة كارنيغي – ميلون في الولايات المتحدة (http://www.cert.org) بعض التدريب في مجال التحقيقات الشرعية السيبرانية دون مقابل أو بأسعار منخفضة للغاية على الخط مباشرة أو من خلال أقراص CD-ROM .

5) ويتعين بمجرد إنشاء وحدة مكافحة الجرائم السيبرانية الإعلان عن وجودها وقدراتها لدى دوائر إنفاذ القانون الأخرى وللمدعين العامين في البلد. وليس من المفيد أن توجد وحدة لمكافحة الجرائم السيبرانية في العاصمة إذا كانت قوة إقليمية لإنفاذ القانون تقوم بالتحقيق في جريمة مروعة تتضمن أدلة إلكترونية إلا أنها لا تدري أن هناك وحدة لمكافحة الجرائم السيبرانية يمكن أن تقوم بعمليات البحث في الحاسوب المعني أو تقديم مساعدات أخرى. وللأسف فإن من الشائع كثيراً، في مختلف أنحاء العالم، أن المؤسسة التي تتولى إنفاذ القوانين في البلد ليس لديها دراية بأن البلد لديه وحدة لمكافحة الجرائم السيبرانية.

6) وينبغي لوحدات مكافحة الجرائم السيبرانية أو الوحدات التي يمكنها القيام بذلك، أن تقيم صلات مع الشركاء الدوليين إلى أقصى حد ممكن. ففي المراحل الأولى، تتوافر المشورة بشأن إنشاء الوحدة من البلدان الأخرى، أو منظمات إنفاذ القانون الدولية. وفي المراحل اللاحقة، يتوافر التدريب بأشكال كثيرة أو حتى الأجهزة والبرمجيات من البلدان الأخرى، ومن منظمات إنفاذ القانون الدولية ومن المنظمات المعنية المتعددة الأطراف ومن القطاع الخاص. وسوف تكون هذه الصلات مهمة لسبب آخر: فإن من المهم في عالم يتزايد ترابطه باطراد أن يستطيع البلد أن يطلب المساعدة من جهة خارجية لإنفاذ القانون.

7) كما ينبغي لوحدات مكافحة الجرائم السيبرانية أن تقيم صلات مع كل قطاع من القطاعات ذات الصلة أو المهتمة داخل بلدانها، من قبيل المنظمات غير الحكومية المحلية وأفرقة الاستجابة لحوادث الأمن الحاسوبي، وكيانات القطاع الخاص والأوساط الأكاديمية لضمان إعلامهم بوجود الوحدة وبقدراتها، وبأنهم يمكنهم التعاون معها، ومعرفة كيفية تقديم تقارير عن أي جرائم سيبرانية محتملة.

4.B.III إقامة علاقات تعاونية مع العناصر الأخرى في البنية التحتية للأمن السيبراني الوطني والقطاع الخاص.

1) تعتبر العلاقات التعاونية فيما بين الكيانات الحكومية والعناصر الأخرى في البنية التحتية للأمن السيبراني الوطني والقطاع الخاص مهمة لعدة أسباب:

أ) لتبادل المعلومات فيما بين هذه المجموعات (مثل الإبلاغ عن أنه يجري التفكير في قانون جديد أو أن هناك تكنولوجيا جديدة قيد الاستحداث)؛

ب) لتبادل وجهات النظر (مثل "هل إذا وضعنا قانوناً جديداً على نسق تلك الخطوط، هل ترى إمكانية حدوث مشاكل تتعلق بالخصوصية؟" أو "هل توجد أية وسيلة يمكن من خلالها تغيير تلك التكنولوجيا لكي يظل من الممكن إجراء عملية تتبع البريد الإلكتروني إذا كانت هناك أسباب مشروعة تتعلق بالسلامة العامة؟")؛

ج) لتبادل التدريب على الرغم من أن التدريب سوف يقدمه القطاع الخاص في معظم الحالات للحكومة؛

د) لتبادل الإنذارات بشأن الأخطار أو مواطن الضعف؛

هـ) لكي يتعرف الناس من مختلف القطاعات بعضهم ببعض بصورة جيدة بما يكفي لبناء الثقة فيما بينهم أثناء حالات الطوارئ.

2) تتمثل الخطوة الأولى الجيدة في تشكيل هذه العلاقات في أن يقوم واحد أو أكثر من الناس بوضع قائمة تعريف بالأشخاص في جميع القطاعات ذات الصلة في البلد. ويمكن أن تدرج في هذه القائمة معلومات عن كيفية الاتصال بهذه الشخصيات. وربما يكون من الأفضل الاحتفاظ بهذه القائمة بصورة غير رسمية لتجنب الصراعات بشأن الشخصية التي أدرجت في هذه القائمة أو التي لم تدرج فيها.

3) ومن المحتمل أن يوجد في كل بلد العديد من القطاعات ذات الصلة التي تنطوي على نقطة مساعدة في مجال الأمن السيبراني – المشرعون والوزارات والمنظمات غير الحكومية وفرق الاستجابة لحوادث الأمن الحاسوبي والأوساط الأكاديمية والقطاع الخاص والأفراد. وقد يكون بعض هؤلاء على النطاق المحلي الخالص والبعض الآخر تابعاً لكيانات أجنبية أكبر.

5.B.III تنمية الفهم بين المدّعين العامّين والقضاة والمشرعين لقضايا الجرائم السيبرانية.

1) من أجل التصدي على النحو الملائم لقضايا الجريمة السيبرانية، من المهم أن يكون المدّعون العامُّون والقضاة على دراية معقولة بمجالات مثل الحواسيب والبرمجيات والشبكات علاوة على الأهمية المتزايدة للأدلة الإلكترونية. وبالمثل، ينبغي أن يتمتع المشرعون بقدر من الدراية بهذه الموضوعات وبما إذا كانت قوانين بلدهم تعالج الجريمة السيبرانية على نحو كاف. والتدريب هو أحد الحلول لهذه المشكلة.

2) وإذا كان التدريب التقني الأساسي مطلوباً، فيمكن أن يأتي من مصادر مختلفة بحسب موارد البلد:

أ) أي إدارة أو وزارة محلية تتمتع باختصاصات تقنية مثل إدارة الشرطة أو أي وزارة خاصة بتكنولوجيا المعلومات؛

ب) الحكومات الأجنبية؛

ج) المنظمات المعنية المتعددة الأطراف؛

د) القطاع الخاص المحلي؛

ه) القطاع الخاص الدولي وخاصة (ولكن ليس حصرياً) إذا كان لديه أعمال على المستوى المحلي؛

و) الأوساط الأكاديمية ذات الصلة؛

ز) فرق الاستجابة لحوادث الأمن الحاسوبي المحلية أو الخارجية؛

ح) المنظمات غير الحكومية المحلية والأجنبية ذات الصلة.

3) وقد يكون من المفيد تدريب كبار صانعي السياسات والموظفين الحكوميين وغيرهم على الأخطار الكامنة في الشبكات الإلكترونية (مثل الكيفية التي يتم بها مهاجمة شبكة المصارف الوطنية) وعن التهديدات التي تفرضها الشبكات الإلكترونية (مثل استخدام الإنترنت في تحديد مواقع الأطفال الضعفاء لاستغلالهم في الاتجار الجنسي). وينبغي أن يتوافر التدريب فيما يتعلق بالجوانب الخاصة بالشبكات الإلكترونية من المصادر المشار إليها أعلاه.

4) قد يكون التدريب مطلوباً للمدعين العامين والقضاة فيما يتعلق بالمحاكمات الخاصة بالجرائم السيبرانية أو غير ذلك من الجرائم التي تنطوي على أدلة إلكترونية أو استخدام الأدلة الإلكترونية أو بشأن وسائل الحصول على التعاون الدولي. ويمكن أن يتوافر التدريب من:

أ) الإدارة أو الوزارة المحلية التي تتمتع بالاختصاصات الصحيحة مثل مكتب المدعي العام أو وزارة العدل؛

ب) الحكومات الأجنبية؛

ج) المنظمات المعنية المتعددة الأطراف؛

د) الأوساط الأكاديمية ذات الصلة؛

ه) المنظمات غير الحكومية المحلية والأجنبية ذات الصلة؛

و) الأفراد المعنيون.

5) قد يرغب البلد في الحصول على تدريب في مجال الصياغة القانونية. ويمكن أن يتوافر هذا التدريب من المجموعات المدرجة في الفقرة أعلاه. وقد يشكّل القطاع الخاص المحلي والقطاع الخاص الدولي، وخاصة (ولكن ليس حصرياً) إذا كان لديه أعمال على المستوى المحلي، مصادر محتملة للخبرة. غير أن الأمر الأرجح هو أن كيانات القطاع الخاص سوف تكون قادرة على المساعدة في مجال قوانين التجارة الإلكترونية أكثر منها في مجال الجرائم السيبرانية والإجراءات الجنائية والقوانين الدولية المتعلقة بالمساعدات القانونية المتبادلة.

6) وبالنسبة لجميع أنواع التدريب، قد تعرض المصادر أن توفر التدريب بنفسها في البلد الطالب أو قد تعرض وحدات تدريبية (إلكترونية أو مطبوعة) يمكن أن يستخدمها المدربون من ذلك البلد في إجراء عمليات التدريب بأنفسهم. وفي بعض الحالات، مثل التدريب في مركز تنسيق فرق الاستجابة لحالات الطوارئ الحاسوبية المشار إليه في القسم 4.3.B.III، يمكن تقديم هذا التدريب دون رسوم أو رسوم ضئيلة للغاية.

7) وفي بعض البلدان، كان العنصر الرئيسي في استثارة الوعي الوطني بقضايا الجرائم السيبرانية يتمثل في الدعم المقدم من كبار المسؤولين، أو حتى في بعض الأحيان من مسؤول كبير ذي نفوذ، ولا سيما أولئك الذين يتحكمون في الميزانيات. ومن المعروف جيداً أنه إذا كان أحد الوزراء شديد الاهتمام بالأمن السيبراني، فإن وزارته – وربما بقية الحكومة، قد تعرض دعماً أفضل على أولئك العاملين الذين يحاولون إنجاز شيء في هذا المجال.

6.B.III المشاركة في نقاط اتصال شبكة الجرائم السيبرانية المفتوحة يومياً على مدار الساعة (7/24).

1) انشأت في عام 1997 مجموعة الدول الصناعية الثمانية الكبرى (G8) مجموعة فرعية معنية بجرائم التكنولوجيا الرفيعة بدأت تعمل في إطار شبكة نقطة الاتصال 24/7 بإدارة وزارتي العدل والداخلية في مجموعة G8 وذلك لتحسين المساعدة الدولية في حالات التحقيقات العاجلة التي تتضمن أدلة إلكترونية. وقد رأى الكثير من المحققين في الجرائم السيبرانية أن ثمة صعوبة شديدة في التعرف على المكان الذي يمكن الحصول منه على مساعدات سريعة من البلدان الأخرى. وعلاوة على ذلك، رأى الكثير من المحققين أن معاهدات المساعدات القانونية المتبادلة لم تساعد في الحالات السريعة التطور التي تتضمن، على سبيل المثال، اقتحامات للحاسوب في منتصف الليل في الأنظمة المالية للبلد. وقد تنامت هذه الشبكة حتى أصبحت تضم ما يقرب من 50 بلداً في أوائل عام 2008. وهذه الشبكة مفتوحة لانضمام أي بلد تكون لديه القدرة اللازمة على تقديم المساعدة على النحو المبين أدناه.

2) ويتعين على البلدان، لكي تنضم إلى هذه الشبكة، أن تقدم جهة اتصال يمكن الوصول إليها طوال 24 ساعة في اليوم و7 أيام في الأسبوع – ومن هنا جاء الاسم غير الرسمي "الشبكة 24/7". ويمكن أن تكون جهة الاتصال شخصاً يتم الوصول إليه بصورة مباشرة أو عن طريق أحد المكاتب. ويتعين أن يفهم هذا الشخص ثلاثة أشياء: 1) التكنولوجيا، حتى يمكن إرسال الطلبات دون التأخير الذي تتطلبه الشروح التكنولوجية المطوَّلة؛ 2) القانون المحلي الساري في بلد هذا الشخص؛ 3) ما هي الأعمال التي يسمح بها القانون المحلي لهذا الشخص بالقيام بها لمساعدة البلدان الأخرى. وإذا لم يكن لدى جهة الاتصال شخصياً هذه الأنماط الثلاثة من المعارف، يتعين عليه أن يكون قادراً على الوصول على الفور إذا اقتضى الأمر (وليس مجرد خلال يوم العمل التالي) إلى أي شخص ذي أهلية في حكومته يكون مأذوناً له بتقديم المساعدة في هذا المجال.

3) ويتعين أن تذهب المراسلات، في البداية على الأقل، من جهة اتصال الشبكة 24/7 في البلد A إلى جهة الاتصال المماثلة في البلد B لضمان الاتساق والأمن. ويعني ذلك أنه يتعين أن لا تقدم جهات الاتصال معلومات الاتصال لمكاتب أخرى في بلدانها. وبدلا من ذلك يتعين على جهات الاتصال أن تجري الاتصال الدولي الأول نيابة عن المكتب الطالب (مثل قوة إنفاذ القانون المحلية) في بلدانها. وبعد إقامة التعاون الأولي بين بلدين، يجوز لجهة الاتصال، إذا رغبت في ذلك، أن تنسحب من التحقيقات وتترك لهيئة إنفاذ القانون المحلية ذات الصلة في البلد A الاتصال بصورة مباشرة بالبلد B.

4) ولا تضمن البلدان، بانضمامها إلى هذه الشبكة، أنها ستساعد بعضها بعضاً دائماً أو أن شبكة الاتصال هذه تحل مكان المساعدات القانونية المتبادلة العادية بين البلدين. وبدلاً من ذلك فإن شبكة الاتصال لا تضمن سوى أن يحصل البلد الطالب على اهتمام واعٍ وقادر بصورة مباشرة حتى في منتصف الليل. وبعد أي مساعدات أولية، قد تطلب البلدان (أو لا تطلب) استخدام قنوات المساعدات المتبادلة الأكثر بطئاً.

5) ولا يعني التوافر على امتداد 24 ساعة من اليوم أن المكتب مجهزٌ ليل نهار بعدد معين من أجهزة الحاسوب ومحققين في الجرائم السيبرانية ينتظرون الرد على المكالمات الهاتفية أو الرسائل بالبريد الإلكتروني. ولا تدير معظم البلدان مثل هذا المكتب. والأمر الأكثر شيوعاً، هو أن يكون هناك أحد موظفي إنفاذ القانون (ربما عدد من الموظفين على أساس التناوب) في أحد البلدان يمكن الوصول إليه عن طريق الهاتف – وربما يكون بوسعه أن يخلد إلى النوم وبجانبه هاتف خلوي.

6) ويتعين على البلدان، لكي تنضم لهذه الشبكة، الاتصال برئيس الفريق الفرعي المعني بجرائم التكنولوجيا الرفيعة في مجموعة البلدان الصناعية الثمانية (G8) (لا تقتصر عضوية هذه الشبكة على أعضاء مجموعة البلدان الصناعية الثمانية (G8) حيث ينتمي لها في الوقت الحاضر أكثر من 50 بلداً). ويتعين ملء استمارة بسيطة قصيرة[11]. ولا تتطلب هذه العملية أي اتفاقات دولية رسمية مثل مذكرة تفاهم أو معاهدات. ومن آن لآخر، توفر شبكة 7/24 التدريب ومؤتمرات الربط الشبكي لجهات الاتصال. وقد قدمت إعانات للسفريات لهذه المؤتمرات حسب مقتضى الحال.

7) وتتحمل الوحدة التي تنضم إلى الشبكة مسؤولية أن تتيح لإدارات الشرطة المعنية الأخرى أو وحدات مكافحة الجرائم السيبرانية في بلدها العلم بوجودها وتوافرها لتقديم المساعدات في إجراء الاتصالات خارج البلد.

[11] ينبغي إرسال هذه الاستمارة على الفاكس 6113 514 202 1+ وتوجه لعناية المنسق، الشبكة 24/7، قسم الجرائم الحاسوبية والملكية الفكرية، وزارة العدل الأمريكية، واشنطن العاصمة، الولايات المتحدة الأمريكية. ويمكن إرسالها أيضاً عبر البريد الإلكتروني richard.green@usdoj.gov.

الجـــزء IV

إنشاء منظمة وطنية لإدارة الحوادث: المراقبة والإنذار والاستجابة والانتعاش

من المهم أن تقوم الحكومة بإنشاء أو تحديد منظمة وطنية تعمل كجهة اتصال لضمان الفضاء السيبراني وحماية البنية التحتية الحيوية للمعلومات تتضمن المهام الموكل إليها المراقبة والإنذار والاستجابة وجهود الانتعاش وتيسير التعاون بين الكيانات الحكومية والقطاع الخاص؛ والدوائر الأكاديمية؛ والمجتمع الدولي.

ويتعلق أحد الأدوار الرئيسية للحكومات في معالجة الأمن السيبراني على المستوى الوطني في الإعداد لرصد وإدارة الحوادث السيبرانية والاستجابة لها. وتتطلب الإدارة الفعالة للحوادث النظر في اعتبارات التمويل والموارد البشرية والتدريب والقدرات التكنولوجية والعلاقات بين الحكومات والقطاع الخاص والمتطلبات القانونية. ويعتبر التعاون على جميع المستويات الحكومية ومع القطاع الخاص والدوائر الأكاديمية والمنظمات الدولية عنصراً ضرورياً لإدارة الحوادث ولاستثارة الوعي بالحوادث المحتملة والخطوات اللازمة صوب العلاج. وللحكومات دور رئيسي لضمان التنسيق بين هذه الكيانات.

A.IV عرض عام للأهداف في إطار هذا الجزء

يتطلب إنشاء قدرات وطنية في مجال إدارة الحوادث سلسلة من الأنشطة الشديدة الترابط فيما بينها، بما في ذلك ما يلي:

1.A.IV إقامة نظام وطني منسق للاستجابة لأمن الفضاء السيبراني لتلافي الحوادث السيبرانية وتتبعها وردعها والاستجابة لها والتعافي منها.

2.A.IV إنشاء جهة تنسيق لإدارة الحوادث السيبرانية بحيث تضم هذه الجهة العناصر المهمة في الحكومة (بما في ذلك عنصر إنفاذ القانون) والعناصر الأساسية من مشغلي البنية التحتية والموردين بغية الحد من المخاطر والتخفيف من حدة الحوادث.

3.A.IV المشاركة في آليات مراقبة الحوادث والإنذار بها والاستجابة لها وتقاسم المعلومات بشأنها.

4.A.IV وضع الخطط والإجراءات والبروتوكولات بشأن الاستجابة لحالات الطوارئ، واختبارها، والتمرين عليها بما يكفل بناء الثقة بين المتعاونين من الجهات الحكومية وغير الحكومية وتعاونهم الفعال وقت الأزمات.

B.IV الخطوات المحددة لتحقيق هذه الأهداف

يعد إنشاء قدرة وطنية لإدارة الحوادث مهمة طويلة الأجل تبدأ بإنشاء قدرة وطنية أو فرقة وطنية للاستجابة لحوادث الحاسوب (CIRT)[12، 13].

1.B.IV تحديد أو إنشاء قدرات وطنية لفرقة (CIRT).

1) قد تؤدي الاستجابة الفعالة للحوادث السيبرانية الكبيرة إلى الحد من الأضرار التي تلحق بأنظمة المعلومات وضمان توافر وسائل فعالة للاستجابة والحد من طول أمد الوقت اللازم للانتعاش وتكاليفه. ويتعين بالاقتران مع القطاعين العام والخاص وجود فرقة استجابة لحوادث الأمن الحاسوبي المعينة وطنياً (CIRT) للعمل كجهة اتصال مع الحكومة وخاصة فيما يتعلق بالحوادث ذات الأهمية الوطنية لتنسيق الدفاع ضد الحوادث السيبرانية والتصدي لها. ويتعين في هذه الحالات، أن تعمل فرقة الاستجابة لحوادث الأمن الحاسوبي مع سلطات إنفاذ القوانين والمعلومات دون أن تقوم بتوجيه أنشطتها أو مراقبتها.

2) يتوقع أن تقوم فرقة الاستجابة لحوادث الأمن الحاسوبي (CIRT) بتوفير الخدمات والدعم لتلافي القضايا ذات الصلة بالأمن السيبراني والاستجابة لها والعمل كجهة اتصال وحيدة للإبلاغ عن حوادث الأمن السيبراني والتنسيق والاتصالات ذات الصلة. ويتعين أن تتضمن مهام هذه الفرقة الوطنية التحليل والإنذار وتقاسم المعلومات والحد من مواطن الضعف

---

[12] انظر القرار 58 للجمعية العالمية لتقييس الاتصالات. يطلق في بعض البلدان على CIRT الفرقة الوطنية للاستجابة لحوادث الأمن الحاسوبي (NCSIRT) أو الفرقة الوطنية للاستجابة لحوادث الحاسوب (N-SIRT).

[13] يمكن أن تؤثر نتائج الأعمال التي يتعين أن يضطلع بها قطاع تقييس الاتصالات بموجب القرار 58 على الجزء الرابع من أفضل الممارسات هذه.

والتخفيف ومعاونة جهود الانتعاش الوطنية للبنية التحتية للمعلومات الحرجة. وينبغي، على وجه الخصوص، أن تقوم الفرقة الوطنية للاستجابة لحوادث الأمن الحاسوبي بالعديد من الوظائف على المستوى الوطني بما في ذلك ما يلي دون أن تقتصر عليه:

- رصد وتحديد النشاط الخارج على القياس؛
- تحليل المخاطر السيبرانية ومواطن الضعف ونشر المعلومات المتعلقة بالإنذار بالأخطار السيبرانية؛
- تحليل وتجميع المعلومات المتعلقة بالحوادث ومواطن الضعف التي توزعها الجهات الأخرى، بما في ذلك الموردون وخبراء التكنولوجيا لتوفير تقييم يقدم لأصحاب المصلحة المهتمين؛
- إقامة آليات اتصالات موثوق بها وتيسير الاتصالات فيما بين أصحاب المصلحة لتقاسم المعلومات ومعالجة القضايا ذات الصلة بالأمن السيبراني؛
- توفير معلومات الإنذار المبكر، بما في ذلك المعلومات المتعلقة بالتخفيف من مواطن الضعف والمشاكل المحتملة؛
- وضع استراتيجيات للتخفيف والاستجابة وتفعيل الاستجابة المنسقة للحوادث؛
- تقاسم البيانات والمعلومات عن الحوادث والاستجابة المقابلة؛
- تتبع ورصد المعلومات لغرض تحديد الاتجاهات واستراتيجيات العلاج طويلة الأجل؛
- نشر أفضل الممارسات العامة المتعلقة بالأمن السيبراني والتوجيهات المتعلقة بالاستجابة للحوادث وتلافيها.

2.B.IV إقامة آلية أو آليات داخل الحكومة للتنسيق بين الوكالات المدنية والحكومية.

1) يتمثل أحد الأدوار الرئيسية للفرقة الوطنية للاستجابة لحوادث الأمن الحاسوبي في نشر المعلومات، بما في ذلك المعلومات عن مواطن الضعف والأخطار الحالية على أصحاب المصلحة المعنيين. وتمثل الوكالات الحكومية المعنية أحد أصحاب المصلحة المجتمعية ويتعين إشراكها في أنشطة الاستجابة.

2) ويمكن أن يتخذ التنسيق الفعال مع هذه الكيانات عدة أشكال منها، على سبيل المثال، ما يلي: إقامة موقع على شبكة الويب لتبادل المعلومات؛ توفير المعلومات عن طريق قوائم المراسلات بما في ذلك النشرات الإخبارية وتقارير الاتجاهات والتحليل؛ إعداد المطبوعات التي تتضمن التنبيهات والأفكار المفيدة والمعلومات عن مختلف جوانب الأمن السيبراني بما في ذلك التكنولوجيات الجديدة ومواطن الضعف والأخطار والنتائج.

3.B.IV إقامة شراكات مع دوائر الصناعة للاستعداد لمواجهة الحوادث السيبرانية على المستوى الوطني وتتبعها والاستجابة لها والتعافي منها.

1) يتعين أن تتعاون الحكومات والفرقة الوطنية للاستجابة لحوادث الأمن الحاسوبي مع القطاع الخاص. ونظراً لأن القطاع الخاص في كثير من البلدان يمتلك الجزء الأكبر من البنية التحتية الحيوية للمعلومات وأصول تكنولوجيا المعلومات، يتعين على الحكومات العمل مع القطاع الخاص لتحقيق هدفها الجامع الخاص بالإدارة الفعالة للحوادث.

2) تتيح العلاقات التعاونية مع القطاع الخاص، والقائمة على الثقة، للحكومات اكتساب نظرة متعمقة في الكثير من جوانب البنية التحتية الحيوية التي يملكها ويديرها القطاع الخاص. ويمكن للتعاون بين القطاعين العام والخاص والناس أن يساعد في إدارة المخاطر المرتبطة بالأخطار السيبرانية ومواطن الضعف والآثار الناجمة، وتحقيق التوعية بالأوضاع على مستوى العالم من خلال تقاسم المعلومات، والتوعية، والمشاركات المتبادلة.

3) التشجيع على تطوير ممارسات تقاسم المعلومات بين القطاع الخاص والحكومة بما يتيح تقاسم المعلومات التشغيلية في الوقت الفعلي.

4) هناك بعض الوسائل لتشجيع هذه الشراكات منها تحديد المنافع التي تعود على كل من الحكومة والقطاع الخاص، ووضع وتنفيذ برامج تضمن حماية بيانات الملكية الحساسة، وإنشاء أفرقة عمل مشتركة بين القطاعين العام والخاص بشأن إدارة المخاطر السيبرانية وإدارة الحوادث، وتقاسم أفضل ممارسات الاستجابة للحوادث وإدارتها ومواد التدريب، والتعاون في تحديد الأدوار والمسؤوليات الخاصة بالحكومة والقطاع الخاص في إدارة الحوادث وفي وضع بروتوكولات متماسكة وقادرة على التنبؤ على مر الوقت.

4.B.IV إقامة جهة أو جهات اتصال داخل الوكالات الحكومية والقطاع الخاص والشركاء الدوليين لتيسير التشاور والتعاون وتبادل المعلومات مع الكيان الوطني المسؤول عن الاستجابة للحوادث (CIRT).

1) يعتبر تحديد جهات الاتصال الملائمة وإقامة علاقات عمل تعاونية لأغراض التشاور والتعاون وتبادل المعلومات عنصراً أساسياً للآلية المنسقة والفعالة الوطنية والدولية المعنية بالاستجابة للحوادث. ويمكن أن تعزز هذه العلاقات من الإنذار المبكر بالحوادث السيبرانية المحتملة وتبادل المعلومات عن الاتجاهات والأخطار والاستجابات فيما بين كيانات الاستجابة للحوادث وأصحاب المصلحة الآخرين.

2) ويمكن أن توفر إقامة جهات اتصال محدَّثة وقنوات اتصال مع دوائر أصحاب المصلحة تبادل المعلومات الاستباقية وفي الوقت المناسب فيما يتعلق بالاتجاهات والأخطار والإسراع بالاستجابة. ومن المهم، إلى أقصى حد ممكن، إقامة اتصالات تستند إلى وظائف الإدارات وليس إلى الأفراد لضمان أن تظل قنوات الاتصال مفتوحة حتى عندما يترك الأفراد المنظمة. وتبدأ العلاقات في كثير من الأحيان ببناء الثقة مع أفراد معينين إلا أنها ينبغي أن تتطور إلى ترتيبات أكثر اتساماً بالطابع النظامي والمؤسسي.

5.B.IV المشاركة في الأنشطة التعاونية وأنشطة تقاسم المعلومات على المستوى الدولي.

1) ينبغي أن تشجع الحكومة التعاون مع المنظمات والبائعين والخبراء الآخرين المعنيين بهذا الموضوع على: (1) الاستجابة المسبقة للحوادث باعتبارها قاعدة عالمية للسلوك. (2) أن تعزز وتدعم الإمكانات لفرق الاستجابة لحوادث الأمن الحاسوبي للانضمام إلى المؤتمرات والمحافل الدولية والإقليمية، بغية بناء القدرات من أجل تحسين آخر ما توصلت إليه التكنولوجيا في الاستجابة للحوادث على المستوى الإقليمي، (3) التعاون في مجال تنمية مواد CIRT على المستوى الوطني وإبلاغها إلى سلطات CIRT بفعالية.

6.B.IV وضع أدوات وإجراءات لحماية الموارد السيبرانية للكيانات الحكومية.

1) تتطلب عملية الإدارة الفعالة للحوادث أيضاً وضع وتنفيذ سياسات وإجراءات ومنهجيات وأدوات أمنية لحماية الأصول السيبرانية للحكومات وأنظمتها وشبكاتها ووظائفها. ويمكن أن يتضمن ذلك، بالنسبة لفرقة الاستجابة لحوادث الأمن الحاسوبي، إجراءات التشغيل المعيارية ومبادئ توجيهية للعملية الداخلية والخارجية وسياسات أمنية للتنسيق مع أصحاب المصلحة وتنفيذ شبكات المعلومات الآمنة لعمليات فرقة الاستجابة لحوادث الأمن الحاسوبي وتأمين الاتصالات. ويتعين على فرق الاستجابة لحوادث الأمن الحاسوبي، بوصفها جهة اتصال بشأن الاستجابة للحوادث، التنسيق مع بعضها الآخر والمساعدة في التمكين من التعاون مع كيانات الاستجابة للحوادث الأخرى. ويتعين على الحكومات أن توفر التدريب المستمر لجميع الموظفين الجدد والحاليين بشأن الاستجابة للحوادث.

7.B.IV القيام من خلال الفرقة الوطنية للاستجابة للحوادث بإنشاء قدرة على تنسيق العمليات الحكومية للاستجابة للهجمات السيبرانية واسعة النطاق والتعافي منها.

1) في حالة وقوع حادثة ترقى إلى مستوى الأهمية الوطنية، سيلزم وجود جهة اتصال مركزية للتنسيق مع الكيانات الحكومية الأخرى ومع أصحاب المصلحة الآخرين، مثل القطاع الخاص. ومن المهم وضع الخطط والإجراءات التي تكفل استعداد الفرقة الوطنية للاستجابة للحوادث للتصدي لأي حادث محتمل.

8.B.IV التشجيع على ممارسات الإفصاح التي تتسم بالمسؤولية من أجل حماية العمليات وسلامة البنية التحتية السيبرانية.

1) من حين لآخر، قد تُكتشف مواطن ضعف في منتجات تكنولوجيا المعلومات كالتجهيزات أو البرمجيات. وينبغي إتخاذ القرارات الخاصة بكشف المعلومات الخاصة بمواطن الضعف للجمهور على أساس كل حالة على حدة، بحيث لا يُساء استعمال هذه المعلومات. وينبغي إتاحة الوقت الكافي للبائعين قبل أي عملية من عمليات الكشف عن المعلومات هذه.

الجـــزء V

الترويج لثقافة وطنية للأمن السيبراني

نظراً لما أصبحت عليه الحواسيب الشخصية من قوة تتزايد باطراد، وأن التكنولوجيات تتقارب في سماتها، وأن استخدام تكنولوجيا المعلومات والاتصالات يتزايد انتشاره باطراد، وأن التوصيلات عبر الحدود الوطنية آخذه في التزايد، يتعين على جميع المشاركين الذين يقومون بوضع وملكية وتوريد وإدارة الخدمات ويستخدمون شبكات المعلومات فهم قضايا الأمن السيبراني، وأن يتخذوا من الإجراءات ما يتناسب وأدوارها في حماية الشبكات. وينبغي للحكومات أن تمسك بزمام القيادة في نشر ثقافة الأمن السيبراني ودعم جهود المشاركين الآخرين.

A.V عرض عام للهدف في إطار هذا الجزء

1.A.V الترويج لثقافة وطنية للأمن بما يتسق مع قرار الجمعية العامة للأمم المتحدة 57/239، إرساء ثقافة عالمية للأمن السيبراني[14]، والقرار 58/199، إرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية البنى التحتية الحيوية للمعلومات[15].

1) تتطرق مسألة الترويج لثقافة وطنية للأمن ليس فقط لدور الحكومة في تأمين تشغيل واستخدام البنية التحتية للمعلومات، بما في ذلك الأنظمة التي تديرها الحكومة، ولكن أيضاً لتوعية القطاع الخاص، والمجتمع المدني، والأفراد. وبالمثل، فإن هذا العنصر يشمل تدريب مستعملي الأنظمة الحكومية والخاصة، وإدخال تحسينات في المستقبل على الجوانب الأمنية، ومسائل أخرى هامة تشمل الخصوصية، والرسائل الاقتحامية، والبرمجيات الضارة.

2) ووفقاً لما أوردته تقارير منظمة التعاون والتنمية في الميدان الاقتصادي، فإن القوى الدافعة الرئيسية لأي ثقافة للأمن على المستوى الوطني تتمثل في تطبيقات الحكومة الإلكترونية وخدماتها، وحماية البنية التحتية الحيوية للمعلومات. ونتيجة لذلك، ينبغي للإدارات الوطنية تنفيذ تطبيقات وخدمات الحكومة الإلكترونية من أجل تحسين عملياتها الداخلية وتوفير الخدمات الأفضل للقطاع الخاص والمواطنين. ولا ينبغي تناول مسألة أمن أنظمة وشبكات المعلومات من منظور تكنولوجي فحسب، ولكن ينبغي أن يشمل هذا المنظور عناصر من قبيل تلافي المخاطر، وإدارة المخاطر، وتوعية المستخدمين. ورأت منظمة التعاون والتنمية في الميدان الاقتصادي أن التأثير المفيد لأنشطة الحكومة الإلكترونية يتمثل في الانتقال إلى ما يتجاوز الإدارة العامة صوب القطاع الخاص والأفراد. ويبدو أن مبادرات الحكومة الإلكترونية قد عملت كعنصر مضاعف نحو تعزيز نشر ثقافة الأمن.

3) ينبغي للبلدان من خلال أنشطتها التعاونية، والأفضل من خلال نوع من الاتفاقات أن تعتمد نهج متعدد التخصصات ومتعدد أصحاب المصلحة إزاء تنفيذ الأمن السيبراني، ويقوم بعضها بإنشاء هيكل إدارة رفيع المستوى لتنفيذ السياسات الوطنية. وتعتبر مبادرات استثارة الوعي والتوعية على جانب كبير من الأهمية، بجانب تقاسم أفضل الممارسات وإقامة الشراكات فيما بين المشاركين واستخدام المعايير الدولية.

4) ويكتسي التعاون الدولي أهمية بالغة في تعزيز ثقافة للأمن، جنباً إلى جنب مع دور المنظمات الإقليمية في تيسير التفاعلات والتبادلات.

B.V الخطوات المحددة لتحقيق هذه الأهداف

1.B.V تنفيذ الخطة الأمنية للأنظمة التي تديرها الحكومة.

1) تتضمن الخطوة الأولية للإجراء الحكومي الرامي إلى تأمين الأنظمة التي تديرها وضع وتنفيذ خطة أمنية وطنية. وينبغي أن يتطرق إعداد هذه الخطة إلى إدارة المخاطر، فضلاً عن تصميم مخطط للأمن وتنفيذه. وينبغي من آن لآخر إعادة تقييم كل من الخطة وتنفيذها لقياس ما تحقق من تقدم وتحديد المجالات التي تحتاج إلى تحسينات في الخطة أو في تنفيذها. كما ينبغي أن تتضمن الخطة أحكاماً تتعلق بإدارة الحوادث، بما في ذلك الاستجابة والمراقبة والإنذار والانتعاش والصلات المتعلقة

[14] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf

[15] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf

بتقاسم المعلومات. كما ينبغي أن تعالج الخطة الأمنية الإجراءات التي طلبت في الفقرة **2.B.V** لتدريب مستخدمي هذه الأنظمة الحكومية والتعاون فيما بين الحكومة والقطاع الخاص والمجتمع المدني بشأن التدريبات والمبادرات الأمنية. وتعتبر توعية المستخدمين ومسؤوليتهم القضايا الرئيسية التي يتعين على التدريب أن يعالجها.

2.B.V تنفيذ برامج ومبادرات التوعية الأمنية لمستخدمي الأنظمة والشبكات الحكومية.

1) ينبغي لأي برنامج وطني فعال للتوعية بالأمن السيبراني أن يعزز من التوعية بالأمن السيبراني فيما بين عامة الجمهور والمجتمعات الرئيسية وداخل هذه المجتمعات، وإقامة روابط مع المتخصصين الحكوميين في مجال الأمن السيبراني من أجل تقاسم المعلومات بشأن مبادرات الأمن السيبراني، وتنمية التعاون وتعزيزه في مجال المسائل المتصلة بالأمن السيبراني. وهناك ثلاثة عناصر وظيفية يتعين النظر فيها لدى وضع برنامج للتوعية في هذا المجال: (1) توعية وإشراك أصحاب المصلحة مما يؤدي إلى بناء وتعزيز روابط تسودها الثقة فيما بين القطاع الخاص والحكومة والأوساط الأكاديمية من أجل زيادة الوعي بالأمن السيبراني وتحقيق الأمن الفعلي للفضاء السيبراني؛ (2) التنسيق الذي من شأنه أن يكفل التعاون بشأن الحوادث والأنشطة المتصلة بالأمن السيبراني بين مختلف القطاعات الحكومية؛ (3) تبادل الاتصالات والرسائل، مع التركيز على تنمية الاتصالات الداخلية (داخل الوكالة الحكومية المسؤولة عن هذا البرنامج)، والاتصالات الخارجية (الوكالات الحكومية الأخرى، ودوائر الصناعة، والمؤسسات التعليمية، ومستعملي الحواسيب المنزلية، وعامة الجمهور).

3.B.V التشجيع على إيجاد ثقافة للأمن داخل مؤسسات الأعمال التجارية.

1) يمكن إيجاد ثقافة للأمن داخل مؤسسات الأعمال التجارية عن طريق عدد من السبل المبتكرة. فقد وُجِّه الكثير من المبادرات الحكومية نحو استثارة الوعي لدى المنشآت التجارية الصغيرة والمتوسطة الحجم. ويمكن أن يساعد الحوار الحكومي، مع روابط دوائر الأعمال أو الشراكات بين القطاعين العام والخاص والناس، الإدارات على تصميم وتنفيذ مبادرات للتوعية والتدريب. ومن بين الأمثلة على هذه المبادرات: إتاحة المعلومات (على الخط مباشرةً وبطريقة غير مباشرة)، مثل الكتيبات والأدلة والكتيبات الإرشادية والسياسات النموذجية والمفاهيم؛ وإنشاء مواقع على شبكة الويب موجهة بصورة خاصة إلى المنشآت التجارية الصغيرة والمتوسطة الحجم وأصحاب المصلحة الآخرين؛ وتوفير التدريب (على الخط مباشرة)؛ وتوفير أدوات للتقييم الذاتي على الخط مباشرة؛ وعرض المساعدة المالية والدعم الضرائبي أو أي حوافز أخرى بغرض تعزيز إنتاج أنظمة مأمونة أو القيام بخطوات استباقية لتحسين الأمن السيبراني.

4.B.V دعم الخدمات الإرشادية التي تقدم للمجتمع المدني مع توجيه اهتمام خاص لاحتياجات الأطفال والشباب والأشخاص ذوي الاحتياجات الخاصة وفرادى المستعملين.

1) تعاونت بعض الحكومات مع قطاع الأعمال لاستثارة وعي المواطنين بالأخطار الناشئة والتدابير التي ينبغي استخدامها لمواجهتها. وتنظم بعض البلدان مناسبات محددة مثل يوم أو أسبوع أمن المعلومات مع تدابير مكررة لتعزيز أمن المعلومات لدى الجمهور العام. وتهدف معظم المبادرات إلى توعية الأطفال والشباب والأشخاص ذوي الاحتياجات الخاصة والطلاب سواء من خلال المدرسين أو الأساتذة أو الآباء أو من خلال التوزيع المباشر لمواد التوجيه. وتتباين مصادر المواد المعاونة المستخدمة، بدءاً من مواقع شبكة الويب أو الألعاب أو الأدوات على الخط مباشرة إلى البطاقات البريدية أو الكتب الدراسية أو منح الدبلومات مقابل اجتياز الامتحانات. ومن الأمثلة على هذه المبادرات تنظيم الدورات التدريبية للآباء لتزويدهم بالمعلومات عن المخاطر الأمنية؛ وتوفير المواد المعاونة للمدرسين؛ وتزويد الأطفال بأدوات للعب على الخط مباشرة أثناء تلقيهم الرسائل التعليمية ذات الصلة بأمن المعلومات؛ ووضع الكتب الدراسية والألعاب؛ وإجراء الامتحانات ومنح الدبلومات، وإعداد ألغاز للتعريف بكيفية التصفح الآمن على الويب.

2) وبوسع الحكومة والقطاع الخاص أن يتبادلا الدروس التي اكتسباها من وضع الخطط الأمنية وتدريب المستعملين، والتعلم من قصص النجاح والابتكارات التي حققها الآخرون؛ والعمل على تحسين أمن البنى التحتية المحلية للمعلومات.

5.B.V الترويج لبرنامج وطني شامل للتوعية حتى يتمكن جميع المشاركين – دوائر الأعمال واليد العاملة العامة والجمهور العام – من تأمين أدوارهم في الفضاء السيبراني.

1) يوجد الكثير من مواطن الضعف في أنظمة المعلومات نتيجة لنقص الوعي بالأمن السيبراني من جانب المستعملين ومديري الأنظمة وواضعي التكنولوجيات وموظفي التوريدات والمدققين وكبار موظفي المعلومات ومجالس المؤسسات. ويمكن أن تشكل مواطن الضعف هذه مخاطر جسيمة على الهياكل الأساسية حتى إذا لم تكن هذه جزءاً فعلياً من هذه الهياكل ذاتها.

وعلى سبيل المثال، فإن نقص الوعي الأمني لدى مديري الأنظمة كثيراً ما يشكل نقطة ضعف للخطة الأمنية للمؤسسة. ولذا فإن تعزيز جهود القطاع الخاص في تدريب الموظفين واعتماد شهادات أمنية مقبولة على نطاق واسع للموظفين سوف تساعد في الحد من مواطن الضعف هذه. ومن ناحية أخرى، فإن التنسيق الحكومي للأنشطة الوطنية للإرشاد والتوعية للتمكين من ثقافة الأمن سوف يبني أيضاً الثقة مع القطاع الخاص. فالأمن السيبراني عبارة عن مسؤولية مشتركة. ويمكن لإنشاء منافذ ومواقع على الويب أن يشكل آلية مفيدة لوضع برنامج وطني للتوعية لتمكين الوكالات الحكومية ودوائر الأعمال وفرادى المستهلكين من الحصول على المعلومات ذات الصلة والقيام بالتدابير التي تحمي الأجزاء الخاصة بهم في الفضاء السيبراني.

6.B.V تعزيز الأنشطة المعنية بالعلم والتكنولوجيا والبحث والتطوير.

1) بالقدر الذي تدعم به الحكومات العلم والتكنولوجيا والبحث والتطوير، يتعين توجيه بعض جهودها صوب أمن البنية التحتية للمعلومات. فبوسع البلدان أن تساعد، من خلال تحديدها أولويات البحوث والتطوير في المجال السيبراني، في تطوير المنتجات ذات الخواص الأمنية الذاتية، فضلاً عن معالجة التحديات التقنية الصعبة. وبالقدر الذي يتم به الاضطلاع بأنشطة البحث والتطوير في المؤسسات الأكاديمية، قد تتاح الفرص لإشراك الطلاب في مبادرات الأمن السيبراني.

7.B.V استعراض نظام الخصوصية السائد وتحديثه ليلائم بيئة الخط المباشر.

1) ينبغي أن ينظر هذا الاستعراض في آليات الخصوصية التي اعتمدتها مختلف البلدان والمنظمات الدولية، مثل منظمة التعاون والتنمية في الميدان الاقتصادي. وما زالت الخطوط التوجيهية التي وضعتها هذه المنظمة بشأن حماية الخصوصية وتدفق البيانات الشخصية عبر الحدود، وهي الخطوط التي اعتمدت في 23 سبتمبر 1980، تمثل توافقاً دولياً في الآراء بشأن التوجيه العام المتعلق بجمع وإدارة المعلومات الشخصية. وتضطلع هذه الخطوط التوجيهية، بما وضعته من مبادئ أساسية، بدور رئيسي في مساعدة الحكومات ودوائر الأعمال وممثلي المستهلكين في جهودهم لحماية الخصوصية والبيانات الشخصية وفي إلغاء القيود غير الضرورية على تدفق البيانات عبر الحدود سواء على الخط مباشرة أو بصورة غير مباشرة.

8.B.V تنمية الوعي بالمخاطر السيبرانية والحلول المتاحة.

1) يقتضي تناول القضايا التقنية تكاتف الحكومات والأعمال التجارية والمجتمع المدني وفرادى المستعملين في العمل معاً لوضع وتنفيذ التدابير التي تدمج بين عنصر *العملية (التكنولوجية)* (أي المعايير) (مثل المبادئ التوجيهية الاختيارية أو اللوائح الإلزامية)، وعنصر *الأفراد* (أي أفضل الممارسات).

2) وأحد الأمثلة على المخاطر السيبرانية الرسائل الاقتحامية وما يرتبط بها من مخاطر مثل البرمجيات الضارة. وهناك عدد من المنظمات، بما فيها لجنة الدراسات 17 لقطاع تقييس الاتصالات المسؤولة عن المسألة 17، تعمل جنباً إلى جنب في مجال القضايا المتعلقة بالرسائل الاقتحامية. انظر الملحق A الذي يقدم لمحة شاملة رفيعة المستوى بشأن هذه القضية.

3) وإدارة الهوية هي أحد الأمثلة على وجود أداة تكنولوجية لمعالجة مختلف احتياجات الأمن السيبراني. وهناك عدد من المنظمات، بما في ذلك لجنة الدراسات 17 لقطاع تقييس الاتصالات، تعمل جنباً إلى جنب في مجال إدارة الهوية. ويقدم الملحق B رؤية شاملة رفيعة المستوى بشأن هذه القضية.

التذييـــل 1

قائمة بالمختصرات

APECTEL فريق العمل المعني بالاتصالات والمعلومات التابع للجماعة الاقتصادية لبلدان آسيا والمحيط الهادئ (*Asia-Pacific Economic CooperationTelecommunications and Information Working Group*)

CAN-SPAM قانون مكافحة الصور الفاحشة والتسويق غير المطلوب لعام 2003 (الولايات المتحدة الأمريكية) (*Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (USA)*)

CCIPS القسم المتعلق بالجرائم الحاسوبية والملكية الفكرية (من وزارة العدل في الولايات المتحدة الأمريكية) (*Computer Crime and Intellectual Property Section (of US Dept of Justice)*)

CERT فريق الاستجابة لحالات الطوارئ الحاسوبية

(Computer Emergency Response Team)

CERT-CC مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية (جامعة كارنيغي ميلون في الولايات المتحدة الأمريكية) (*Computer Emergency Response Team Coordination Center (of Carnegie- Mellon University, USA)*)

CII البنية التحتية الحيوية للمعلومات (*Critical Information Infrastructure*)

CIIP حماية البنية التحتية الحيوية للمعلومات (*Critical Information Infrastructure Protection*)

CIRT فريق الاستجابة للحوادث الحاسوبية (*Computer Incident Response Team*)

COE مجلس أوروبا (*Council of Europe*)

CPNI مركز حماية البنية التحتية الوطنية (المملكة المتحدة) (*Centre for the Protection of National Infrastructure (UK)*)

CSIRT فرقة الاستجابة لحوادث الأمن الحاسوبي (*Computer Security Incident Response Team*)

CVE قائمة مشتركة لمواطن الضعف والتعرض (الولايات المتحدة الأمريكية) (*Common Vulnerabilities and Exposures List (USA)*)

DHS وزارة الأمن الداخلي (الولايات المتحدة الأمريكية) (*Department of Homeland Security (USA)*)

DOJ وزارة العدل (الولايات المتحدة الأمريكية) (*Department of Justice (USA)*)

EU الاتحاد الأوروبي (*European Union*)

FAR لوائح الاقتناء الاتحادية (الولايات المتحدة الأمريكية) (*Federal Acquisition Regulations (USA)*)

FCC لجنة الاتصالات الاتحادية (الولايات المتحدة الأمريكية) (*Federal Communications Commission (USA)*)

FIRST منتدى فرق أمن الاستجابة للحوادث (*Forum of Incident Response Security Teams*)

G8 مجموعة الدول الصناعية الثمانية (*Group of Eight (Nations)*)

ICT تكنولوجيا المعلومات والاتصالات (*Information & Communication Technologies*)

IMPACT الشراكة الدولية متعددة الأطراف لمواجهة التهديدات السيبرانية

(*International Multilateral Partnership Against Cyber Threats*)

ISAC مراكز تقاسم المعلومات وتحليلها (وهي مراكز مختلفة مثل مركز تقاسم معلومات تكنولوجيا المعلومات وتحليلها في الولايات المتحدة الأمريكية) (*Information Sharing and Analysis Centers (various, such as IT-ISAC; USA)*)

IT-ISAC مركز تقاسم معلومات تكنولوجيا المعلومات وتحليلها (*Information Technology Information Sharing and Analysis Center)*)

ITAA	رابطة تكنولوجيا المعلومات في أمريكا (*Information Technology Association of America*)
LAP	خطة عمل لندن (*London Action Plan*)
MSCM	خدمة الرسائل التجارية في الهواتف المحمولة (*Mobile Service Commercial Message*)
NIAC	المجلس الوطني لضمان المعلومات (التابع لرابطة تكنولوجيا المعلومات في أمريكا) (*National Information Assurance Council (of ITAA)*)
NIATEC	المركز الوطني للتدريب والتعليم في مجال ضمان نوعية المعلومات (في جامعة إيداهو في الولايات المتحدة الأمريكية) (*National Information Assurance Training and Education Center (at (USA) University of Idaho*)
NIST	المعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة الأمريكية) (*National Institute of Standards and Technology (USA)*)
NRIC	مجلس شبكة الموثوقية والتشغيل البيني (لجنة الاتصالات الاتحادية، الولايات المتحدة الأمريكية) (*Network Reliability and Interoperability Council (FCC USA)*)
NSTAC	اللجنة الوطنية الاستشارية للأمن والاتصالات (وزارة الأمن الداخلي، الولايات المتحدة الأمريكية) (*National Security and Telecommunications Advisory Committee (DHS USA)*)
NVD	قاعدة البيانات الوطنية بشأن مواطن الضعف (الولايات المتحدة الأمريكية) (*National Vulnerability Database (USA)*)
OECD	منظمة التعاون والتنمية في الميدان الاقتصادي (*Organisation for Economic Co-operation and Development*)
OVAL	لغة التقييم المفتوحة لمواطن الضعف (*Open Vulnerability Assessment Language*)
PSTN	الشبكة الهاتفية العمومية التبديلية (*Public Switched Telecommunication Network*)
R&D	البحث والتطوير (*Research and Development*)
S&T	العلم والتكنولوجيا (*Science and Technology*)
SME	المنشآت التجارية الصغيرة والمتوسطة (*Small and medium-sized enterprise*)
SMS	خدمة الرسائل القصيرة (*Short Message Service*)
SOP	إجراءات التشغيل المعيارية (*Standard Operating Procedures*)
TCPA	قانون حماية مستهلكي الهاتف (الولايات المتحدة الأمريكية) (*Telephone Consumer Protection Act (USA)*)
UNGA	الجمعية العامة للأمم المتحدة (*United Nations General Assembly*)

التذييـــل 2

استراتيجية تنفيذ التعاون في مجال الأمن السيبراني وتدابير الفعالية

يستخدم النهج المبين أدناه منهجية برامج صممت للانتقال بالبلدان قدماً نحو وضع أنظمة قوية للأمن السيبراني كأولوية وطنية. وتنقسم هذه المنهجية إلى ثلاث مراحل برامجية متميزة تنقل البلد من مرحلة التقييم الأولي للقدرات إلى تنفيذ برنامج وتقييمه. وفيما يلي عرض لهذا النهج المقسم إلى مراحل:

استراتيجية التنفيذ للتعاون من أجل تحقيق الأمن السيبراني وتدابير الفعالية

المرحلة 1 – تقدير وتقييم خطة لبرنامج لتبادل التعاون والتوصية بها.

- **التقدير:** الخطوة الأولى تتمثل في قيام البلد بإجراء تقدير للحالة الراهنة لبرنامج الأمن فيها. ويتم ذلك من خلال فرقة من الخبراء تستخدم أداة تقييم موحدة.
- **التقييم:** توفر المعلومات التي يتم جمعها خلال مرحلة التقدير فهماً لجوانب القوة ومواطن الضعف في برنامج الأمن السيبراني الحالي في البلد ويحدد المجالات التي ينبغي أن تتركز عليها الجهود.
- **التوصية:** يوفر الفهم المكتسب من عملية التقييم الأساس لوضع خطة لتلبية احتياجات البلد.

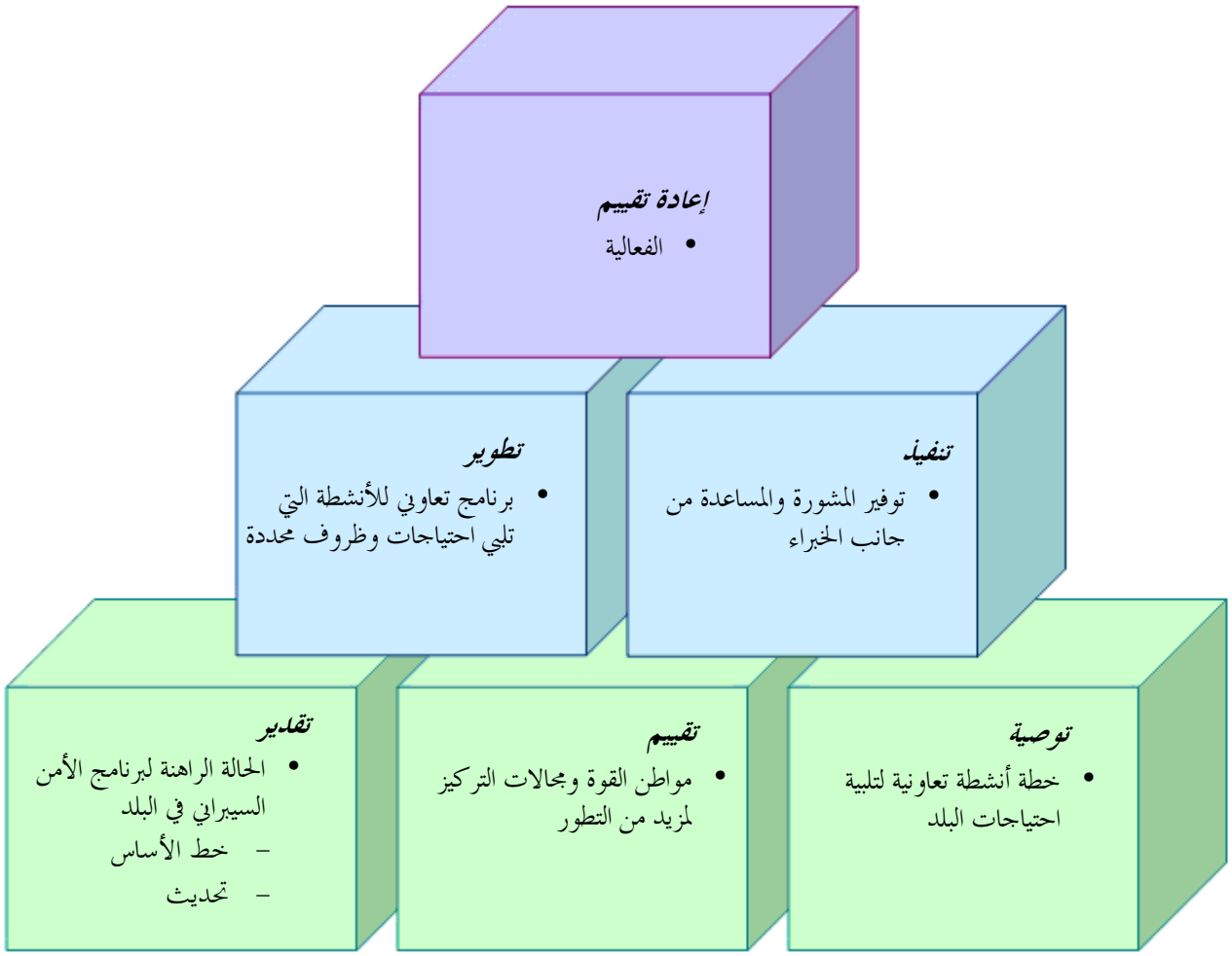
المرحلة 2 – وضع وتنفيذ برنامج تعاوني.

- **وضع البرنامج التعاوني:** يجتمع الخبراء القطريون سواءً داخلياً أو مع نظرائهم الدوليين لتصميم وتشكيل ومواءمة الأنشطة اللازمة للوفاء بالاحتياجات الفريدة والظروف السائدة في البلد المعين. ويمكن أن تشتمل الأنشطة على طائفة من أنشطة التبادل والتعاون وتحديد المتطلبات المادية الطويلة الأجل.
- **تنفيذ البرنامج:** يقوم الخبراء المحليون وربما الدوليون بتنفيذ البرنامج وتقديم المشورة العملية.

المرحلة 3 – تقييم البرنامج التعاوني لقياس النجاح واستكمال البرنامج.

- **البرنامج التعاوني الخاضع للتقييم:** يجري من آن لآخر إعادة تقييم البرنامج التعاوني للأمن السيبراني للتأكد من فاعليته داخلياً أو مع النظراء القطريين. وقد تصبح المجالات التي يرى أنها تعاني من قصور موضوعاً لمزيد من المبادلات التعاونية وبدء العملية السابقة من جديد. وإذا كان البلد يتعاون مع بلدان أخرى، يمكن إنهاء هذا التعاون بمجرد تقييم برنامج البلد بأنه فعال.

الشكل 1: منهجية برنامج لبناء القدرة في مجال الأمن السيبراني



تدابير الفعالية

فيما يلي أسلوب لقياس الأداء بمرور الوقت في هذا المجال وعرض التقدم المحرز على كبار المسؤولين. ويتركز هذا النهج على سلسلة من الأسس المنطقية التي تربط المدخلات الأساسية (البرامج الخاصة ببلد و/أو منطقة التي تستهلك الوقت والمال وموارد الموظفين) بالنتيجة المنشودة بنهاية المطاف (زيادة الأمن السيبراني). وتبين هذه السلسلة في الجدول الوارد أدناه:

فئة التدابير:	**عناصر الأداء:**
المدخلات الأساسية:	**البرامج القطرية:** • الوقت • المال • الموظفون
عمليات العمل الأساسية:	**العمل بما في ذلك المبادلات التعاونية المحتملة في:** • وضع الاستراتيجية الوطنية • وضع الأسس القانونية والتنظيمية • إدارة الحوادث • الشراكات بين الحكومة والصناعة • ثقافة الأمن السيبراني

المخرجات الأساسية: **عدد من:**

- الاجتماعات أو المبادلات التعاونية
- الاتصالات مع كبار المسؤولين عن السياسات والنواحي التقنية

النتائج الوسيطة: **الإجراءات القطرية:**

- القوانين واللوائح الجديدة المعنية بالجرائم السيبرانية
- إجراءات الإنفاذ
- إنشاء وحدات الاستجابة لحوادث الأمن الحاسوبي (CSIRT)
- برامج التوعية المشتركة بين الحكومة والصناعة
- استفسارات الاستجابة للحوادث
- المشاركة في أنشطة الأمن السيبراني في المنظمات الدولية
- الانضمام إلى الاتفاقيات والخطوط التوجيهية الدولية

نتيجة التقييم: انخفاض مخاطر الأمن السيبراني نتيجة لوضع استراتيجية وطنية وقوانين ولوائح لمواجهة الجرائم السيبرانية وخطوط توجيهية طوعية والنهوض بالتوعية الذاتية للمستهلكين.

النتيجة النهائية: زيادة الأمن السيبراني المحلي والأمن العالمي.

الملحق ألف

لجنة الدراسات: رسائل اقتحامية (Spam)

الاتحـــــــاد الدولـــــــي للاتصـــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X

الإضافة 6
(2009/09)

السلسلة X: شبكات البيانات والاتصالات
بين الأنظمة المفتوحة ومسائل الأمن

سلسلة التوصية ITU-T X.1240 – إضافة بشأن مكافحة الرسائل الاقتحامية وما يتصل بها من تهديدات

تحذيـــر

تمهيد لنشر توصيـــة

هذا المنشور صيغة غير محررة لتوصية معتمدة مؤخراً. وسيجري الاستعاضة عنها بصيغة منشورة ما أن يتم تحريرها، ولذلك، ستكون هناك اختلافات بين المنشور التمهيدي والصيغة المنشورة.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه المنشورة لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه المنشورة اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه المنشورة حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه المنشورة إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه المنشورة أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد المنشور.

وعند الموافقة على هذه المنشورة، [كان/لم يكن] الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه المنشورة. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه المنشورة بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

الإضافة 6 إلى سلسلة التوصيات X لقطاع تقييس الاتصالات

سلسلة التوصيـــة ITU-T X.1240 – إضافة بشأن مكافحة الرسائل الاقتحامية وما يتصل بها من تهديدات

ملخص

تشير الإضافة 6 لسلسلة التوصيات X لقطاع تقييس الاتصالات إلى أنه للتصدي بفعالية للرسائل الاقتحامية تحتاج الحكومات إلى استخدام مجموعة متنوعة من النهج، بما في ذلك قوانين فعالة، وأدوات تكنولوجية، وتثقيف المستهلك ودوائر الأعمال. وتستعرض هذه الإضافة المحافل الدولية التي يجري في إطارها تناول مسألة الرسائل الاقتحامية. وهي توفر باعتبارها دراسة حالة، لأغراض التوضيح، بعض المعلومات بشأن الأساليب التي اتبعتها الولايات المتحدة الأمريكية واليابان في تناول مشكلة الرسائل الاقتحامية.

المصدر

وافقت لجنة الدراسات 17 بقطاع تقييس الاتصالات (2009-2012) على الإضافة 6 لسلسلة التوصيات X لقطاع تقييس الاتصالات بتاريخ 25 سبتمبر 2009.

المحتـــويات

1 مجال التطبيق

2 المراجع

3 التعاريف

4 المختصرات والأسماء المختصرة

5 الاصطلاحات

6 معلومات أساسية

7 النهج الوطنية في التصدي بفعالية للرسائل الاقتحامية وما يتصل بها من تهديدات

8 المبادرات الدولية (المتعددة الأطراف والثنائية) فيما يتعلق بالرسائل الاقتحامية

9 دراسة حالة لبعض أنشطة مكافحة الرسائل الاقتحامية

1.9 الولايات المتحدة الأمريكية

1.1.9 قانون إرساء اشتراطات لمن يرسلون البريد الإلكتروني التجاري (CAN-SPAM Act)

2.1.9 قواعد حظر إرسال البريد الإلكتروني التجاري على الأجهزة اللاسلكية

3.1.9 نُهُج للحد من التصيد الاحتيالي على الإنترنت

2.9 اليابان

1.2.9 إنفاذ القانون

2.2.9 مجلس النهوض بتدابير مكافحة الرسائل الاقتحامية

3.2.9 مركز التنظيف السيبراني (CCC)

4.2.9 سد البوابة 25 خارج الحدود (OP25B)

5.2.9 تكنولوجيات استيقان المرسل

6.2.9 تبادل معلومات مرسل الرسائل الاقتحامية بين مشغلي الاتصالات المتنقلة

ثبت المراجع

الإضافة 6 إلى سلسلة التوصيات X لقطاع تقييس الاتصالات

سلسلة التوصيـــة ITU-T X.1240 – إضافة بشأن مكافحة الرسائل الاقتحامية وما يتصل بها من تهديدات

1 مجال التطبيق

موضوع هذه الإضافة هو الرسائل الاقتحامية وما يتصل بها من تهديدات. والهدف من هذه الإضافة توفيرها للإدارات الوطنية التي تعتبر الرسائل الاقتحامية بمثابة مفهوم جديد بالنسبة لها وترغب في الحصول على بعض المعلومات بشأنها.

تنظر هذه الإضافة إلى الأدوات التي يتعين نشرها لمكافحة الرسائل الاقتحامية بطريقة فعالة ويصف بعض الأعمال التي تضطلع بها بعض المحافل الدولية في هذا المجال. وتقدم هذه الإضافة باعتبارها، دراسة حالة ولأغراض التوضيح، وصفاً لما تضطلع به الولايات المتحدة واليابان لمكافحة الرسائل الاقتحامية.

2 المراجـــع

لا يوجد.

3 التعاريف

تعرف هذه الإضافة المصطلحات التالية:

1.3 التصيد الاحتيالي – هو مجرد محاولة للاحتيال على شخص لكي يدخل إلى موقع الويب غير المقصود بغرض سرقة المعلومات الشخصية لهذا الشخص.

2.3 الرسالة الاقتحامية – ولئن كان لا يوجد تعريف معترف به على الصعيد العالمي للرسالة الاقتحامية، إلا أن المصطلح يستخدم بشكل عام لوصف معظم الاتصالات الإلكترونية غير المطلوبة عن طريق رسائل البريد الإلكتروني أو المراسلة عن طريق الهواتف المحمولة (خدمة الرسائل القصيرة (SMS)، المراسلة متعدد الوسائط (MMS)).

4 المختصرات والأسماء المختصرة

تستعمل هذه الإضافة المختصرات التالية:

ADSP ممارسات إرسال ميدان المؤلف *(Author Domain Sending Practices)*

APEC TEL فريق العمل المعني بالاتصالات والمعلومات التابع للجماعة الاقتصادية لبلدان آسيا والمحيط الهادئ (*Asia-Pacific Economic Community – Telecommunication & Information Working Group*)

CAN-SPAM قانون مكافحة الصور الفاحشة والتسويق غير المطلوب لعام 2003 (الولايات المتحدة الأمريكية) (*Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (U.S.)*)

CNSA شبكة الاتصال بسلطات مكافحة الرسائل الاقتحامية (الاتحاد الأوروبي) (*Contact Network of Spam Authorities (European Union)*)

DKIM رسالة التعرف على مفاتيح الميدان *(Domain Keys Identified Mail)*

FCC لجنة الاتصالات الاتحادية (الولايات المتحدة) (*Federal Communications Commission (U.S.)*)

FTC لجنة التجارة الاتحادية (الولايات المتحدة) (*Federal Trade Commission (U.S.)*)

ISP مورد خدمة إنترنت *(Internet Service Provider)*

JEAG فريق مكافحة إساءة استعمال البريد الإلكتروني في اليابان *(Japan Email Anti-abuse Group)*

LAP خطة عمل لنـــدن (*London Action Plan*)

MAAWG فرقة العمل المعنية بمكافحة إساءة استعمال المراسلة (*Messaging Anti-Abuse Working Group*)

MMS خدمة المراسلة متعددة الوسائط (*Multimedia Messaging Service*)

MSCM خدمة الرسائل التجارية في الهواتف المحمولة (*Mobile service commercial messages*)

OECD منظمة التعاون والتنمية في الميدان الاقتصادي
(*Organization for Economic Cooperation & Development*)

OP25B سد البوابة 25 خارج الحدود *(Outbound Port 25 Blocking)*

SMS خدمة الرسائل القصيرة (*Short Messaging Service*)

SPF إطار سياسات المرسل *(Sender Policy Framework)*

5 الاصطلاحات

لا يوجد.

6 معلومات أساسية

1.6 تحولت **الرسائل الاقتحامية** من كونها اتصالات مزعجة تتضمن إعلانات تجارية إلى تيسير لمشكلة أكثر خطورة للأمن السيبراني. وعلى سبيل المثال، يمكن أن تكون الرسائل الاقتحامية وسيلة للخداع، ونشر البرمجيات الخبيثة مثل الفيروسات وبرمجيات التجسس، وإغراء المستهلكين على تقديم معلومات سرية يمكن أن تستخدم في وقت لاحق في ارتكاب عمليات انتحال الشخصية (أي التصيد الاحتيالي). ويمكن للمرسلين إرسال رسائلهم في أي مكان في العالم لأي شخص دون أن يكلفهم ذلك سوى تكلفة ضئيلة جداً. وهو ما يجعل الرسائل الاقتحامية مشكلة دولية لا بد من معالجتها من خلال التعاون الدولي.

2.6 يستفيد **التصيد الاحتيالي** من واقع أن أي شخص يمكن أن يرسل بريد إلكتروني إلى أي شخص دون أي شكل من أشكال الاستيقان تقريباً، ويعزى ذلك إلى الخصائص الأساسية التي يتميز بها نظام البريد الإلكتروني عبر الإنترنت[16]. والتصيد الاحتيالي هو محاولة للاحتيال على شخص لكي يدخل إلى موقع الويب غير المقصود بهدف سرقة المعلومات الشخصية لهذا الشخص. ويوجد التصيد الاحتيالي على نطاق واسع لأن الناس يتوقعون أحياناً تلقي بريد من موقع معروف وهم لا يدركون أن الرسالة التي تلقوها ليست من المصدر المشروع. ونظراً لعدم وجود سوى استيقان ضئيل في البريد الإلكتروني، فإن من الصعب تحديد ما إذا كانت الرسالة صحيحة دون الفحص الدقيق في البريد الإلكتروني. ويتطلب هذا الفحص الدقيق دراية كبيرة بالآليات المستخدمة على الشبكة الإلكترونية.

ويحدث هذا التصيد الاحتيالي أيضاً لأن معظم الناس يجدون صعوبة في التحقق مما إذا كانت المواقع التي يزورونها على شبكة الويب مشروعة. وأحياناً ما لا ندقق النظر في تفاصيل الوصلة الإلكترونية (URL) على صفحة الويب قبل إدخال معلومات حساسة، وأحياناً ما نجهل ما هي الوصلة الصحيحة للدخول إلى موقعها.

ومخدمات الويب المستعملة في "تصيد" المعلومات الحساسة تكون هي غالباً ضحية البرمجيات الضارة مما يضاعف من جديد من تقفي أثر المتصيدين.

3.6 **البرمجيات الخبيثة**، أو البرمجيات الضارة، تصفح أداة دون دراية مالكها ودون إذن منه، وهي مشكلة هائلة أيضاً.

---

[16] صمم نظام البريد الإلكتروني عبر الإنترنت في السبعينات حينما كانت الإنترنت مقتصرة على عدد ضئيل من الباحثين وأعضاء الحكومات. ولم تكن هناك حاجة إلى الاستيقان لتحديد هوية الأفراد الذين يرسلون البريد الإلكتروني، ولذلك لم تبذل أي جهود لوضع نظام يستطيع القيام بذلك. وإن كان نظام البريد الإلكتروني قد تطور منذ ذلك الحين، إلا أن الإغفال الأساسي لا يزال قائماً.

7 النهج الوطنية في التصدي بفعالية للرسائل الاقتحامية وما يتصل بها من تهديدات

1.7 الاستراتيجية الوطنية والرسائل الاقتحامية: يتعين على البلدان فيما يتعلق بالاستراتيجية الوطنية وضع توليفة من القوانين الفعالة وسلطات إنفاذ القوانين وأدوات تكنولوجية وأفضل الممارسات وتوعية المستهلكين ودوائر الأعمال بطريقة التعامل الفعال مع الرسائل الاقتحامية.

2.7 الأساس القانوني والتنظيمي والرسائل الاقتحامية: فيما يتعلق بالأساس القانوني والإطار التنظيمي، يتعين أن يكون للسلطات المختصة بالمسائل المتعلقة بالرسائل الاقتحامية السلطة اللازمة للتحقيق واتخاذ الإجراءات ضد مخالفات القوانين ذات الصلة بالرسائل الاقتحامية التي ترتكب من بلدها أو تتسبب في تأثيرات في بلدها. كما يتعين أن يكون لدى السلطات المختصة بالنظر في المسائل المتعلقة بالرسائل الاقتحامية الآليات اللازمة للتعاون مع السلطات الأجنبية. وينبغي ترتيب أولويات طلبات المساعدة من السلطات الأجنبية استناداً إلى مجالات المصلحة المشتركة وفي الحالات التي تحدث فيها أضرار بالغة.

3.7 التعاون بين الحكومة والصناعة وتعزيز التوعية الوطنية بقضايا الرسائل الاقتحامية: يتعين أن يتعاون جميع الأشخاص المعنيين، بما في ذلك سلطات الإنفاذ ودوائر الأعمال ومجموعات المستهلكين في تتبع مخالفات القوانين ذات الصلة بالرسائل الاقتحامية. ويتعين أن تشترك وكالات الإنفاذ الحكومية مع الصناعة ومجموعات المستهلكين في توعية المستهلكين وتعزيز عملية تقاسم المعلومات. ويتعين على وكالات الإنفاذ الحكومية أن تتعاون مع القطاع الخاص لتعزيز عملية استحداث أدوات تكنولوجية لمكافحة الرسائل الاقتحامية، بما في ذلك تحديد مواقع مرسلي هذه الرسائل والتعرف على شخصيتهم.

والتصيد الاحتيالي (phishing) جريمة يمكن توقّيها في أحيان كثيرة. وينبغي أن تعمل مع القطاع الخاص لتحسين سبل حماية المواطنين من التصيد الاحتيالي، وتوعية المستهلكين والأعمال التجارية بطرق الاستيقان المأمونة.

وتستطيع الحكومات أيضاً أداء دور في تثقيف الجمهور بشأن الحاجة إلى التحقق من البرمجيات الخبيثة وذلك عن طريق استخدام أدوات مثل برمجيات مكافحة الفيروسات وذلك بتطبيق أحدث مجموعات نظام التشغيل وتقنيات الحوسبة الموثوقة.

8 المبادرات الدولية (المتعددة الأطراف والثنائية) فيما يتعلق بالرسائل الاقتحامية

هناك العديد من المنتديات المتعددة الأطراف والثنائية التي يتم في إطارها اتخاذ مبادرات لمكافحة الرسائل الاقتحامية:

1.8 خطة عمل لندن

استضافت لجنة التجارة الاتحادية ومكتب التجارة النزيهة في المملكة المتحدة مؤتمراً دولياً بشأن الإنفاذ فيما يتعلق بالرسائل الاقتحامية في لندن عام 2004. وقد أدى هذا المؤتمر إلى وضع خطة عمل لندن بشأن التعاون الدولي في الإنفاذ ذي الصلة بالرسائل الاقتحامية. وقد صدق على الخطة، حتى يوليو 2008 وكالات حكومية وممثلين عن القطاع الخاص من أكثر من 25 بلداً. وتشجع خطة عمل لندن الأطراف المعنية، بما في ذلك وكالات الإنفاذ الخاصة بالرسائل الاقتحامية وأصحاب المصلحة من القطاع الخاص على بحث الانضمام لعضوية المنظمة.

والغرض من خطة عمل لندن هو تعزيز التعاون الدولي في مجال الإنفاذ بشأن الرسائل الاقتحامية ومعالجة المشاكل ذات الصلة بهذه الرسائل مثل الاحتيال والخداع على الخط مباشرة وعمليات الاحتيال ونشر الفيروسات. وتقيم خطة عمل لندن علاقات بين هذه الكيانات استناداً إلى وثيقة قصيرة تحدد خطة عمل أساسية بشأن التعاون الدولي في مجال الإنفاذ والتوعية ضد الرسائل الاقتحامية غير المشروعة. وهذه الوثيقة ليست ملزمة حيث لا تتطلب من المشتركين إلا بذل أفضل الجهود لإحراز تقدم في تنفيذ خطة العمل. http://londonactionplan.org/.

ومنذ بداياتها، تقوم خطة عمل لندن (LAP) بعقد ورش عمل سنوية، عادة بالترافق مع شبكة اتصال الاتحاد الأوروبي لسلطات الرسائل الاقتحامية (CNSA). وفي أكتوبر 2007، جمعت خطة عمل لندن وشبكة اتصال الاتحاد الأوروبي لسلطات الرسائل الاقتحامية حلقة العمل المشتركة لهما مع مؤتمر فريق العمل المعني بمكافحة إساءة استعمال المراسلة في آرلنغتون، فرجينيا، والتي أدت إلى تسهيل التعاون في إنفاذ القوانين مع القطاع الخاص. وفي أكتوبر 2008، جمعت كل من LAP وCNSA ورشة العمل المشتركة لهما مع القمة الألمانية الاقتصادية السادسة لمكافحة الرسائل الاقتحامية في فيسبادن بألمانيا.

2.8 مجموعة أدوات منظمة التنمية والتعاون في الميدان الاقتصادي لمكافحة الرسائل الاقتحامية، وتوصية المجلس بشأن التعاون في الإنفاذ المضاد للرسائل الاقتحامية

أصدر فريق المهام المعني بالرسائل الاقتحامية في منظمة التعاون والتنمية في الميدان الاقتصادي في أبريل 2006 "مجموعة أدوات" لمكافحة الرسائل الاقتحامية تتضمن توصيات لمساعدة صانعي السياسات والمنظمين والعناصر الفاعلة من الصناعة في توجيه سياساتهم المتعلقة بالحلول التي تستخدم في مكافحة الرسائل الاقتحامية واستعادة الثقة في الإنترنت والبريد الإلكتروني. وتتضمن مجموعة الأدوات ثمانية عناصر تشمل لائحة مكافحة الرسائل الاقتحامية، والحلول الموجهة للصناعة، وتكنولوجيات مكافحة الرسائل الاقتحامية، والتعليم والتوعية والتعاون والإرشاد على المستوى العالمي. وإدراكاً من الحكومات الأعضاء في منظمة التعاون والتنمية في الميدان الاقتصادي بأن التعاون الدولي هو عنصر رئيسي في مكافحة الرسائل الاقتحامية، وافقت أيضاً على "توصية بشأن التعاون عبر الحدود في إنفاذ قوانين مكافحة الرسائل الاقتحامية"، وهي التوصية التي تحث البلدان على أن تضمن أن تمكن قوانينها سلطات الإنفاذ من تقاسم المعلومات مع البلدان الأخرى وأن تفعل ذلك بسرعة وفعالية. http://www.oecd-antispam.org/sommaire.php3.

3.8 الندوة الدراسية التي عقدها فريق العمل المعني بالاتصالات والمعلومات التابع للتعاون الاقتصادي لبلدان آسيا والمحيط الهادئ بشأن الرسائل الاقتحامية

عقد هذا الفريق في أبريل 2006 ندوة دراسية بشأن "الرسائل الاقتحامية وما يتصل بها من أخطار" جمعت معاً 30 متحدثاً وعضواً في الأفرقة المتخصصة لمناقشة تطور مشكلة الرسائل الاقتحامية ووضع جدول أعمال مشترك لفريق العمل المعني بالاتصالات والمعلومات. وتضمنت المواضيع الرئيسية التي تمت مناقشتها:

1) وضع وتطبيق أنظمة وطنية تنظيمية لمكافحة الرسائل الاقتحامية بما في ذلك الإنفاذ ومدونات السلوك؛

2) دور الصناعة في مكافحة الرسائل الاقتحامية بما في ذلك الشراكات بين القطاعين العام والخاص؛

3) ردود الفعل التقنية إزاء رسائل اقتحامية؛

4) التعاون والإنفاذ عبر الحدود بما في ذلك اتفاقية مجلس أوروبا المعنية بالجرائم السيبرانية وتوصية مجلس منظمة التعاون والتنمية في الميدان الاقتصادي بشأن التعاون في الإنفاذ بوصفها أدوات رئيسية لتعزيز التعاون؛

5) الحاجة إلى التوعية واستثارة الوعي الموجهة لمصادر الرسائل.

وتتضمن الخطوات العملية التي وافق فريق العمل المعني بالاتصالات والمعلومات على اتخاذها لتحقيق تقدم:

1) التشجيع على تقاسم المعلومات بشأن اللوائح والسياسات بالاعتماد على بعض الموارد مثل مجموعة أدوات مكافحة الرسائل الاقتحامية في منظمة التعاون والتنمية في الميدان الاقتصادي؛

2) وضع قائمة مراسلات لسلطات مكافحة الرسائل الاقتحامية في التعاون الاقتصادي لبلدان آسيا والمحيط الهادئ لإضافة المواد المماثلة التي وضعتها منظمة التنمية والتعاون في الميدان الاقتصادي والاتحاد الدولي للاتصالات؛

3) تشجيع الاقتصاديات على الانضمام إلى منتديات التعاون الطوعي مثل خطة عمل لندن أو اتفاق سول - ملبورن؛

4) التعاون مع منظمة التنمية والتعاون في الميدان الاقتصادي بشأن تقاسم المعلومات والمبادرات المتعلقة بالتوجيه؛

5) دعم بناء القدرات في الاقتصادات النامية للنهوض بعملية التعامل مع الرسائل الاقتحامية.

9 دراسة حالة لبعض أنشطة مكافحة الرسائل الاقتحامية

تعرض هذه الفقرة أنشطة مكافحة الرسائل الاقتحامية في بعض البلدان

1.9 الولايات المتحدة الأمريكية

1.1.9 قانون إرساء اشتراطات لمن يرسلون البريد الإلكتروني التجاري (CAN-SPAM Act)

سنت الولايات المتحدة قانون مكافحة الهجوم بالصور الفاحشة والتسويق غير المطلوب لعام 2003 ("CAN-SPAM Act")، وهو القانون الذي يحدد الشروط لأولئك الذين يقومون بإرسال رسائل تجارية بالبريد الإلكتروني، ويحدد العقوبات ضد القائمين بإرسال

الرسائل الاقتحامية والشركات التي يتم الإعلان عن منتجاتها إذا قامت بمخالفة القانون، ويعطي المستهلكين الحق في أن يطلبوا من راسلي الرسائل بالبريد الإلكتروني التوقف عن إرسال رسائل اقتحامية إليهم.

وتشمل الأحكام الرئيسية لهذا القانون ما يلي:

- **يفرض حظراً على المعلومات المزيفة أو المضللة التي ترد في عناوين الرسائل**. فلا بد أن تكون معلومات "من" و"إلى" في بريدك الإلكتروني ومعلومات التسيير الأخرى – بما في ذلك اسم المصدر وعنوان البريد الإلكتروني – تتسم بالدقة وتحدد الشخص مصدر رسالة البريد الإلكتروني.
- **يفرض حظراً على رؤوس الموضوعات المضللة**. يتعين ألا يؤدي رأس الموضوع إلى تضليل المستقبِل بشأن محتويات الرسالة أو موضوعها.
- **يتطلب أن يتيح بريدك الإلكتروني للمستقبل طريقة اختيار الخروج**. يتعين أن توفر عنواناً للرد على البريد الإلكتروني أو آلية رد أخرى تعتمد على الإنترنت تتيح للمستقبل أن يطلب منك عدم إرسال رسائل بالبريد الإلكتروني في المستقبل لذلك العنوان وعليك أن تحقق هذه الطلبات. ويمكن أن تستحدث "قائمة" من الاختيارات تتيح للمستقبل أن يختار الخروج من بعض أنماط الرسائل، إلا أن عليك أن تتضمن خياراً بإنهاء أي رسائل تجارية من الراسل. ويتعين أن تتمكن أية آلية لاختيار الخروج من تجهيز طلبات اختيار الخروج لمدة 30 يوماً على الأقل بعد إرسال بريدك الإلكتروني التجاري. وعندما تتلقى طلب اختيار الخروج، يمنحك الخروج فترة 10 أيام عمل لوقف إرسال البريد الإلكتروني إلى عنوان الطالب. ولا يمكنك مساعدة كائن آخر على إرسال بريد إلكتروني إلى ذلك العنوان أو أن تكلف كياناً آخر بإرسال بريد إلكتروني بالنيابة عنك إلى ذلك العنوان. وأخيراً فإن من غير القانوني أن تقوم ببيع أو إرسال عناوين البريد الإلكتروني الخاصة بالأشخاص الذين اختاروا عدم تلقي بريدك الإلكتروني حتى في شكل قائمة مراسلات ما لم يكن تحويلك للعنوان راجعاً إلى تمكين كيان آخر من الامتثال للقانون.
- **يتطلب القانون تحديد البريد الإلكتروني التجاري بأنه إعلان، ويتضمن العنوان البريدي المادي الصحيح للراسل**. يتعين أن تتضمن رسالتك إشارة واضحة وبارزة على أن هذه الرسالة إعلان أو طلب وأن بوسع المستقبل أن يختار عدم استقبال رسائل تجارية أخرى بالبريد الإلكتروني منك. ويتعين أن تتضمن الرسالة عنوانك البريدي المادي الصحيح.

تخوَّل لجنة التجارة الاتحادية (FTC) باستعمال السلطة التي لديها في إنفاذ القانون المدني لإنفاذ قانون هجوم الصور الفاحشة والرسائل الاقتحامية (CAN-SPAM) وتحصيل عقوبات مدنية تصل إلى 11 000 دولار أمريكي عن كل مخالفة. ومنذ عام 1997، عندما قامت لجنة التجارة الاتحادية باتخاذ أول إجراء إنفاذ استهدفت به بريداً إلكترونياً لا يطلبه المتلقّي أو "رسائل اقتحامية"، لاحقت اللجنة بنشاط ممارسات مضللة وغير أمينة للرسائل الاقتحامية من خلال إجراءات إنفاذ بلغت 94 إجراءً، كان من بينها 31 إجراءً استهدفت به مخالفين للقانون CAN-SPAM.

ويخوِّل القانون CAN-SPAM وزارة العدل (DOJ) سلطة إنفاذ عقوباته الجنائية. وينص قانون مكافحة هجوم الصور الفاحشة والتسويق غير المطلوب لعام 2003 في الولايات المتحدة الأمريكية على عقوبات جنائية جسيمة، تشمل قضاء وقت في السجن لمرسلي الرسائل الاقتحامية. ويمكن لوكالات اتحادية أو تابعة للولايات أن تقوم بإنفاذ القانون ضد المنظمات التي تقع تحت ولايتها، ويجوز للشركات التي توفر النفاذ إلى الإنترنت أن تقاضي المخالفين كذلك.

2.1.9 قواعد حظر إرسال البريد الإلكتروني التجاري على الأجهزة اللاسلكية

وقد اعتمدت الولايات المتحدة كذلك قواعد لحماية المستهلكين من تلقي الرسائل التجارية غير المطلوبة (الرسائل الاقتحامية) على أجهزتهم اللاسلكية. وتحظر القواعد، مع بعض الاستثناءات، إرسال الرسائل التجارية بالبريد الإلكتروني، بما في ذلك رسائل البريد الإلكتروني وبعض الرسائل النصية إلى الأجهزة اللاسلكية مثل الهواتف الخلوية التي توفر خدمات الإذاعة المحمولة التجارية. ولا تسري هذه القواعد إلا على الرسائل التي تستوفي تعريف "التجارية" المستخدمة في قانون مكافحة هجوم الصور الفاحشة والتسويق غير المطلوب لعام 2003 – وعلى تلك الرسائل التي الغرض الرئيسي منها هو الإعلان أو الترويج التجاري لمنتج أو سلعة تجارية أو خدمة. ولا تخضع لهذه القواعد الرسائل غير التجارية مثل الرسائل عن المرشحين لمناصب عامة أو الرسائل التي تبلغ أحد العملاء بتحديث حسابه أوحسابها.

ويحظر استخدام رسائل خدمة الرسائل القصيرة ما لم يكن الذي توجه إليه الرسائل قد أعطى المرسل تفويضاً مسبقاً (معروف بأنه شرط الاختيار بالقبول). وتحظر هذه القواعد إرسال أية رسائل تجارية إلى العناوين التي تتضمن أسماء مجالات تكون قد أدرجت في

قائمة لجنة الاتصالات الاتحادية وذلك لمدة 30 يوماً على الأقل أو أي وقت قبل 30 يوماً إذا كان الراسل يعرف بدلا من ذلك أن الرسالة موجهة إلى جهاز لا سلكي. ولمساعدة مرسلي الرسائل التجارية على تحديد العناوين الخاصة بالمشتركين في الأجهزة اللاسلكية، تتطلب هذه القواعد أن يتولى موردو الخدمات اللاسلكية تزويد لجنة الاتصالات الاتحادية بأسماء المجال البريدي ذات الصلة. ويمكن أن تتضمن الرسائل التجارية لخدمات الهاتف المحمول أية رسائل تجارية يتم إرسالها إلى عنوان على البريد الإلكتروني يقدمه مورد خدمة الهاتف المحمول للتسليم لجهاز المشترك اللاسلكي. ولا تخضع رسائل خدمة الرسائل القصيرة التي يتم إرسالها فقط إلى أرقام الهاتف لهذه الحماية إلا أن النداءات الذاتية المراقبة يغطيها بالفعل قانون حماية مستهلكي الهاتف.

ووفقاً لقواعد لجنة الاتصالات الاتحادية، يجوز للجنة أن تفرض غرامات نقدية على مرسلي الرسائل الاقتحامية تتراوح بين ما يصل إلى 11 000 دولار لكل مخالفة بالنسبة لغير المرخصين ومبلغ يصل إلى 130 000 دولار للمخالفة الواحدة من شركات البريد العامة المرخصة. وعلاوة على الغرامات النقدية، يمكن للجنة أن تصدر أمراً بالوقف والكف عن العمل ضد مرسلي الرسائل الاقتحامية الذين يخالفون أي حكم من أحكام قانون الاتصالات أو أي قاعدة من قواعد لجنة الاتصالات الاتحادية مرخص بها بحكم القانون. وعلاوة على ذلك، فإنه وفقاً لقانون الاتصالات، يخضع أي شخص يخالف أحكام القانون لإجراءات المحاكمة الجنائية بواسطة وزارة العدل (بالإضافة إلى العقوبة النقدية) وقد يواجه السجن لفترة تصل إلى عام واحد (أو إلى عامين للمرتكبين بصورة متكررة). و لم تصدر لجنة الاتصالات الاتحادية حتى الآن أي وقائع إنفاذ تتعلق بهذه الرسائل التجارية.

3.1.9 نُهُج للحد من التصيد الاحتيالي على الإنترنت

وكما جرت مناقشته أعلاه، فإن الفرضية الأساسية التي يستند إليها مرسلو الرسائل الاقتحامية والمتصيدون الاحتياليون هي عدم معرفة الشخص المرسِل. وقد أصدر فريق مهام هندسة الإنترنت (IETF) معيارين، رسالة تعريف مفاتيح الميدان (DKIM)، b-IETF RFC 4871، وممارسات إرسال ميدان المؤلف (ADSP)، b-IETF- RFC 5617، من شأنهما أن يحسنا قدرة متلقي الرسالة على التعرف على هوية المرسل. ولدى الانتهاء من هذا المسعى، سيبدأ البائعون في إتاحة وسائل التنفيذ للعملاء. وهناك أيضاً على الأقل تطبيق واحد مجاني[17] لهذا المعيار. ويتمثل أحد مصادر المساعدة في فريق العمل المعني بمكافحة التصيد الاحتيالي (APWG)، وهو رابطة صناعية تركز على القضاء على عمليات سرقة الهوية والتدليس الناجمة عن تزايد مشكلة التصيد الاحتيالي والغش الإلكتروني. وتوفر الرابطة منتدى لمناقشة المسائل المتصلة بالتصيد الاحتيالي (APWG)، وإجراء اختبارات وتقييمات للحلول التكنولوجية الممكنة، والنفاذ إلى مستودع مركزي للحوادث المتعلقة بعمليات التصيد الاحتيالي (http://www.antiphishing.org/index.html).

ومن خلال هذا المعيار فقط يمكن إتاحة "قائمة تصديق بيضاء"، أو القدرة على التحقق، على سبيل المثال، مما إذا كان مصرفك الشخصي هو الذي يحاول الاتصال بك فعلاً. وعن طريق هذا المعيار، يمكن للمستهلكين التثبت مما إذا كان أصدقاؤهم أو ذويهم هم الذين يحاولون فعلاً الاتصال بهم. وهذا المعيار في حد ذاته سيحد من بعض أشكال التصيد الاحتيالي، ولكن ليس جميعها.

2.9 اليابان

1.2.9 إنفاذ القانون

يوجد في اليابان قانونان لتقييد إرسال البريد الإلكتروني من أجل القضاء على الرسائل الاقتحامية. وتتمثل العناصر الرئيسية في هذين القانونيين فيما يلي:

- تُطبق القواعد التالية على إرسال رسائل الإعلانات عبر البريد الإلكتروني (حرية رفض أو قبول استقبال الرسائل)

  يُحظر إرسال رسائل الإعلانات عبر البريد الإلكتروني إلى مستقبلين دون الحصول على موافقتهم.

  يتعين أن يكون لدى المنظمة المرسلة الدليل على موافقة المستقبلين عند إرسال رسائل الإعلانات إليهم.

  يتعين أن تقدم رسائل الإعلانات معلومات عن إجراءات وقف إرسال هذه الرسائل واسم المرسل وما إلى ذلك.

  إذا اتبعت الجهة المستقبلة الإجراءات السليمة لإخطار المنظمة المرسلة بعدم رغبتها في استقبال رسائل إعلانات، يجب على المنظمة المرسلة عدم إرسال أي رسائل إعلانات أخرى إلى الجهة المستقبلة.

[17] لفظة "مجاني" في هذا السياق تشير إلى إمكانية تنفيذ هذه الخاصية مجانا بموجب الشروط التي يحددها صاحب حق ملكية الاختراع.

- يُحظر إرسال رسائل بريد إلكتروني تحمل معلومات مزيفة عن المرسل، مثل عنوان البريد الإلكتروني وعنوان بروتوكول الإنترنت واسم الميدان.
- يُحظر إرسال رسائل بريد إلكتروني إلى عناوين خيالية لمستقبلين يتم توليدها آلياً عن طريق برنامج حاسوبي.

2.2.9 مجلس النهوض بتدابير مكافحة الرسائل الاقتحامية

نظم عدد كبير من الأطراف المعنية مثل موردي خدمات الإنترنت والمعلنين وموردي خدمات التطبيقات الخاصة بإرسال الرسائل الإعلانية وبائعي المنتجات الأمنية ومنظمات المستهلكين والإدارات وما شابه، مجلساً للنهوض بتدابير مكافحة الرسائل الاقتحامية وذلك في عام 2008. وقد اعتمد المجلس في نوفمبر 2008 إعلاناً "نحو استئصال الرسائل الاقتحامية".

3.2.9 مركز التنظيف السيبراني (CCC)

أُنشئ مركز التنظيف السيبراني الذي يكتشف أجهزة الحاسوب المصابة بالبرامج الروبوتية الضارة، بعد التعاون الوثيق بين الحكومة اليابانية والمنظمات الخاصة بموردي خدمات الإنترنت وموردي خدمات الإنترنت الرئيسيين. ويعمل هذا المركز على النحو التالي:

- يدير المركز نظاماً ضخماً مضاداً للبرمجيات الروبوتية يقوم باستقبال الأنشطة الضارة من البرمجيات الضارة (برمجيات روبوتية عادة) من أجهزة الحاسوب المصابة. ويقوم نظام مكافحة البرمجيات الروبوتية بجمع عناوين بروتوكول الإنترنت لأجهزة الحاسوب المرسلة لهذه البرمجيات وشفرات برامج البرمجيات الضارة (البرمجيات الروبوتية).
- ترسل قوائم بعناوين بروتوكول الإنترنت المكتشفة وتاريخ/موعد اكتشافها إلى كل مورد من موردي خدمات الإنترنت. ويبلغ مورد خدمة الإنترنت مشتركيه بهذه العواني وأن حواسيبهم قد تُصاب ببرمجيات ضارة منها. كما يرسل مورد الخدمة إلى مشتركيه معلومات عن مركز التنظيف السيبراني (رابط الصفحة الويب) وبرمجية لعلاج الإصابة.
- يقوم المركز بتحليل شفرات البرامج التي تم تجميعها. فإذا كانت شفرة البرنامج غير محددة من قبل، يتم استنباط برمجية جديدة لعلاج الإصابة من هذه البرمجية الضارة الجديدة ثم يتم إطلاقها.

ويساهم هذا النشاط في كبت أنشطة الإصابة بالبرمجيات الروبوتية الضارة في اليابان. ولما كانت معظم الرسائل الاقتحامية تُرسل من أجهزة حاسوب مصابة ببرمجيات روبوتية ضارة، فإن هذا النشاط يساهم أيضاً في الحد من الرسائل الاقتحامية المرسلة من اليابان.

4.2.9 سد البوابة 25 خارج الحدود (OP25B)

عند إرسال مشتركي خدمة الإنترنت واستقبال رسائل البريد الإلكتروني، يستعملون خدمة بريد إلكتروني يقدمها مورد خدمة إنترنت عادة. لذا يرسل المشتركون رسائلهم إلى مخدمات بريد المورد ثم تقوم هذه المخدمات بنقل رسائل البريد الإلكتروني هذه إلى مخدمات البريد الإلكتروني لجهة المقصد مباشرة. ولا يرسل المشتركون رسائل بريدهم الإلكتروني إلى مخدمات البريد الإلكتروني لجهة المقصد مباشرة. ونظراً إلى أن أجهزة الحاسوب المصابة ببرمجيات روبوتية ضارة أو بفيروسات ترسل الرسائل الاقتحامية إلى مخدمات البريد الإلكتروني لجهة المقصد مباشرة، فإن هذه الرسائل لا تمر عبر مخدمات البريد الإلكتروني لموردي خدمات الإنترنت. فإذا تسنى وقف الاتصالات من أجهزة حاسوب المشتركين التي لا تمر عبر شبكة مورد خدمة الإنترنت باستعمال بروتوكول نقل البريد البسيط (SMTP) (عبارة عن بروتوكول تحكم في النقل تحمل بوابة المقصد الخاصة به الرقم 25)، فإنه يمكن وقتها منع كثير من الرسائل الاقتحامية. ولذا درست الحكومة اليابانية وموردي خدمات الإنترنت والمنظمات ذات الصلة القضايا التالية وذلك بالتعاون الوثيق فيما بينها.

- التأثير الواقع على المشتركين عند إدخال بروتوكول التحكم في النقل الخاص بالمعيار OP25B، b-MAAWG.MP25.
- القيود على سد اتصالات محددة في إطار القوانين اليابانية السارية.

وبعد هذه الدراسات، طبق كثير من الموردين المعيار OP25B في إطار الأنشطة التالية. ويلعب الفريق JEAG (فريق مكافحة إساءة استعمال البريد الإلكتروني في اليابان) دوراً هاماً في هذه العملية من خلال نشر توصية لموردي خدمات الإنترنت تحثهم على إدخال المعيار OP25B.

- على الرغم من أن إدخال المعيار OP25B ليس إجبارياً على موردي خدمات الإنترنت اليابانية، فإن نحو 52 مورداً من موردي خدمات الإنترنت، من بينهم أغلبية الموردين الرئيسيين، أدخلوا المعيار OP25B حتى يوليو 2009.

- يوفر الكثير من موردي خدمات الإنترنت عند إدخال المعيار OP25B البوابة رقم 587 لبروتوكول التحكم في النقل مع SMTP AUTH، كأسلوب بديل للاتصالات، سعياً نحو تجنب خفض جودة الخدمة. ويمكن للمستعملين إرسال رسائل البريد الإلكتروني عن طريق مورد خدمة إنترنت آخر يعتمد المعيار OP25B إلى مخدم بريد هذا المورد.

5.2.9 تكنولوجيات استيقان المرسل

تكنولوجيات استيقان المرسل هي تقنيات تكتشف الخداع في عنوان مصدر البريد الإلكتروني. وقد نشر الفريق JEAG توصية بإدخال هذه التقنيات ونشرت وزارة الشؤون الداخلية والاتصالات وثيقة "المسائل القانونية الهامة المتعلقة بإدخال استيقان المرسل عند جانب الاستقبال بواسطة مورد خدمة الإنترنت". وفي الوقت الحالي، انتهى كل مشغلي الاتصالات المتنقلة تقريباً وبعض موردي خدمات الإنترنت من إدخال إطار سياسات المرسل (SPF)، [b-IETF REC 4408]، ويمثل هذا الإطار إحدى تكنولوجيات استيقان المرسل ويمكن لمشتركيهم استعمال نتائج الاستيقان لأغراض الترشيح. وقد بلغت نسبة الإطارات SPF المنشورة المسجلة للميادين "JP" في أغسطس 2009 نحو 35,99%. كما بدأ العديد من موردي خدمات الإنترنت في إدخال المعيار DKIM، [b-IETF RFC 4871] كوسيلة استيقان إضافية للمرسل.

6.2.9 تبادل معلومات مرسل الرسائل الاقتحامية بين مشغلي الاتصالات المتنقلة

تملك أغلب الهواتف الخلوية في اليابان إمكانية تداول رسائل البريد الإلكتروني العامة. ولما كان الكثير من الرسائل الاقتحامية يرسل من هواتف خلوية متنقلة في اليابان، فإن جميع مشغلي الاتصالات المتنقلة يتبادلون المعلومات الخاصة بمرسلي الرسائل الاقتحامية حسب الخطوات التالية:

- يتم فحص معرف هوية أي فرد يرغب في إبرام عقد للحصول على هاتف متنقل وذلك بموجب "قانون منع إساءة استعمال الهواتف المحمولة".
- إذا توصل مشغل خدمة اتصالات متنقلة إلى مستعمل هاتف خلوي يقوم بإرسال رسائل اقتحامية وهو ما يخالف "قانون تنظيم إرسال بريد إلكتروني محدد"، تُقدم المعلومات الخاصة بهذا المستعمل إلى جميع مشغلي الاتصالات المتنقلة الآخرين.

لذا، فإنه إذا قام مستعمل بإرسال رسائل اقتحامية من هاتف خلوي، فإنه سيواجه صعوبات في الدخول في تعاقد باستعمال الهواتف المتنقلة في اليابان.

وهناك منظمة غير ربحية ذات صلة تقوم بتركيب محاسيس وتجمع الرسائل الاقتحامية وتحللها. وهي تقدم معلومات عن مرسلي الرسائل الاقتحامية إلى موردي خدمات الإنترنت الموجودين في اليابان وبتبادل هذه المعلومات مع بعض الوكالات الموجودة في بلدان أخرى.

ثبت المراجـــع

[b-IETF RFC 4871] IETF RFC 4871 (2007), *Domainkeys Identified Mail (DKIM) Signatures*. http://www.ietf.org/rfc/rfc4871.txt

[b-IETF RFC 5617] IETF RFC 5617 (2009), *DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)*. http://www.ietf.org/rfc/rfc5617.txt

[b-MAAWG MP25] MAAWG Recommendation (2005), *Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction*. http://www.maawg.org/port25

[b-IETF RFC 4408] IETF RFC 4408 (2007), *Sender Policy Framework (SPF) fo Authorizing Use of Domains in E*-Mail*, Version 1*. http://www.ietf.org/rfc/rfc4408.txt

[b-contr-spam] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (United States Code). This Act is documented in the following laws: 15 U.S.C. §§ 7701-7713; 18 U.S.C. § 1037; 28 U.S.C. § 994; 47 U.S.C. § 227. http://www.gpsaccess.gov/uscode/index.html

[b-ITU-T cyb] Messaging Anti-Abuse Working Group Conference reports: http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html.

الملحق بـــاء

إدارة الهوية

الاتحـــــــاد الدولـــــــي للاتصـــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X

الإضافة 7
(2009/02)

السلسلة X: شبكات البيانات والاتصالات
بين الأنظمة المفتوحة ومسائل الأمن

إضافة تتعلق بلمحة عامة لإدارة الهوية في سياق الأمن السيبراني

تحذيـــر

تمهيد لنشر توصيـــة

هذا المنشور صيغة غير محررة لتوصية معتمدة مؤخراً. وسيجري الاستعاضة عنها بصيغة منشورة ما أن يتم تحريرها، ولذلك، ستكون هناك اختلافات بين المنشور التمهيدي والصيغة المنشورة.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه المنشورة لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه المنشورة اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه المنشورة حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه المنشورة إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه المنشورة أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد المنشور.

وعند الموافقة على هذه المنشورة، [كان/لم يكن] الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه المنشورة. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه المنشورة بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

الإضافة 7 إلى توصيات السلسلة X – سلسلة التوصيـــات ITU-T X.1250

إضافة تتعلق بلمحة عامة لإدارة الهوية في سياق الأمن السيبراني

ملخص

جرى تناول أمن الشبكة الهاتفية التقليدية العمومية التبديلية (PSTN) على مدى عشرات السنين من تشغيلها. على أنه لا يمكن القول بنفس الشيء بالنسبة للشبكات العمومية الموزعة لمقدمي خدمات متعددة مثل الإنترنت وشبكات الجيل التالي (NGNs) وتستعمل هذه الشبكات منصة نقل مشتركة للتحكم في الحركة وحركة المستعمل، بالإضافة إلى الإغفال الممكن لهذه الحركة. ويمكن نقل حركة بروتوكول الإنترنت بدون تعريف وهذا يجعل الشبكات القائمة على هذه التكنولوجيا معرضة لإساءة الاستعمال من جانب المستعملين. وجميع الخدمات الإلكترونية (مثل الأعمال التجارية الإلكترونية، والتجارة الإلكترونية، والصحة الإلكترونية، والحكومة الإلكترونية) معرضة للهجوم. وهذه المشكلة يمكن معالجتها على الأقل جزئياً عن طريق زيادة الثقة في هوية المستعملين، وفي تجهيزات الشبكة ومقدمي الخدمة، ومن ثم يمكن التثبت من شخصيتهم، ومنحهم حق النفاذ الملائم، ومراقبتهم. ولذلك فإن إدارة الهوية توفر مزيداً من الضمانات والثقة في المستعمل ومقدم الخدمة، وهويات أجهزة الشبكة وتحسن الأمن بتقليل التعرض للمخاطر الأمنية. وهذا الجانب من جوانب الأمن السيبراني هو من الجوانب التي يتعين على موفري الخدمات النظر فيها على مستوى الأعمال والمستوى التقني، كما ينبغي للحكومات النظر فيها على المستوى الوطني كجزء من الخطة الوطنية للأمن السيبراني.

مقدمـــة

إدارة الهوية (IdM)، هي وسيلة لإدارة المعلومات والتحكم فيها تستعمل في عملية الاتصالات لتمثيل كيانات (مثل مقدمي الخدمات ومنظمات المستعملين النهائيين، والأشخاص، وتجهيزات الشبكات، وتطبيقات البرمجيات، والخدمات). ويمكن لأي كيان وحيد أن تكون له مجموعة متعددة من نعوت الهوية كي يمكنه النفاذ إلى خدمات شتى ذات متطلبات أمنية متباينة، ويمكن لهذه المتطلبات أن توجد في مواقع متعددة.

وإدارة الهوية هي عنصر رئيسي من عناصر الأمن السيبراني لأنها توفر القدرة على إقامة ودعم الاتصالات الموثوق بها بين الكيانات. وهي تدعم التحقق من هوية كيان ما، ولكنها تتيح أيضاً التحقق من طائفة كبيرة من امتيازات النفاذ (وليس النفاذ المقصور على النفاذ الكلي)، وسهولة تغيير الامتيازات في حالة حدوث تغيير في دور الكيان. وتتيح إدارة الهوية أيضاً للمنظمة ضمان التطبيق الملائم لسياساتها الأمنية عن طريق رصد ومراقبة أنشطة الكيان. ويمكن عن طريق إدارة الهوية توفير النفاذ للكيانات داخل المنظمة وخارجها. وخلاصة القول، فإن وجود تطبيقات جيدة لإدارة الهوية من شأنه أن يوفر القدرات الموثوق بها للتحقق من الهويات، وتوفير إدارة الهويات الخاصة بالكيانات، وامتيازات النفاذ، ومراقبة النفاذ الخاص بكيان معين.

وإدارة الهوية هي عنصر حاسم في إدارة الأمن وتمكين النفاذ الترحالي وعند الطلب إلى الشبكات والخدمات الإلكترونية. وإلى جانب الآليات الدفاعية الأخرى (مثل حوائط الحماية، وأنظمة تتبع الاقتحام، والحماية من الفيروسات)، تؤدي إدارة الهوية دوراً هاماً في حماية المعلومات وشبكات وخدمات الاتصالات من الجرائم السيبرانية من قبيل التدليس وسرقة الهوية. ويضاعف هذا بدوره من ثقة المستعملين في أن التعاملات الإلكترونية مأمونة وموثوق بها، الأمر الذي ييسر من استعمال شبكات بروتوكول الإنترنت في الخدمات الإلكترونية.

وعند تنفيذ نظام ما لإدارة الهوية، يجب تناول الاهتمامات الأساسية المتعلقة بالخصوصية. وهذا يعني وضع أساليب تكفل دقة معلومات الهوية والوقاية من استخدام معلومات الهوية لأغراض تتجاوز تلك التي جمعت من أجلها.

1 مجال التطبيق

ظهرت إدارة الهوية باعتبارها مكوناً حيوياً من شأنه تحسين الأمن عن طريق توفير مزيد من الضمانات وذلك بالتحقق من صحة معلومات الهوية. وتوفر هذه الإضافة لمحة عامة بشأن هذه الخدمة الجديدة.

ولا يشير استعمال تعبير "هوية" في هذه الإضافة إلى إدارة الهوية بمعناها المطلق. ولا يشكل صحة إيجابية على وجه الخصوص.

2 المراجع

لا يوجد.

3 التعاريف

يمكن الاطلاع على التعاريف في سائر توصيات السلسلة X.1205.

4 المختصرات

IdM إدارة الهوية (*Identity Management*)

IP بروتوكول الإنترنت (*Internet Protocol*)

PSTN الشبكة الهاتفية العمومية التبديلية (*Public Switched Telephone Network*)

5 الاصطلاحات

لا يوجد.

6 أهمية إدارة الهوية لحماية البنية التحتية للشبكة العالمية والتنسيق متعدد البلدان من أجل الأمن

من شأن التنفيذ السليم واستعمال قدرات إدارة الهوية وممارساتها في الشبكات الوطنية والإقليمية والدولية أن يعزز أمن البنية التحتية للشبكة العالمية. وأفضل ممارسات إدارة الهوية وتنفيذها من الأمور الهامة والضرورية لتوفير ضمانات لمعلومات الهوية وسلامة وتيسر البنية التحتية للشبكة العالمية.

ويمكن استعمال قدرات إدارة الهوية لدعم خدمات اتصالات الطوارئ الوطنية والدولية من خلال تحديد المستعملين المأذون لهم باستعمال الخدمات الخاصة.

بالإضافة إلى ذلك، يمكن استعمال قدرات إدارة الهوية للوقاية من حوادث الأمن السيبراني ودعم تنسيق الاستجابة على المستويين الوطني والدولي. وفي بعض الحالات، يمكن أن تساعد إدارة الهوية السلطات والكيانات على تنسيق جهودها لتتبع مصدر هذه الحوداث وتحديده.

7 إدارة الهوية كداعم للاتصالات الموثوقة بين كيانين

من الوظائف الهامة لإدارة الهوية، دعم الاستيقان من المستعملين والشبكات والخدمات. وفي إطار عملية استيقان تنطوي على كيانين، ينبغي أن يقدم كيان واحد تأكيدات تتعلق بهويته للكيان الآخر. ووفقاً لمتطلبات الأمن للكيان الثاني، قد يتعين التحقق من هذه التأكيدات قبل أن يثق الكيان الثاني في الكيان الأول بما فيه الكفاية لمنحه امتيازاته.

وهناك مستويات شتى من الثقة في الاستيقان تتراوح من بضعة إلى لا شيء، من ضعيفة (أي اسم المستعمل وكلمة السر) إلى قوية (أي البنية التحتية الرئيسية العمومية (ITU-T X.509)). ويمكن أن يحدد تقييم المخاطر المستوى الملائم من الاستيقان وقد تكون هناك مستويات أعلى من الاستيقان لكيان واحد أكثر من الآخر، مثلاً، نظراً لتحكم كيان واحد في المصادر الحيوية.

8 حماية بيانات الهوية وصيانتها وإلغاؤها والتحكم فيها

تشمل الوظائف الهامة الأخرى لإدارة الهوية حماية بيانات الهوية الموثوق بها وصيانتها والتحكم فيها، بما في ذلك القدرة على التحكم في الحالة الجارية لهوية ما.

يجوز أن تقضي القوانين أو السياسات بحماية المعلومات الشخصية القابلة للتحديد ووقاية بيانات الهوية من استخدامها لأغراض تتجاوز تلك التي جمعت من أجلها. وضمان استمرار صحة بيانات الهوية من الشواغل الأولية الأخرى. وبالنسبة للخدمات التي تستعملها لكي تكون قابلة للبقاء، يجب صيانة بيانات الهوية على نحو سليم بحيث تتسم بالدقة وحسن التوقيت والثبات.

وحسب الاقتضاء، ينبغي أن تشمل نعوت بيانات الهوية القدرة على التحقق من بيانات الهوية لمعرفة ما إذا كانت قد ألغيت.

9 "اكتشاف" المصادر الموثوقة لبيانات الهوية

ينطوي مفهوم إدارة الهوية أيضاً على فكرة "اكتشاف" بيانات الهوية الموثوقة. وفي البيئات عالية التوزيع ومتعددة موفري الخدمة (مثل الإنترنت وشبكات الجيل التالي)، يمكن لبيانات الهوية اللازمة لتوفير الثقة والتأكيدات ذات الصلة لأي كيان أن توضع في مواقع مختلفة على الشبكة. ويمكن أن يكون للكيانات هويات رقمية متعددة من مصادر مختلفة لمعلومات الهوية في مواقع مختلفة. وعندما يكون كيان واحد من الكيانين في عملية استيقان ترحالية، ستحتاج الكيانات الأخرى إلى تحديد الموقع وإقامة علاقة ثقة بالمصدر الملائم من معلومات الهوية بحيث يستكمل عملية استيقان الكيان الترحالي. ومفهوم اكتشاف مصادر المعلومات الموثوقة مماثل لما يحدث اليوم في استعمال الهواتف الخلوية في الشبكات المتنقلة.

10 خدمات الحكومة الإلكترونية

تشمل المزايا الممنوحة لكيان ما من أجل تنفيذ عملية إدارة الهوية، خفض المخاطر، وتعزيز الثقة وزيادة الخصائص الوظيفية وقدراتها من أجل تخفيض التكلفة. وهذه الأسباب صالحة بنفس القدر حينما تكون الحكومة هي الكيان. وفي سياق الحكومة الإلكترونية، تتمثل هذه الأهداف الرئيسية أيضاً في تخفيض التكلفة وتقديم خدمات أكثر كفاءة وأكثر فعالية لمواطني الحكومة وشركائهم التجاريين.

وتواجه الحكومة، شأنها شأن الكيانات الأخرى، التحدي المتمثل في الاستخدام الفعال والكفؤ في عالم مترابط شبكياً. ولكي تصبح الحكومة الإلكترونية حقيقة واقعة، يجب على الحكومة أن تجري تحليلات للمخاطر على الخدمات الإلكترونية التي تزمع تقديمها وأن تقوم بتنفيذ التدابير الوقائية المناسبة. ويمكن أن تتطلب الطبيعة الحساسة لخدمات الحكومة الإلكترونية (مثلاً، الصحة الإلكترونية) من الحكومة استخدام آليات استيقان قوية.

11 الاعتبارات التنظيمية لإدارة الهوية

ينبغي أن تنظر الإدارات الوطنية والمجموعات الإقليمية في عدد من القضايا التنظيمية المحتملة المتعلقة بتنفيذ إدارة الهوية، مثل الخصوصية وحماية البيانات، والأمن الوطني، والاستعداد لحالات الطوارئ، والتسوية الإلزامية بين الموجات الحاملة. ولا تستعمل الحكومات تقنيات إدارة الهوية فحسب لكن يمكن أن تفرضها أيضاً على كيانات أخرى لتلبية شريحة أوسع من أهداف السياسة الوطنية والأمنية.

ثبت المراجـــع

هناك منتديات شتى تعكف على العمل بشأن المسائل المتعلقة بإدارة الهوية. ومن بين هذه المنتديات ما يلي:

مفتاح موارد المحفوظات (ARK) (مفتاح موارد محفوظات مكتبة كاليفورنيا الرقمية): http://www.cdlib.org/inside/diglib/ark/

مشروع الشركة من أجل الجيل الثالث – محرك المعالجة ثلاثي الأبعاد:
3GPP SA3: http://www.3gpp.org/SA3-Security?page=type_url

فرقة العمل 7 المعنية ببيان أثر القيمة المضافة لأنظمة أمن الاتصالات وأنظمة المعلومات الأوتوماتية:
ETSI TISPAN WG7: http://www.etsi.org/tispan/

خارطة طريق الاتحاد الأوروبي وبطاقة الهوية الإلكترونية:
http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

بطاقة المواطنة الأوروبية: http://europa.eu.int/idabc/servlets/Doc?id=19132

مستقبل الهوية في مجتمع المعلومات (التابع للاتحاد الأوروبي): http://www.fidis.net/

منتدى أفرقة الأمن والاستجابة للحوادث (FIRST): http://www.first.org/

مشروع الاتحاد الأوروبي من أجل هوية المستعمل من أجل أوروبا: http://www.ist-world.org/ProjectDetails.aspx?ProjectId=4ddb2e61c84343f0acd370607e5a8499&SourceDatabaseId=7cff9226e582440894200b751bab883f

Handle: http://www.handle.net/

Higgins: http://www.eclipse.org/higgins/index.php

المعهد الوطني الأمريكي لمعايير الوقاية من سرقة الهوية وخبراء معايير إدارة الهوية:
http://www.ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3

إطار إدارة هوية ORACLE: http://www.oracle.com/technology/tech/standards/idm/igf/index.html

مركز إدارة سرقة الهوية: http://www.idtheftcenter.org/

فريق مهام هندسة الإنترنت: http://sec.ietf.org/

قطاع تقييس الاتصالات – فريق التركيز للجنة الدراسات 17 المعني بإدارة الهوية:
www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

قطاع تقييس الاتصالات – لجنة الدراسات 17 المعنية بالأمن، المسألة 10:
http://www.itu.int/ITU-T/studygroups/com17/index.asp

قطاع تقييس الاتصالات – لجنة الدراسات 13 (شبكات المستقبل) المسألة 13:

http://www.itu.int/ITU-T/studygroups/com13/index.asp

مشروع التحالف من أجل الحرية: http://www.projectliberty.org/

مشروع الهوية المبسطة: http://lid.netmesh.org/wiki/Main_Page

اتحاد إدارة الهوية: http://www.egov-goodpractice.org

و https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

مخططات بطاقة الهوية الوطنية: http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/

http://en.wikipedia.org/wiki/Identity_document

منظمة النهوض بمعايير المعلومات المنظمة (OASIS): http://www.oasis-open.org/home/index.php

منظمة التعاون والتنمية في الميدان الاقتصادي (OECD)، ورشة العمل بشأن إدارة الهوية الرقمية المعقودة في Trondheim، النرويج، 8-9 مايو 2007: http://www.oecd.org/sti/security-privacy/idm

التحالف المفتوح للهواتف المتنقلة (OMA): http://www.openmobilealliance.org/

مجموعة Open: http://www.opengroup.org

نظام هوية الموارد المفتوحة (OSIS): http://osis.idcommons.net/wiki/Main_Page

ريادة النهوض بالخصوصية والأمن في عالم الهواتف المتنقلة (PAMPAS) (برنامج للاتحاد الأوروبي): http://www.pampas.eu.org/

مبادرة الاتحاد الأوروبي لمجتمع المعلومات لتقييس المزايا والأدوار

إدارة الخصوصية والهوية من أجل أوروبا:
https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium – PRIME

التجمع العالمي للشبكة الإلكترونية: http://www.w3.org/

منظمة Yadis: http://yadis.org/wiki/Main_Page

الملحق جيم

روابط ومراجع

سيتم تحديث قائمة المواد المرجعية التالية بشكل منتظم، على أن يؤخذ في الاعتبار نواتج جدول الأعمال العالمي للأمن السيبراني للاتحاد الدولي للاتصالات ونواتج المشروع المخصص لتنفيذ القرار 45 (WTDC-06)، والعمل المنفذ من جانب لجنة الدراسات 17 لقطاع تقييس الاتصالات (لجنة الدراسات الرئيسية في مجال الأمن داخل قطاع تقييس الاتصالات) فيما يخص قرارات الجمعية العالمية لتقييس الاتصالات فضلاً عن متابعة خط العمل جيم5 للقمة العالمية لمجتمع المعلومات بشأن الأمن السيبراني ونتائج الأعمال بشأن قرارات مؤتمر المندوبين المفوضين لعام 2006 (مثل القرارات 130 و131 و149).

الجـــزء I: وضع والحصول على اتفاق بشأن استراتيجية وطنية للأمن السيبراني

1.C.I استثارة الوعي (1.B.I و2.B.I)

دوليـــاً

- قرار الجمعية العامة للأمم المتحدة 55/63 بشأن "مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية": http://www.un.org/Depts/dhl/resguide/r55.htm.
- قرار الجمعية العامة للأمم المتحدة 56/121 بشأن "مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية": http://www.un.org/Depts/dhl/resguide/r56.htm.
- قرار الجمعية العامة للأمم المتحدة 57/239 بشأن "إنشاء ثقافة عالمية بشأن الأمن السيبراني": http://www.un.org/Depts/dhl/resguide/r57.htm.
- قرار الجمعية العامة للأمم المتحدة 58/199 بشأن "إنشاء ثقافة عالمية بشأن الأمن السيبراني وحماية البنى التحتية الحرجة للمعلومات": http://www.un.org/Depts/dhl/resguide/r58.htm.
- إعلان مبادئ وخطة عمل جنيف الصادران عن القمة العالمية لمجتمع المعلومات التابعة للأمم المتحدة والتزام وبرنامج عمل تونس بشأن مجتمع المعلومات: http://www.itu.int/WSIS/index.html.
- المبادئ التوجيهية لمنظمة التعاون في الميدان الاقتصادي بشأن أمن أنظمة وشبكات المعلومات: نحو ثقافة أمنية (2005): http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.
- كتيِّب حماية البنية التحتية الدولية الحرجة للمعلومات لعام 2006 (المجلد 1): http://www.isn.ethz.ch/pubs/ph/details.cfm?id=250.
- موارد الاتحاد الدولي للاتصالات المتعلقة بالأمن السيبراني: http://www.itu.int/cybersecurity/.
- جدول الأعمال العالمي للأمن السيبراني للاتحاد الدولي للاتصالات: http://www.itu.int/cybersecurity/gca/.
- بوابة الاتحاد الدولي للاتصالات للأمن السيبراني: http://www.itu.int/cybersecurity/gateway/.
- صفحة الويب الخاصة بالأمن السيبراني لمكتب تنمية الاتصالات بالاتحاد الدولي للاتصالات: http://www.itu.int/ITU-D/cyb/.
- مبادرة الاتحاد الدولي للاتصالات لحماية الأطفال على الخط والمبادئ التوجيهية ذات الصلة: http://www.itu.int/cop/.

2.C.I الاستراتيجيات الوطنية والإقليمية الدولية (2.B.I و3.B.I و4.B.I و5.B.I و6.B.I)

دوليـــاً

- الأمن السيبراني الوطني للاتحاد الدولي للاتصالات/مجموعة أدوات التقييم الذاتي لحماية البنية التحتية الحرجة للمعلومات: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

- الاتحاد الدولي للاتصالات والمؤسسة الاتحادية السويسرية للتكنولوجيا (ETH Zurich) – إطار وطني عام لحماية البنية التحتية الحرجة للمعلومات:
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf.
- قطاع تنمية الاتصالات، المسألة 22/1: تأمين شبكات المعلومات والاتصالات: أفضل الممارسات في مجال إرساء ثقافة للأمن السيبراني:
http://www.itu.int/ITU-D/study_groups/SGP_2006-2010/documents/DEFQUEST-SG1/DEFQUEST-Q22-1-E.pdf.
- جدول الأعمال العالمي للاتحاد الدولي للاتصالات بشأن الأمن السيبراني: http://www.itu.int/cybersecurity/gca/.
- دليل الأمن السيبراني للاتحاد الدولي للاتصالات للدول النامية، المراجع في 2009:
http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf.
- القرار 45 الصادر عن المؤتمر العالمي لتنمية الاتصالات: آليات تعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية (الدوحة، 2006):
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf
- قطاع تقييس الاتصالات، لجنة الدراسات 17، ملخص المسألة 4 – قائمة توصيات قطاع تقييس الاتصالات التي تمت الموافقة عليها والمتعلقة بأمن الاتصالات:
http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090001MSWE.doc.
- قطاع تقييس الاتصالات، لجنة الدراسات 17، المسألة 4 – الأمن في الاتصالات وتكنولوجيا المعلومات:
http://www.itu.int/pub/T-HDB-SEC.03-2006/en/.
- دراسة مكتب تنمية الاتصالات بشأن الجوانب المالية لأمن الشبكات: البرمجيات الضارة والرسائل الاقتحامية:
http://www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf.
- المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي بشأن أمن أنظمة وشبكات المعلومات: نحو ثقافة أمنية:
http://www.oecd.org/document/42/0,3343,en_21571361_36139259_15582250_1_1_1_1,00.html.
- خطة تنفيذ منظمة التعاون والتنمية في الميدان الاقتصادي بشأن سياسات الأمن الإلكتروني الوطنية المنسقة:
http://www.oecd.org/dataoecd/23/11/31670189.pdf.
- تقرير البنك الدولي عن "الأمن السيبراني: نموذج جديد لحماية الشبكة":
http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2006/12/12/000020953_20061212113151/Rendered/PDF/381170CyberSec1uly0250200601PUBLIC1.pdf.
- الرابطة الأمريكية لتكنولوجيا المعلومات (ITAA)، ورقة بيضاء بشأن أمن المعلومات:
http://www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf.

إقليمياً

- فريق العمل المعني بالاتصالات والمعلومات التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC) – استراتيجية الأمن السيبراني للرابطة (2002):
http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf.
- الكتاب الأزرق للجنة البلدان الأمريكية للاتصالات (CITEL): سياسات الاتصالات في البلدان الأمريكية (2005)، القسمان 4.8 و5.8: http://www.citel.oas.org/publications/azul-fin-r1c1_i.pdf.
- قرار مجلس الاتحاد الأوروبي – استراتيجية من أجل مجتمع معلومات مؤمن – حوار وشراكة وتحسين (2007):
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf .

- إعلان الدوحة بشأن الأمن السيبراني (2008):
http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf.
- رسالة الاتحاد الأوروبي بشأن "استراتيجية من أجل مجتمع معلومات مؤمن" (2006):
http://ec.europa.eu/information_society/doc/com2006251.pdf.
- برنامج الاتحاد الأوروبي بشأن إنترنت أكثر أمناً:
http://europa.eu.int/information_society/activities/sip/index_en.htm.
- الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)، بدأت الوكالة دراسة بشأن "اقتصاديات الأمن والسوق الداخلية" (2008): http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm.
- استراتيجية منظمة البلدان الأمريكية (OAS) لمكافحة تهديدات الأمن السيبراني (2004):
http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.

وطنيـــاً

- البرنامج الأسترالي لنمذجة وتحليل حماية البنية التحتية الحيوية (CIPMA):
http://www.csiro.au/partnerships/CIPMA.html.
- الدليل الدولي لحماية البنية التحتية الحيوية للمعلومات الصادر عن شبكة الأزمات والمخاطر: جرد لسياسات الحماية الوطنية وتحليلها: http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250.
- الخطة الوطنية الألمانية لحماية البنية التحتية للمعلومات:
http://www.en.bmi.bund.de/cln_028/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf.
- الاستراتيجية الوطنية اليابانية بشأن أمن المعلومات (ترجمة مؤقتة):
http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.
- استراتيجيات التنفيذ الوطنية لعدد 11 عضواً في منظمة التعاون والتنمية في الميدان الاقتصادي:
http://www.oecd.org/document/63/0,2340,en_21571361_36139259_36306559_1_1_1_1,00.html
- الاستراتيجية الرقمية لنيوزيلندا: http://www.digitalstrategy.govt.nz.
- الخطة الرئيسية الثانية لأمن المعلومات والاتصالات في سنغافورة:
http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20080417090044/MR17Apr08MP2.pdf.
- استراتيجية سنغافورة لتأمين الفضاء السيبراني:
http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21.
- مركز المملكة المتحدة لحماية البنية التحتية الوطنية (CPNI): http://www.cpni.gov.uk/.
- الاستراتيجية الوطنية للولايات المتحدة الأمريكية لحماية الفضاء السيبراني: http://www.whitehouse.gov/.

3.C.I التقييم وتطوير البرنامج (5.B.I، 7.B.I، 8.B.I)

- أهداف مراقبة المعلومات والتكنولوجيا المتصلة بها (COBIT)، الإصدار 4.1:
http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981 (الملخص التنفيذي بالمجان؛ ويتعين التسجيل لتحميل النسخة الكاملة).
- إدارة أمن مكتبة البنية التحتية لتكنولوجيا المعلومات (ITIL):http://www.itil-itsm-world.com/ (مطلوب مقابل للتحميل).

- المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC)، السلسلة 27000، تكنولوجيا المعلومات – تقنيات الأمن – أنظمة إدارة أمن المعلومات: http://www.iso27001security.com/index.html.
- المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية، السلسلة 13335، تكنولوجيا المعلومات – تقنيات الأمن – إدارة أمن تكنولوجيا المعلومات والاتصالات – الجزء 1: مفاهيم ونماذج لإدارة أمن تكنولوجيا المعلومات والاتصالات: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066 (مطلوب رسوم للتحميل).
- المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية، السلسلة 17799، 2005، تكنولوجيا المعلومات – تقنيات الأمن – مدونة ممارسات لإدارة أمن المعلومات: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612 (مطلوب مقابل للتحميل).
- المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية، السلسلة 21827، هندسة أمن الأنظمة – نموذج اكتمال القدرات (SSE-CMM®): http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34731 (مطلوب مقابل للتحميل).
- مكتب تنمية الاتصالات بالاتحاد الدولي للاتصالات، دراسة بشأن الجوانب المالية لأمن الشبكات: البرمجيات الضارة والرسائل الاقتحامية: http://www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf.
- القرار 50 للجمعية العالمية لتقييس الاتصالات بالاتحاد الدولي للاتصالات بشأن "الأمن السيبراني" (المراجع في جوهانسبرغ، 2008): http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf.
- القرار 52 للجمعية العالمية لتقييس الاتصالات بالاتحاد الدولي للاتصالات بشأن "مكافحة الرسائل الاقتحامية ومحاربتها" (المراجع في جوهانسبرغ 2008): http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf.
- القرار 58 للجمعية العالمية لتقييس الاتصالات بالاتحاد الدولي للاتصالات (جوهانسبرغ، 2008): تشجيع تشكيل أفرقة وطنية للاستجابة للحوادث الحاسوبية، خاصة في البلدان النامية): http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf
- المعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة الأمريكية)، النشرة الخاصة رقم 800-12، مقدمة لأمن أجهزة الحاسوب: كتيب المعهد (فبراير، 1996): http://csrc.nist.gov/publications/nistpubs/800-12/.
- المعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة الأمريكية)، النشرة الخاصة رقم 800-30، دليل إدارة المخاطر لأنظمة تكنولوجيا المعلومات (يوليو، 2002): http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
- المعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة الأمريكية)، النشرة الخاصة رقم 800-53، ضوابط الأمن الموصى بها لأنظمة المعلومات الاتحادية (ديسمبر، 2007): http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf.
- المعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة الأمريكية)، مشروع النشرة الخاصة رقم 800-53A، دليل لتقييم ضوابط الأمن في أنظمة المعلومات الاتحادية (ديسمبر، 2007): http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-A.
- المعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة الأمريكية)، النشرة الخاصة رقم 800-50، بناء وعي عام بأمن تكنولوجيا المعلومات وبرنامج للتدريب (أكتوبر، 2003): http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf .

- المعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة الأمريكية)، النشرة الخاصة رقم 30-800، دليل إدارة المخاطر لأنظمة تكنولوجيا المعلومات (يوليو، 2002):
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
- إدارة أمن التهديدات والأصول الحرجة من الناحية التشغيلية وتقييم مواطن الضعف (OCTAVESM):
http://www.cert.org/octave/.

4.C.I جهات اتصال المساعدة الدولية (6.B.I)

- فريق العمل المعني بمكافحة الاحتيال على المعلومات الإلكترونية (APWG): http://www.antiphishing.org.
- منتدى أفرقة أمن الاستجابة في حالات الحوادث (FIRST): http://www.first.org.
- معهد مهندسي الكهرباء والإلكترونيات: http://www.ieee.org.
- فريق مهام هندسة الإنترنت: http://www.ietf.org.
- الفريق المعني بمكافحة إساءة استعمال تبادل الرسائل إلكترونياً: http://www.maawg.org.
- التحالف العالمي لخدمات تكنولوجيا المعلومات: http://www.witsa.org.
- الاتحاد العالمي لشركات الويب: http://www.w3c.org.

الجـــزء II: إقامة التعاون بين الحكومة والصناعة على الصعيد الوطني

1.C.II هياكل التعاون بين الحكومة والصناعة

دوليـــاً

- تحالف صناعة الأمن السيبراني: http://www.csialliance.org/about_csia/index.html.
- مجموعة أدوات منظمة التعاون والتنمية في الميدان الاقتصادي لمكافحة الرسائل الاقتحامية – شراكات تعاونية ضد الرسائل الاقتحامية: http://www.oecd-antispam.org/article.php3?id_article=243.
- تحالف القضاء على الرسائل الاقتحامية: http://stopspamalliance.org/.

إقليميـــاً

- الشرق الأوسط: تقرير عن المنتدى الرابع عشر لمجلس التعاون لدول الخليج العربية بشأن الحكومة الإلكترونية والخدمات الإلكترونية: http://www.zawya.com/Story.cfm/sidZAWYA20080529073202/SecMain/pagHomepage/chnAll%20Regional%20News/obj2A17E941-F5E0-11D4-867D00D0B74A0D7C/.

وطنيـــاً

- الشراكة الأسترالية بين الحكومة ودوائر الأعمال التجارية: شبكة تبادل المعلومات الموثوقة لحماية البنية التحتية الحرجة: http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_CriticalInfrastructureProtectionModellingandAnalysis(CIPMA).
- مراكز تبادل وتحليل المعلومات (ISAGs) ومجالس التنسيق بالولايات المتحدة الأمريكية:
  - مركز ISAC للخدمات المالية: http://www.fsisac.com/.
  - مركز ISAC للقطاع الكهربائي: http://www.esisac.com/.
  - مركز ISAC لتكنولوجيا المعلومات: http://www.it-isac.org.

- مركز ISAC للاتصالات: http://www.ncs.gov/ncc/.
- المجلس المعني باعتمادية الشبكات وقابلية تشغيلها بينياً (NRIC): http://www.nric.org/.
- اللجنة الاستشارية للأمن الوطني والاتصالات (NSTAC): http://www.ncs.gov/nstac/nstac.html.

- هيئة التعاون بين الحكومة والصناعة في الولايات المتحدة الأمريكية بشأن المعايير: المعهد الوطني الأمريكي للمعايير – الفريق الوطني لمعايير الأمن: http://www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3.
- الورقة البيضاء لرابطة تكنولوجيا المعلومات بأمريكا بشأن أمن المعلومات: http://www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf.
- المجلس الأمريكي لتنسيق قطاع تكنولوجيا المعلومات (SCC): http://www.it-scc.org.
- الشراكة الوطنية الأمريكية للأمن السيبراني: http://www.cyberpartnership.org/.
- المجلس الوطني الأمريكي لأمن المعلومات (NIAC)، تقرير عن فريق العمل المعني بنموذج شراكة في القطاع: http://itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf.
- الخطة الوطنية الأمريكية لحماية البنية التحتية: http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.
- خطط أمريكية محددة حسب القطاع: http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm.
- خطة أمريكية خاصة بقطاع تكنولوجيا المعلومات: http://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf.
- الإدارة الوطنية الأمريكية للاتصالات والمعلومات: http://www.ntia.doc.gov/.

2.C.II تبادل معلومات الأمن السيبراني

دولياً

- فريق العمل المعني بمكافحة إساءة استعمال تبادل الرسائل إلكترونياً: http://www.maawg.org.

وطنياً

- المعهد الوطني الأمريكي للمعايير والتكنولوجيا، مركز أمن وأبحاث الحاسوب: http://csrc.nist.gov/.
- فريق الاستجابة الأمريكي للطوارئ الحاسوبية US-CERT، النظام الوطني للإنذار السيبراني: http://www.us-cert.gov/cas/.

3.C.II زيادة الوعي والتوعية: أدوات من أجل الحكومات ودوائر الأعمال التجارية

دولياً

- برنامج خلق وعي أمني: http://www.gideonrasmussen.com/article-01.html.
- مركز موارد ومنشورات أمن الإنترنت المعنية بأمن المؤسسات: http://www.cisecurity.org/resources.html.
- استراتيجيات مشتركة للوعي الأمني: http://articles.techrepublic.com.com/5100-10878_11-5193710.html.
- دليل موحد للأمن السيبراني للأعمال التجارية الصغيرة: http://www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm.

- موارد الوعي الأمني لرابطة EDUCAUSE للحكومات والصناعة:
http://www.educause.edu/Security%20Task%20Force/CybersecurityAwarenessResource/Browse SecurityAwarenessResourc/8770?time=1215527945.
- مبادرات الوعي بأمن المعلومات للوكالة الأوروبية لأمن الشبكات والمعلومات (متاحة بعدة لغات):
http://www.enisa.europa.eu/Pages/05_01.htm.
- أساليب الأنتربول في مجال أمن تكنولوجيا المعلومات والوقاية من جرائمها (للوقاية من الجرائم في الشركات):
http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp.
- قائمة الأنتربول للشركات الضالعة في جرائم تكنولوجيا المعلومات:
http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp.
- ملصقات شركة NoticeBored للوعي الأمني: http://www.noticebored.com/html/posters.html.
- مجموعة أدوات منظمة التعاون والتنمية في الميدان الاقتصادي لمكافحة الرسائل الاقتحامية – التعليم والوعي: http://www.oecd-antispam.org/article.php3?id_article=242.
- مؤسسة إدارة النظام وربطه شبكياً وتأمينه (SANS)، موارد السياسات الأمنية: http://www.sans.org/resources/policies/.
- مجموعة أدوات الوعي الأمني – موقع حرب المعلومات:
http://www.iwar.org.uk/comsec/resources/sa-tools/.
- الشراكة الوطنية الأمريكية للأمن السيبراني – زيادة الوعي بالنسبة للأعمال التجارية الصغيرة ومراكز مواردها:
http://www.cyberpartnership.org/init-aware.html.

وطنيـــاً

- اللجنة الفيدرالية الأمريكية للتجارة: http://www.ftc.gov/infosecurity.
- النشرة رقم 800-50 للمعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة الأمريكية)، برنامج الوعي الأمني والتدريب:
http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

الجـــزء III: ردع الجريمة السيبرانية/الأساس القانوني والإنفاذ

دوليـــاً

- المجلس الأوروبي: الاتفاقية المعنية بالجرائم السيبرانية (2001):
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp.
- مبادئ الجرائم عالية التقنية لمجموعة الدول الثماني (G8):
http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html.
- بوابة الأمن السيبراني للاتحاد الدولي للاتصالات: مواد أساسية بشأن تنسيق النهج القانونية الوطنية والتنسيق القانوني الدولي والإنفاذ: http://www.itu.int/cybersecurity/gateway/laws_legislation.html.
- الاتحاد الدولي للاتصالات/شعبة المعلومات، مجموعة أدوات تنظيم تكنولوجيا المعلومات والاتصالات:
http://www.ictregulationtoolkit.org/.
- منشور الاتحاد الدولي للاتصالات بشأن فهم الجريمة السيبرانية: دليل للبلدان النامية:
http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html
- مجموعة أدوات الاتحاد الدولي للاتصالات بشان تشريعات الجريمة السيبرانية:
http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

- موارد الأنتربول الخاصة بجرائم تكنولوجيا المعلومات:
http://www.interpol.com/Public/TechnologyCrime/.
- النهج التنظيمية لمكافحة الرسائل الاقتحامية لمنظمة التعاون والتنمية في الميدان الاقتصادي:
http://www.oecd-antispam.org/article.php3?id_article=1.
- مجموعة أدوات مكافحة الرسائل الاقتحامية لمنظمة التعاون والتنمية في الميدان الاقتصادي:
http://www.oecd-antispam.org/article.php3?id_article=265.
- قرار الجمعية العامة للأمم المتحدة رقم 55/63 بشأن "مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية":
http://www.un.org/Depts/dhl/resguide/r55.htm.
- قرار الجمعية العامة للأمم المتحدة رقم 56/121 بشأن "مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية":
http://www.un.org/Depts/dhl/resguide/r56.htm.
- معهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة (UNICRI)، موارد لتحسين المعارف وإقامة شراكات جديدة لمواجهة الجرائم السيبرانية: http://www.unicri.it/.
- قوانين نموذجية للجنة الأمم المتحدة للقانون التجاري الدولي (UNCITRAL) بخصوص التجارة الإلكترونية والتوقيعات الإلكترونية:
http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html.
- موارد مكتب الأمم المتحدة المعني بالمخدرات والجريمة: http://www.unodc.org/.

إقليميـــاً

- رابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC): وثائق وعروض وبيانات وزارية خاصة بالجرائم السيبرانية:
http://www.apectelwg.org/.
- إعلان القاهرة الصادر عن المؤتمر المعني بالجرائم السيبرانية:
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf.
- قانون نموذجي لكومنولث الدول المستقلة بشأن الحاسوب والجرائم الحاسوبية:
http://www.thecommonwealth.org/Internal/38061/documents/.
- المجلس الأوروبي: الاتفاقية المعنية بالجرائم السيبرانية (2001):
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp.
- منظمة الدول الأمريكية: بوابة التعاون بين البلدان الأمريكية بشأن الجرائم السيبرانية:
http://www.oas.org/juridico/english/cyber.htm.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: كيف يحقق مكتب التحقيقات الفيدرالي (FBI) في الجرائم الحاسوبية:
http://www.cert.org/tech_tips/FBI_investigates_crime.html.
- قانون الجرائم السيبرانية: مسح عالمي للتشريعات الخاصة بالجرائم السيبرانية:
http://www.cybercrimelaw.net/index.html.
- المجلس الأوروبي: مسح للتشريعات الخاصة بالجرائم السيبرانية في بلدان المجلس:
http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/Legprofiles.asp#TopOfPage.

- شركة ميكروسوفت: "تحليل للتشريعات في منطقة آسيا والمحيط الهادئ: القوانين الحالية والوشيكة بشأن السلامة الإلكترونية والجرائم السيبرانية": http://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf.
- قوانين مكافحة الرسائل الاقتحامية لدى الدول الأعضاء في منظمة التعاون والتنمية في الميدان الاقتصادي: http://www.oecd-antispam.org/countrylaws.php3.
- "نماذج للتشريعات السيبرانية لدى الدول الأعضاء في اللجنة الاقتصادية والاجتماعية لغرب آسيا (ESCWA)" الصادرة عن الأمم المتحدة: http://www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf .
- موقع الويب لقسم الجرائم الحاسوبية والملكية الفكرية بوزارة العدل الأمريكية (USDOJ): http://www.cybercrime.gov.
- كتيب وزارة العدل الأمريكية (USDOJ) بشأن محاكمة الجرائم الحاسوبية (الفصل 1 – قانون الاحتيال وإساءة الاستعمال في مجال الحاسوب): http://www.cybercrime.gov/ccmanual/.
- دائرة الأمن الخاص الأمريكية – أفضل الممارسات في الحصول على أدلة إلكترونية: http://www.forwardedge2.com/pdf/bestPractices.pdf.

الجـــزء IV: إنشاء منظمة وطنية لإدارة الحوادث: المراقبة والإنذار والاستجابة والإنعاش

1.C.IV خطط الاستجابة الوطنية وفرق الاستجابة الوطنية لحوادث الأمن الحاسوبي

دوليـــاً

- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية (CERT/CC) بجامعة كارينغي ميلون في الولايات المتحدة الأمريكية: http://www.cert.org/csirts/.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: قائمة بإجراءات إنشاء فريق استجابة وطني لحوادث الأمن الحاسوبي: http://www.cert.org/csirts/action_list.html.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: إنشاء فريق استجابة وطني لحوادث الأمن/الحاسوبي عملية للبدء: http://www.cert.org/csirts/Creating-A-CSIRT.html.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: تحديد عمليات إدارة الحوادث لفرق الاستجابة الوطنية لحوادث الأمن الحاسوبي: عمل جار: http://www.cert.org/archive/pdf/04tr015.pdf.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: الأسئلة التي توجه كثيراً إلى فرق الاستجابة لحوادث الأمن الحاسوبي: http://www.cert.org/csirts/csirt_faq.html.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: كتيب بخصوص فرق الاستجابة لحوادث الأمن الحاسوبي: http://www.cert.org/archive/pdf/csirt-handbook.pdf.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: قياس قدرات إدارة الحوادث، الإصدار 0.1: http://www.cert.org/archive/pdf/07tr008.pdf.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: نماذج تنظيمية لفرق الاستجابة لحوادث الأمن الحاسوبي: http://www.cert.org/archive/pdf/03hb001.pdf.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: خدمات فرق الاستجابة لحوادث الأمن الحاسوبي: http://www.cert.org/csirts/services.html.

- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: اختيار العاملين في فريق الاستجابة لحوادث الأمن الحاسوبي لديك – ما هي المهارات الأساسية المطلوبة؟: http://www.cert.org/csirts/csirt-staffing.html.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: وضع العمل بالنسبة لفريق الاستجابة لحوادث الأمن الحاسوبي: http://www.cert.org/archive/pdf/03tr001.pdf.
- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: خطوات إنشاء الفرق الوطنية للاستجابة لحوادث الأمن الحاسوبي: http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.
- بيئة التدريب الافتراضي (VTE) لمركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: http://www.vte.cert.org/.
- الوكالة الأوروبية لأمن الشبكات والمعلومات: نهج خطوة بخطوة بشأن كيفية تشكيل فريق استجابة لحوادث الأمن الحاسوبي: http://www.enisa.europa.eu/pages/05_01.htm.
- هيئة التعاون بين ITU وIMPACT والموارد ذات الصلة: http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html
- نموذج معد لفريق استجابة لحوادث الأمن الحاسوبي – معلومات عن تشكيل فريق استجابة لحوادث الأمن السيبراني: http://www.govcert.nl/render.html?it=69.
- مركز حماية البنية التحتية الوطنية بالمملكة المتحدة: مجموعة أدوات لنقطة الإنذار وتقديم المشورة والإبلاغ (WARP): http://www.warp.gov.uk/.

إقليميـــاً

- فريق الاستجابة للطوارئ الحاسوبية لمنطقة آسيا والمحيط الهادئ: http://www.apcert.org/index.html.
- الموارد الشبكية لفريق الاستجابة الأوروبي للطوارئ الحاسوبية: http://www.ecsirt.net/.
- فريق أفرقة الاستجابة الحكومية الأوروبية للطوارئ الحاسوبية: http://www.egc-group.org/.

وطنيـــاً

- أستراليا: الفريق الأسترالي للاستجابة للطوارئ الحاسوبية: http://www.auscert.org.au.
- النمسا: فريق الاستجابة للطوارئ الحاسوبية بالنمسا: http://www.cert.at.
- البرازيل: فريق الاستجابة للطوارئ الحاسوبية بالبرازيل: http://www.cert.br/.
- شيلي: فريق الاستجابة للطوارئ الحاسوبية بشيلي: http://www.clcert.cl/.
- الصين: مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية بالصين: http://www.cert.org.cn/.
- فنلندا: فريق الاستجابة للطوارئ الحاسوبية بفنلندا: http://www.cert.fi.
- هنغاريا: فريق الاستجابة للطوارئ الحاسوبية بهنغاريا: http://www.cert-hungary.hu.
- الهند: فريق الاستجابة للطوارئ الحاسوبية بالهند: http://www.cert-in.org.in.
- إيطاليا: فريق الاستجابة للطوارئ الحاسوبية بإيطاليا: http://security.dico.unimi.it/.
- اليابان: مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية باليابان: http://www.jpcert.or.jp/.
- كوريا: مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية بكوريا: http://www.krcert.or.kr/.
- ماليزيا: فريق الاستجابة للطوارئ الحاسوبية بماليزيا: http://www.cybersecurity.org.my.
- هولندا: http://www.csirt.dk/.
- بولندا: فريق الاستجابة للطوارئ الحاسوبية ببولندا: http://www.cert.pl/.

- سلوفينيا: فريق الاستجابة للطوارئ الحاسوبية بسلوفينيا: http://www.arnes.si/en/si-cert/.
- سنغافورة: فريق الاستجابة للطوارئ الحاسوبية بسنغافورة: http://www.singcert.org.sg/.
- السويد: مركز حوادث تكنولوجيا المعلومات بالسويد: http://www.sitic.se.
- سويسرا: مركز MELANI: http://www.melani.admin.ch.
- تايلاند: فريق الاستجابة للطوارئ الحاسوبية بتايلاند: http://www.thaicert.nectec.or.th/.
- تونس: المركز TCC التابع لفريق الاستجابة للطوارئ الحاسوبية: http://www.ansi.tn/en/about_cert-tcc.htm.
- قطر: http://www.qcert.org.
- الإمارات العربية المتحدة: http://aecert.ae/.
- خطة الاستجابة الوطنية الأمريكية: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml.
- الولايات المتحدة الأمريكية: فريق الاستجابة الأمريكي للطوارئ الحاسوبية: http://www.us-cert.gov/.
- مواقع الويب للفرق الوطنية الأخرى للاستجابة للطوارئ الحاسوبية/الاستجابة لحوادث الأمن الحاسوبي.

2.C.IV التعاون وتبادل المعلومات

دولياً

- مركز تنسيق فرق الاستجابة للطوارئ الحاسوبية: مواطن الضعف الأمنية والحلول: http://www.cert.org/nav/index_red.html.
- مركز تبادل المعلومات بشأن أدوات التعامل مع الحوادث (CHIHT): http://chiht.dfn-cert.de/.
- موارد منتدى الاستجابة للحوادث والفرق الأمنية (FIRST): http://www.first.org/.
- موارد خدمات دعم الأمن لموردي خدمات الإنترنت: http://www.donelan.com/ispsupport.html.
- بوابة الاتحاد الدولي للاتصالات للأمن السيبراني: مواد أساسية تتعلق بمراقبة الحوادث والإنذار والاستجابة بشأنها: http://www.itu.int/cybersecurity/gateway/watch_warning.html.
- نظام إنذار آمن لتكنولوجيا المعلومات من أجل الأعمال التجارية الصغيرة والأفراد: http://www.itsafe.gov.uk/.
- منظمة التعاون والتنمية في الميدان الاقتصادي: مجموعة أدوات مكافحة الرسائل الاقتحامية: http://www.oecd-antispam.org/article.php3?id_article=265.

إقليمياً

- رابطة شبكات البحوث والتعليم عبر أوروبا (TERENA): http://www.terena.org/.

وطنياً

- هولندا: خدمة الإنذار الوطنية الهولندية: http://www.waarschuwingsdienst.nl/render.html?cid=106.
- المملكة المتحدة (مركز حماية البنية التحتية الوطنية): مجموعة أدوات نقطة الإنذار وتقديم المشورة والإبلاغ (WARP): http://www.warp.gov.uk/.
- مركز تبادل معلومات تكنولوجيا المعلومات وتحليلها بالولايات المتحدة الأمريكية: https://www.it-isac.org/.

- المجلس الأمريكي لتنسيق قطاع تكنولوجيا المعلومات (ISCC): تكنولوجيا المعلومات: البنية التحتية الحرجة وخطة الموارد الرئيسية الخاصة بالقطاع:
http://www.it-scc.org/documents/itscc/Information_Technology_SSP_2007.pdf.
- المعهد الوطني للمعايير والتكنولوجيا (NIST) بالولايات المتحدة الأمريكية: http://csrc.nist.gov/.

3.C.IV معلومات/أدوات مواطن الضعف والتقنيات

- بناء الأمن بجمع المعلومات الخاصة بأمان وأمن البرمجيات للمساعدة في إنشاء أنظمة آمنة:
https://buildsecurityin.us-cert.gov/daisy/bsi/home.html.
- قائمة مشتركة بمواطن الضعف والتعرض (CVE): http://www.cve.mitre.org/about/.
- لغة مفتوحة لتقييم مواطن الضعف (OVAL): http://oval.mitre.org/.
- قاعدة البيانات الوطنية الأمريكية لمواطن الضعف (NVD) بالنسبة للبرمجيات: http://nvd.nist.gov/nvd.cfm.

الجـــزء V: الترويج لثقافة وطنية للأمن السيبراني

1.C.V الأنظمة والشبكات الحكومية (1.B.V و2.B.V و7.B.V)

دوليـــاً

- خط العمل جيم5 العالمية لمجتمع المعلومات، خطة عمل:
http://www.itu.int/wsis/implementation/index.html.
- جدول الأعمال العالمي للاتحاد الدولي للاتصالات بشأن الأمن السيبراني: http://www.itu.int/osg/csd/cybersecurity/gca/.
- الاجتماع المواضيعي المعني بمكافحة الرسائل الاقتحامية للقمة العالمية لمجتمع المعلومات للاتحاد الدولي للاتصالات:
http://www.itu.int/osg/spu/spam/meeting7-9-04/index.html.
- خط العمل جيم5 للقمة العالمية لمجتمع المعلومات، تقرير رئيس الاجتماع الأول:
http://www.itu.int/osg/spu/cybersecurity/2006/chairmansreport.pdf.
- خط العمل جيم5 للقمة العالمية لمجتمع المعلومات، تقرير رئيس الاجتماع الثاني:
http://www.itu.int/wsis/docs/geneva/official/poa.html.
- جدول أعمال الاجتماع الثاني طبقاً للتقديمات:
http://www.itu.int/osg/csd/cybersecurity/WSIS/meetingAgenda.html.
- خط العمل جيم5 للقمة العالمية لمجتمع المعلومات، تقرير الاجتماع الثالث:
http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.
- جدول أعمال الاجتماع الثالث طبقاً للتقديمات:
http://www.itu.int/osg/csd/cybersecurity/WSIS/agenda-3_new.html.
- شركة ميكروسوفت: خصوصية المحاسبات، معلومات سلامة وأمن الإنترنت من أجل صانعي السياسات في جميع أنحاء العالم: http://www.microsoft.com/mscorp/twc/policymakers_us.mspx.
- منظمة التعاون والتنمية في الميدان الاقتصادي، بوابة ثقافة الأمن مع مواردها: http://www.oecd.org/sti/cultureofsecurity.
- منظمة التعاون والتنمية في الميدان الاقتصادي "مبادئ توجيهية بشأن أمن أنظمة وشبكات المعلومات: نحو ثقافة أمنية" (2002):
http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.
- منظمة التعاون والتنمية في الميدان الاقتصادي: "مبادئ توجيهية بشأن حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود" (1980):
http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html.

- "تقرير منظمة التعاون والتنمية في الميدان الاقتصادي بشأن الترويج لثقافة لأمن أنظمة وشبكات المعلومات في بلدان المنظمة" (2005): http://www.oecd.org/dataoecd/16/27/35884541.pdf.
- كتيب أمن تكنولوجيا المعلومات للبنك الدولي – أمن المعلومات والسياسات الحكومية: http://www.infodev-security.net/handbook/part4.pdf.
- القرار رقم 57/239 للجمعية العامة للأمم المتحدة (المرفقات أ وب): http://www.un.org/Depts/dhl/resguide/r57.htm.

إقليميـــاً

- الوكالة الأوروبية لأمن الشبكات والمعلومات: "مبادرات التوعية بأمن المعلومات: الممارسات الحالية وقياس النجاح" (2007): http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf.
- الوكالة الأوروبية لأمن الشبكات والمعلومات "دليل للمستعملين: كيفية زيادة الوعي بأمن المعلومات" (2006): http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf.
- المصدر الأوروبي لمعلومات سلامة الإنترنت (InSafe): http://www.saferinternet.org/ww/en/pub/insafe/index.htm.
- منظمة الدول الأمريكية (OAS): استراتيجية البلدان الأمريكية لمكافحة التهديدات التي يتعرض لها الأمن السيبراني: نهج متعدد الأبعاد ومتعدد الأنظمة لإرساء ثقافة للأمن السيبراني (تذييلات مفصلة) (2004): http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.

وطنيـــاً

- البرازيل: موارد مكتب مكافحة الرسائل الاقتحامية: http://antispam.br/
- البرازيل: مبادئ توجيهية بشأن سلامة الإنترنت للجنة التوجيه البرازيلية المعنية بالأنترنت – CGI.br: http://cartilha.cert.br/
- مبادرات منظمة التعاون والتنمية في الميدان الاقتصادي للترويج لثقافة للأمن (لكل بلد): http://www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html.
- موقع فريق الاستجابة للطوارئ الحاسوبية بالولايات المتحدة الأمريكية: http://www.us-cert.gov/.
- خطة البحث والتطوير لحماية البنية التحتية الوطنية الحرجة لوزارة الأمن الداخلي بالولايات المتحدة الأمريكية: http://www.dhs.gov/xres/programs/gc_1159207732327.shtm.
- الممارسات الأمنية للوكالة الاتحادية بالولايات المتحدة الأمريكية: http://csrc.nist.gov/fasp/.
- لوائح الاقتناء الاتحادية بالولايات المتحدة الأمريكية (FAR)، الأجزاء 1 و2 و7 و11 و39: http://www.acqnet.gov/FAR/.
- خطة البحث والتطوير الاتحادية بالولايات المتحدة الأمريكية بخصوص الأمن السيبراني وأمن المعلومات: http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf.
- المجلس الاستشاري بالولايات المتحدة الأمريكية لأمن المعلومات والخصوصية: http://csrc.nist.gov/ispab/.
- التوجيه الرئاسي للأمن الداخلي بالولايات المتحدة الأمريكية، التوجيه رقم HSPD-7، "تحديد البنى التحتية الحرجة وترتيب أولوياتها وحمايتها": http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.
- مركز تبادل المعلومات وتحليلها للولايات المتعددة بأمريكا: http://www.msisac.org/.
- الاستراتيجية الوطنية الأمريكية لتأمين الفضاء السيبراني: http://www.whitehouse.gov/pcipb/.
- تقرير اللجنة الاستشارية لرئيس الولايات المتحدة الأمريكية المعنية بتكنولوجيا المعلومات بخصوص أولويات البحوث في مجال الأمن السيبراني: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

2.C.V منظمات الأعمال التجارية والقطاع الخاص (3.B.V و5.B.V و7.B.V)

- حركة إنترنت آمنة في البرازيل: http://www.internetsegura.org/
- مركز Cisco للأمن (قسم أفضل الممارسات): http://tools.cisco.com/security/center/home.x.
- الحاسوبية المعتمدة لشركة ميكروسوفت: http://www.microsoft.com/mscorp/twc/default.mspx.
- المواد التدريسية للمركز الوطني للتدريب والتعليم في مجال ضمان نوعية المعلومات (NIATEC): http://niatec.info/index.aspx?page=105.
- دليل أمن تكنولوجيا المعلومات للبنك الدولي – الأمن للمنظمات: http://www.infodev-security.net/handbook/part3.pdf.
- ملصقات وبطاقات إعلامية لأماكن العمل صادرة عن فريق الاستجابة للطوارئ الحاسوبية بالولايات المتحدة الأمريكية: http://www.uscert.gov/reading_room/distributable.html.
- ممارسات "العاصفة السيبرانية" لوزارة الأمن الداخلي/دوائر الصناعة بالولايات المتحدة الأمريكية: http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm.

3.C.V الأفراد والمجتمع المدني (4.B.V و6.B.V و7.B.V)

- البرازيل: منظمة SaferNet بالبرازيل: http://www.safernet.org/
- لتكن آمناً على الخط (الاستخدام الأكثر أمناً للخدمات على الإنترنت – SUSI): http://www.besafeonline.org/.
- إرشادات أمنية لمنظمة CASEScontact: http://casescontact.org/tips_list.php.
- موارد الشبكة الدولية للأطفال Childnet: http://www.childnet-int.org.
- مبادرة السلام السيبراني: http://www.cyberpeaceinitiative.org/.
- موقع CyberTipline: تعليم المراهقين كيفية تحقيق الأمان على الخط: http://tcs.cybertipline.com/.
- موارد نطاق أمان الإنترنت للأطفال والوالدين: http://www.internetsafetyzone.co.uk/root/.
- القائمة المرجعية الخاصة للأنتربول بشأن جرائم تكنولوجيا المعلومات: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/privateChecklist.asp.
- مبادرة الاتحاد الدولي للاتصالات لحماية الأطفال على الخط والمبادئ التوجيهية ذات الصلة: http://www.itu.int/cop/
- أدوات منظمة GetNetWise للأسر: http://kids.getnetwise.org/tools/.
- موقع OnGuard على الخط – إرشادات للحماية من الاحتيال: http://onguardonline.gov/index.html.
- موقع MakeItSecure – معلومات عن أخطار الإنترنت الشائعة: http://www.makeitsecure.org/en/index.html.
- مبادرات الأمن الإلكتروني الماليزية: http://www.esecurity.org.my/.
- موقع NetSmartz: موارد للوالدين والأوصياء: http://www.netsmartz.org/netparents.htm.
- شبكة Netsafe النيوزيلندية: http://www.netsafe.org.nz.
- الخط الساخن SafeLine للإبلاغ عن المحتويات غير القانونية: http://www.safeline.gr/.
- رسوم كاريكاتورية بخصوص الأمن: http://www.securitycartoon.com/.
- فلتظل آمناً على الخط: http://www.staysafeonline.info/.
- منظمة WiredSafety: http://www.wiredsafety.org/.
- دليل أمن تكنولوجيا المعلومات للبنك الدولي – الأمن للأفراد: http://www.infodev-security.net/handbook/part2.pdf.

- موارد مركز الحماية ضد استغلال الأطفال والحماية على الخط بالمملكة المتحدة: http://www.ceop.gov.uk/.
- موقع فلتكن آمناً على الخط للمملكة المتحدة: http://www.getsafeonline.org/.
- فريق الاستجابة للطوارئ الحاسوبية الولايات المتحدة للمستعملين غير التقنيين: http://www.us-cert.gov/nav/nt01/.

وغير ذلك من المبادرات الدولية والإقليمية والوطنية لزيادة الوعي لدى المستعملين النهائيين

طبع في سويسـرا
جنيف، 2010
إعداد الصور: الاتحاد الدولي للاتصالات، مكتبة الصور