برنامج الأمن السيبراني لقطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات

الرقم القياسي العالمي للأمن السيبراني (الإصدار الخامس) – GCIv5

الاستبيان النهائي المنقَّح

جدول المحتويات

الإصدار الخامس من الرقم القياسي العالمي للأمن السيبراني (GCIv5) - سِجل التغييرات، والتعاريف

الاستبيان المنقَّح للإصدار الخامس من الرقم القياسي العالمي للأمن السيبراني (GCIv5)، بما في ذلك التدابير المتصلة بالإصدارات السابقة للرقم القياسي العالمي للأمن السيبراني، وتعاريف المصطلحات الأساسية، والمسوغات المبرِّرة للمؤشرات/الإطار

دليل الرموز

الرمز- [رقم الإصدار] – يرمز إلى كل من الأسئلة/الأقسام الواردة في رقم الإصدار المعني من الرقم القياسي GCI.

الأساس المنطقي- [رقم الإصدار] –يرمز إلى جميع المسوغات المنطقية المقدمة بشأن أسئلة الاستبيان أو المسوغات المتعلقة بخلفيات هذه الأسئلة في الإصدار المعني من الرقم القياسي GCI.

مؤشرات الرقم القياسي العالمي للأمن السيبراني بحسب دعائمه

التدابير القانونية

الأساس المنطقي-الإصدار الخامس من الرقم القياسي العالمي للأمن السيبراني (GCIv5): يمثل التشريع تدبيراً حاسماً يُقر إطاراً منسقاً للكيانات لتُلزم أنفسها بقاعدة تنظيمية مشتركة، سواء في مسألة حظر سلوكيات جُرمية محددة أو فيما يتعلق بتحديد المقتضيات التنظيمية الدنيا. إذ تحدد الأُطرُ القانونية أدوار مختلف أصحاب المصلحة وواجباتهم ومسؤولياتهم. ويمكن تعريف قانون الأمن السيبراني بالإجابة على خمسة أسئلة أساسية، هي: "1) ما هو الشيء الذي نؤمِّنه؟؛ و2) أين نؤمِّنه وما هي الجهات التي نؤمِّنها؟؛ و3) كيف نؤمِّن هذا الشيء؟؛ و4) متى نؤمِّنه؟، و5) لِمَ نؤمِّنه؟"[1] وأمن البيانات جزء مهم من الأمن السيبراني، لكنه ليس مكوِّنه الوحيد، ذلك أن الأمن السيبراني يشمل "الأنظمة التي تخزَّن عليها البيانات والشبكات التي يجري تناقل البيانات عليها."[2]

وتُتيح التدابير القانونية أيضاً للبلدان إنشاء الآليات الأساسية للاستجابة للخروقات، بالتحقيق في الجرائم ومقاضاة مرتكبيها وتوقيع عقوبات لمخالفة القوانين أو خرقها. فالقوانين تحمي الأمن العام وتكفل حقوق المواطنين وتحميها من انتهاك الغير إياها وتضمن الحماية من إساءة استخدام أحدث التكنولوجيات. ويُقر الإطار التشريعي المعايير السلوكية الدنيا الشاملة، الواجبة التطبيق على الجميع، والتي يمكن أن يُبنى عليها المزيد من القدرات الأمنية السيبرانية. ففي النهاية، تكمن غاية هذه الدعامة من دعائم الرقم القياسي العالمي للأمن السيبراني في تمكين البلدان من وضع تشريعات كافية من أجل تنسيق ممارساتها خارج حدودها الوطنية، وفي تهيئة بيئة مؤاتية لتنفيذ تدابير مشتركة، بما ييسر مكافحة الجريمة السيبرانية دولياً.

ويمكن قياس البيئة القانونية بمدى وجود المؤسسات والأُطر القانونية المعنية بالأمن السيبراني والجريمة السيبرانية، وعددها. وتشمل مجموعة المؤشرات المتفرعة من هذه الدعامة مؤشرات الأداء التالية:

1 قانون الجريمة السيبرانية

الرمز- GCIv5: Legal1

الأساس المنطقي-GCIv5: تحدد قوانين الجريمة السيبرانية أفعال النفاذ، والتدخل، والاعتراض، غير المصرح به (أي الممارَس بغير وجه حق) التي تستهدف الحواسيب والأنظمة والبيانات. وقد تتخذ هذه القوانين شكل قانون موضوعي و/أو إجرائي، أو قانون عام و/أو خاص، أو قانون مشترك أو سوابق قضائية أو قانون تشريعي أو قانون إداري أو غيرها من أشكال القانون المعمول بها.

1.1 قوانين السلوكيات غير المشروعة على الإنترنت

الرمز- GCIv5: Legal1.1

الأساس المنطقي-GCIv5: قد تؤثر العديد من السلوكيات الممارسة على شبكة الإنترنت تأثيراً سلبياً على سلامة الأنشطة المنفذة عبر الإنترنت (يُشار إليها فيما بعد باسم "أنشطة الإنترنت") وإمكانية الاطمئنان إليها. وقد أُشير إلى بعض هذه السلوكيات في اتفاقات دولية من قبيل اتفاقية مجلس أوروبا لمكافحة الجريمة السيبرانية ("اتفاقية بودابست"). ويمكن للتشريعات النافذة لمكافحة هذه السلوكيات أن تقدم مبادئ توجيهية واضحة لإنفاذ القانون وترشد الأحكام القضائية وتوفر الانتصاف للأطراف المتضررة من تلك السلوكيات.

1 https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022

2 https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022

1.1.1 هل يعتمد بلدكم تشريعاً نافذاً لمكافحة النفاذ غير القانوني إلى الأجهزة، والأنظمة الحاسوبية، والبيانات؟

الرمز- GCIv5: Legal1.1.1

الأساس المنطقي-GCIv5: قد تؤثر العديد من السلوكيات الممارسة على الإنترنت تأثيراً سلبياً على سلامة أنشطة الإنترنت وإمكانية الاطمئنان إليها. وتشكل التشريعات أحد سبل التصدي لهذه السلوكيات. والقصد من هذا السؤال قياس مدى وجود تشريعات محددة نافذة لدى البلد، عند الرد على هذا الاستبيان، لمكافحة النفاذ غير القانوني إلى الأجهزة، والأنظمة الحاسوبية، والبيانات، الذي قد يؤدي بدوره إلى وقوع أضرار أو خسائر منها الإضرار بالخصوصية أو الممتلكات أو المساس بالكرامة الشخصية. ولا يُعتد بالتشريعات المخطط لسنِّها والتشريعات المصاغة وغير النافذة حالياً للحصول على نقطة كاملة في هذا السؤال.

2.1.1 هل يعتمد بلدكم تشريعاً نافذاً لمكافحة التدخل غير القانوني (بإدخال بيانات و/أو تغيير البيانات و/أو إزالتها) في الأجهزة، والبيانات، والأنظمة الحاسوبية؟

الرمز- GCIv5 Legal1.1.2

الأساس المنطقي-GCIv5: قد تؤثر العديد من السلوكيات الممارسة على الإنترنت تأثيراً سلبياً على سلامة أنشطة الإنترنت وإمكانية الاطمئنان إليها. وتشكل التشريعات إحدى سبل التصدي لهذه السلوكيات. والقصد من هذا السؤال قياس مدى وجود تشريعات محددة نافذة لدى البلد، عند الرد على هذا الاستبيان، لمكافحة التدخل غير المشروع (بإدخال بيانات و/أو تغيير البيانات و/أو إزالتها) في الأجهزة، والبيانات، والأنظمة الحاسوبية. ولا يُعتد بالتشريعات المخطط لسنِّها والتشريعات المصاغة وغير النافذة حالياً للحصول على نقطة كاملة في هذا السؤال.

3.1.1 هل يعتمد بلدكم تشريعاً نافذاً لمكافحة الاعتراض غير القانوني للأجهزة، والبيانات، والأنظمة الحاسوبية؟

الرمز- GCIv5 Legal1.1.3

الأساس المنطقي-GCIv5: قد تؤثر العديد من السلوكيات الممارسة على الإنترنت تأثيراً سلبياً على سلامة أنشطة الإنترنت وإمكانية الاطمئنان إليها. وتشكل التشريعات إحدى سبل التصدي لهذه السلوكيات. والقصد من هذا السؤال قياس مدى وجود تشريعات محددة نافذة لدى البلد، عند الرد على هذا الاستبيان، لمكافحة الاعتراض غير القانوني للأجهزة والبيانات والأنظمة الحاسوبية. ولا يُعتد بالتشريعات المخطط لسنِّها والتشريعات المصاغة وغير النافذة حالياً للحصول على نقطة كاملة في هذا السؤال.

4.1.1 هل يعتمد بلدكم قانوناً موضوعياً لحماية الهوية على الإنترنت؟

الرمز- GCIv5 Legal1.1.4

الأساس المنطقي-GCIv5: مع تزايد كم أنشطة الإنترنت التي تستلزم ممارستها قدرة الأشخاص على تعريف هوياتهم بطرق موثوقة، تساعد القوانين، سواء الخاصة بأنشطة الإنترنت أو المُضمَّنة في القوانين الأخرى المتعلقة بالهوية، أو غيرها، في إرساء الأساس القانوني لاستخدام الهوية وإدارتها وسلوكياتها على الإنترنت.

2.1 هل يعتمد بلدكم تشريعاً نافذاً لمكافحة التزوير الحاسوبي (كالقرصنة الإلكترونية/انتهاك حقوق المؤلف)؟

الرمز- GCIv5 Legal1.2

الأساس المنطقي-GCIv5: تشكل الثقة أساس النظام الإيكولوجي الرقمي، لكنَّ التزوير الحاسوبي يقوِّضها. "ويشمل التزوير الحاسوبي تعمُّد إدخال بيانات إلى الحاسوب أو تغيير بيانات الحاسوب أو حذفها أو إزالتها، بغير وجه حق، بما يؤدي إلى إنتاج بيانات غير أصلية بقصد أن يُنظر فيها أو يُتصرَّف بالاستناد إليها لأغراض قانونية وكأنها البيانات الأصلية، بصرف النظر عن مدى إمكانية قراءة هذه البيانات وفهمها، مباشرةً".[3] "ومثال ذلك أن يقوم الجاني بتعديل رسالة إلكترونية أصلية واردة من مؤسسة مالية ثم يرسل النسخة المعدَّلة إلى عدد من المتلقِّين (وهو ما يُشار إليه أيضاً "بالتصيُّد"). وتقتضي بعض النُهج الوطنية أن تتعلق البيانات الأصلية في الحاسوب بوثائق الغرض منها إنشاء التزامات قانونية ملزمة، بينما تكتفي نُهج أخرى باقتضاء أن يقصد الجاني من فعله أن يُنظر في النسخة المعدَّلة على أنها التزامات قانونية أو يُتصرَّف استناداً إليها بشأن التزامات قانونية."[4]

---

3 https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html

4 http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime_questionnaires/Member_State_questionnaire.xls

3.1 قوانين الأمان على الإنترنت

الرمز- GCIv5: Legal1.3

الأساس المنطقي-GCIv5: في إطار ردع السلوكيات المعادية للمجتمع في أنشطة الإنترنت، التي تُشعر المستخدمين والمجتمعات المحلية بنقص الأمان، تقيس الأسئلة أدناه مدى تنظيم بعض السلوكيات. وفي أغلب الأحوال، يجب في تنظيم هذه السلوكيات أن يوازن بعناية فيما بين حقوق الإنسان والقيم الأخرى المعتمدة في جملة معاهدات دولية منها اتفاقية الأمم المتحدة لحقوق الإنسان. ويرجى الالتفات إلى أنه لا يلزم أن تذكر قوانين البلد صراحةً أن أحكامها تُطبَّق على ظروف فضاء الإنترنت/الظروف الرقمية، بل يكفي أن يكون وجوب تطبيقها على هذه الظروف متعارفاً عليه لدى الهيئات القضائية في البلد.

1.3.1 هل يعتمد بلدكم تشريعاً نافذاً واجب التطبيق على نشر المواد العنصرية والمواد المحرِّضة على كره الأجانب على الإنترنت؟

الرمز- GCIv5: Legal1.3.1

الأساس المنطقي-GCIv5: إن نشر مواد عنصرية ومواد محرِّضة على كره الأجانب على الإنترنت له آثار سلبية فادحة على مجتمعات الإنترنت، منها الحد من التنوع وتأجيج الانقسامات، كما أنه قد يُلحق الأذى بالأفراد. وينبغي أن يكون التشريع النافذ لمكافحة العنصرية وكره الأجانب واضحاً بحيث يسهل على الأفراد فهمه والتقيد به. وتُقبل هنا الإشارة إلى التشريعات غير التكنولوجية؛ إذ لا يلزم أن يحدد التشريع ذو الصلة أن أحكامه تنطبق على نشر المواد العنصرية والمواد المحرِّضة على كره الأجانب على الإنترنت، ما دامت تقترن به بيانات قانونية أو جهات صديقة للمحاكم أو سوابق قضائية أو مواد أخرى مناسبة تثبت وجوب تطبيقه على ظروف فضاء الإنترنت.

2.3.1 هل يعتمد بلدكم تشريعاً نافذاً واجب التطبيق على التحرش والاعتداء على الكرامة/السلامة الشخصية عبر الإنترنت؟

الرمز- GCIv5: Legal1.3.2

الأساس المنطقي-GCIv5: قد تترتب على التحرش والاعتداء على الكرامة/السلامة الشخصية آثار سلبية فادحة على الأشخاص، وبخاصة في حال وقوع ذلك عبر الإنترنت. ويرشد التشريع النافذ ذو الصلة أجهزة إنفاذ القانون بشأن الحالات التي توجب اتخاذ إجراء، والمحاكمَ في كيفية الفصل في هذه القضايا، ويقدم التوجيه بشأن سبل الانتصاف للأطراف المتضررة، بما يُسهم في النهاية في تعزيز الثقة والأمان على الإنترنت. وتُقبل هنا الإشارة إلى التشريعات غير التكنولوجية؛ إذ لا يلزم أن يحدد التشريع ذي الصلة أن أحكامه تنطبق على أفعال التحرش والاعتداء عبر الإنترنت أو على نشر المواد المحرِّضة على كره الأجانب على الإنترنت، ما دامت تقترن به بيانات قانونية أو جهات صديقة للمحاكم أو سوابق قضائية أو مواد أخرى مناسبة تثبت وجوب تطبيقه على ظروف فضاء الإنترنت.

2 لوائح الأمن السيبراني

الرمز- GCIv5: Legal2

الأساس المنطقي-GCIv5: إن تنظيم الأمن السيبراني يحدد القواعد المتعلقة بحماية البيانات، والإبلاغ عن الخروقات، ومتطلبات إصدار الشهادات/الاشتراطات التقييسية في مجال الأمن السيبراني، وتنفيذ التدابير الأمنية السيبرانية، ومتطلبات التدقيق الأمني السيبراني، وكذلك القواعد المتعلقة بحماية الخصوصية، وحماية الأطفال على الإنترنت (COP)، والتوقيعات الرقمية والمعاملات الإلكترونية، والمسؤولية القانونية لمقدمي خدمات الإنترنت. وغالباً ما تشكل اللوائح الإطار التنفيذي للقوانين، المحدِّد لكيفية إنفاذها. وتستطيع البلدان تحسين وفائها بالتزامها بتعزيز الأمن السيبراني بإصدار لوائح واضحة ومتسقة وواجبة التطبيق ومحدَّثة.

1.2 هل يعتمد بلدكم نظاماً قانونياً (لوائح) لحماية البيانات الشخصية؟

الرمز- GCIv5: Legal2.1

الأساس المنطقي-GCIv5: إن تنظيم حماية البيانات يعزز إدارة البيانات ويحدد مسؤوليات حافظي البيانات وحقوق الأفراد. كما يمكنه أن يستهدف حافظي البيانات بتوجيهات بشأن مساءلتهم عن كيفية استخدام البيانات الشخصية، ويضمن ألا تسيء المنظمات استخدام البيانات التي يجري جمعها.

2.2 هل يعتمد بلدكم نظاماً قانونياً (لوائح) لحماية الخصوصية؟

الرمز- GCIv5: Legal2.2

الأساس المنطقي-GCIv5: تضمن لوائح حماية الخصوصية حماية البيانات الشخصية، وشفافية المنظمات في كيفية استخدام البيانات، وتمتع الأفراد بالحق في النفاذ إلى بياناتهم الشخصية وتصحيحها. إذ يمكن لهذه اللوائح أن تحظر على المنظمات بيع البيانات الشخصية أو إطلاع الغير عليها دون موافقة أصحابها. وحماية الخصوصية يمكن أن تضمن قدرة الأفراد على التحكم في بياناتهم الشخصية. وقد تُسهم إساءة استخدام البيانات الشخصية في وقوع جرائم سيبرانية وتقويض الثقة في التكنولوجيات الرقمية.

3.2 هل يعتمد بلدكم نظاماً قانونياً (لوائح) للإبلاغ عن خروقات/حوادث أمن البيانات تُطبَّق على الجهات الفاعلة في القطاع الخاص؟

الرمز- GCIv5: Legal2.3

الأساس المنطقي-GCIv5: إن خرق البيانات يمكن أن يؤثر سلباً على الأفراد والشركات والحكومات، بتعريضهم لسرقات مالية وسرقة الهوية والإضرار بسمعتهم، وبنشوء آثار جزائية على حافظي البيانات. والتنظيم الفعال لهذه المسألة يمكن أن يشمل حالات الإبلاغ عن خروقات البيانات، ويُلزم الجهات الفاعلة بإبلاغ الأفراد والشركات والحكومات عن خروقات البيانات في الوقت المناسب. فمن شأن ذلك أن يمكِّن الأفراد والشركات والحكومات من اتخاذ الإجراءات اللازمة لحماية أنفسهم من الأضرار التي قد تترتب على خرق البيانات. ويمكن للوائح الإبلاغ عن خروقات البيانات أن تشجع على اعتماد الممارسات الرشيدة في مجال إدارة البيانات، وتُلزم بالإبلاغ عن هذه الخروقات في الوقت المناسب، وتكفل للأطراف المتضررة حق المقاضاة.

4.2 هل يعتمد بلدكم نظاماً قانونياً (لوائح) لمتطلبات التدقيق الأمني السيبراني تُطبَّق على الوكالات والدوائر الحكومية الوطنية أو على الجهات التي تتعاقد معها هذه الكيانات؟

الرمز- GCIv5: Legal2.4

الأساس المنطقي-GCIv5: إن إصدار لوائح تتعلق بمتطلبات التدقيق الأمني السيبراني يمكن أن يعزز تحديد المخاطر الأمنية السيبرانية ويحفز تحسين الممارسات الأمنية السيبرانية بتشجيع الوكالات والدوائر والجهات المتعاقَد معها على تحديد مواطن الضعف في أنظمتها وتقويمها. إضافةً إلى ذلك، يمكن أن تشجع هذه اللوائح الوكالات والدوائر والجهات المتعاقَد معها على اعتماد أفضل الممارسات في مجال الأمن السيبراني واتباع المعايير الدولية.

5.2 هل يعتمد بلدكم نظاماً قانونياً (لوائح) لمعايير الأمن السيبراني تُطبَّق على الجهات الفاعلة الوطنية في القطاع العام؟

الرمز- GCIv5: Legal2.5

الأساس المنطقي-GCIv5: غالباً ما تستهدف الهجمات السيبرانية الجهات الفاعلة في القطاع الخاص. وعلى ذلك، فمن المهم أن تنفذ هذه الجهات تدابير رصينة لحماية أمنها السيبراني لتتمكن من حماية أنفسها والمواطنين. ووجود نظام قانوني للمعايير الأمنية السيبرانية يُطبَّق على الجهات الفاعلة الوطنية في القطاع العام يمكن أن يساعد في ضمان تحسين حماية هذه الجهات من الهجمات السيبرانية، وفي اتباعها أفضل الممارسات في مجال الأمن السيبراني.

وتتضمن هذه المعايير، على سبيل المثال لا الحصر، ما يلي: معرفة أمن الحوسبة السحابية (التحالف المعني بأمن الحوسبة السحابية) وCISSP وSSCP وCBK وCSSLP والتحليل الجنائي في مجال الأمن السيبراني (ISC[2]) وGIAC وGIAC GSSP (SANS) وCISM وCISA و(ISACA) CRISC والرابطة الصناعية لتكنولوجيا الحوسبة (CompTIA) وC|CISCO وCEH وECSA وCHFI (مجلس المجموعة الأوروبية) و(ISECOM) OSSTMM وPCIP/CCISP (معهد البنى التحتية الحيوية) وQ/ISP وشهادة هندسة أمن البرمجيات (جامعة الأمن) وCPP وPSP و(ASIS) PCI وLPQ وLPC (معهد منع الخسائر) ورابطة مفتشي الاحتيال المعتمدين (CFE) ومعالجو حوادث الأمن الحاسوبي المعتمدون (SEI) التابعون لأفرقة التصدي للطوارئ الحاسوبية (CERT) ومعهد التعليم المالي الاستهلاكي (CITRMS) ومعهد الأمن السيبراني (CSFA) و(IAPP) CIPP وABCP وCBCP و MBCP (DRI) وBCCP وBCCS وBCCE وDRCS و(BCM) DRCE وCIA وCCSA (معهد المراجعين الداخليين) والرابطة الدولية لمديري المخاطر المحترفين ومعهد إدارة المشاريع (PMP)، والمعيار 27001 للمتطلبات المعيارية لنظام إدارة أمن المعلومات والمعيار 28000 لأمن إدارة سلسلة التوريد الصادران عن المنظمة الدولية للتوحيد القياسي (ISO) والمعيار 62443 لأمن أنظمة الأتمتة والتحكم الصناعية، الصادر عن الجمعية الدولية للأتمتة (ISA).

6.2 هل يعتمد بلدكم نظاماً قانونياً (لوائح) بشأن استخدام التوقيعات الرقمية والمعاملات الإلكترونية في الخدمات والتطبيقات الحكومية (الحكومة الإلكترونية)؟

الرمز- GCIv5: Legal2.6

الأساس المنطقي-GCIv5: يتزايد استخدام الحكومات للتوقيعات الرقمية والمعاملات الإلكترونية في خدماتها وتطبيقاتها. ولهذا التحول إلى الأنظمة الإلكترونية عدد من الفوائد منها رفع الكفاءة وزيادة الأمن. بيد أنه إن لم يُنفذ نظام قانوني مناسب بهذا الشأن، يمكن التعرض لخطر عدم فعالية أو مأمونية استخدام هذه الأنظمة.

فتنظيمها يساعد في ضمان ثقة المواطنين في أمن بياناتهم وفي فعالية وموثوقية الأنظمة الحكومية.

7.2 هل يعتمد بلدكم نظاماً قانونياً (لوائح) لمكافحة الاتصالات غير المرغوبة، المعروفة أيضاً باسم الرسائل الاقتحامية؟

الرمز- GCIv5: Legal2.7

الأساس المنطقي-GCIv5: إن قيام البلدان بإصدار لوائح لمكافحة الاتصالات غير المرغوبة يمكّنها من أن تهيئ للجميع تجربةً أكثر أماناً وإمتاعاً على الإنترنت. وتساعد هذه اللوائح في حماية المواطنين من الآثار السلبية للرسائل الاقتحامية، ومنع مُرسليها من استغلال الأشخاص.

8.2 هل يعتمد بلدكم نظاماً قانونياً (لوائح) لتحديد البنى التحتية الحيوية الوطنية وحمايتها؟

الرمز- GCIv5: Legal2.8

الأساس المنطقي-GCIv5: بتحديد البنى التحتية الحيوية الوطنية وحمايتها، يستطيع البلد إدارة المخاطر السيبرانية. ووجود نظام قانوني لحماية البنى التحتية الحيوية الوطنية يساعد البلد في التخطيط لكيفية الاستجابة لما قد يتعرض له من كوارث أو اعتداءات أو هجمات خطيرة، فيضمن بذلك قدرته على الاستجابة لها بسرعة وفعالية. ولا بد أيضاً من أن تتوفر لدى البلد خطة للتعافي من آثار مثل هذه الكوارث أو الهجمات الخطيرة.

9.2 هل يعتمد بلدكم نظاماً قانونياً (لوائح) لحماية الأطفال على الإنترنت؟

الرمز- GCIv5: Legal2.9

الأساس المنطقي-GCIv5: إن معالجة قضية حماية الأطفال على الإنترنت بإصدار لوائح تنظم هذه الحماية يمكّن الوكالات والجهات الفاعلة المختصة من اتخاذ الإجراءات اللازمة وتنفيذ المتطلبات والقواعد المحددة للتعامل مع الجرائم المرتكبة عبر الإنترنت/السيبرانية بحق الأطفال والشباب ومكافحتها. ومن اللازم أن تنفذ هذه القواعد الطائفة الواسعة لأصحاب المصلحة في جميع القطاعات وجميع شرائح المجتمع، بدءاً من مشغلي الاتصالات في هذه الصناعة ومروراً بجهات إنفاذ القانون وانتهاءً بأصحاب المصلحة من المجتمع المدني، الذين ينبغي أن يعملوا سوياً دعماً لتحقيق بيئة مأمونة وسالمة للأطفال والشباب.

التدابير التقنية

الأساس المنطقي-GCIv5: تشكل التكنولوجيا خط الدفاع الأول ضد التهديدات السيبرانية والجهات المخرِّبة على الإنترنت. فبافتقار البلدان إلى ما يكفي من تدابير وقدرات تكنولوجية لكشف الهجمات السيبرانية والاستجابة لها، تظل والكيانات التابعة لها عرضة للتهديدات السيبرانية. ولا يمكن لنشوء تكنولوجيات المعلومات والاتصالات ونجاحها أن يزدهرا إلا في مناخ من الثقة والأمن. ومن ثم، تلزم البلدان القدرة على استحداث استراتيجيات لوضع معايير أمنية دنيا ونظم اعتماد، معترف بها، للتطبيقات والأنظمة البرمجية. ولا بد من أن تقترن هذه الجهود بإنشاء كيان وطني يختص بالحوادث السيبرانية وطنياً ويكون، على أقل تقدير، تابعاً لوكالة حكومية ومزوداً بإطار وطني للمراقبة والإنذار والاستجابة للحوادث.

ويمكن قياس التدابير التقنية بمدى وجود المؤسسات والأطر التقنية المعنية بالأمن السيبراني التي أقرَّها البلد أو أنشأها، وعددها. وتتألف مجموعة المؤشرات المتفرعة من دعامة التدابير التقنية هذه من مؤشرات الأداء التالية:

1 فريق التصدي للطوارئ الحاسوبية/فريق التصدي للحوادث الحاسوبية/فريق التصدي للحوادث الأمنية الحاسوبية أو مركز العمليات الأمنية، على الصعيد الوطني

الرمز- GCIv5: Tech1

الأساس المنطقي-GCIv5: إن إنشاء آليات، وهياكل مؤسسية، فعالة ضرورة لكشف التهديدات والحوادث السيبرانية والوقاية منها والاستجابة لها وتخفيف آثارها. وتُعنى أفرقة التصدي للحوادث الحاسوبية (CIRT)، فضلاً عن أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) وأفرقة التصدي للطوارئ الحاسوبية (CERT) ومراكز العمليات الأمنية (SOC)[5] ، بالحماية من الحوادث الأمنية السيبرانية وكشفها والاستجابة لها، ويمكنها أن تعزز قدرة البلد على إدارة هذه الحوادث. كما يمكن لأفرقة التصدي للحوادث الحاسوبية أو مراكز العمليات الأمنية أن تفيد في بناء القاعدة المعرفية الداعمة لتنفيذ البلد استراتيجية وطنية للأمن السيبراني، فضلاً عن نهج لحماية البنى التحتية الحيوية للمعلومات؛ فتدعم بذلك بناء ثقافة ونظام إيكولوجي وطنيَيْن للأمن السيبراني وتنفيذ ما يتصل بذلك من مبادرات توعية؛ وتدعم كذلك استحداث منصات وطنية للأمن السيبراني تتصل بهذه الاستراتيجية وهذا النهج كخدمات الحكومة الإلكترونية والأطر الوطنية لإدارة النفاذ والهوية؛ وتزيد من تمكين البلد من بناء وتعزيز قدراته في مجال الاستجابة للحوادث وتنسيق هذه الاستجابة.

1.1 هل لدى بلدكم على الصعيد الوطني/الحكومي فريق للتصدي للحوادث الحاسوبية/فريق للتصدي للحوادث الأمنية الحاسوبية/فريق للتصدي للطوارئ الحاسوبية أو مركز للعمليات الأمنية، يعمل بكامل طاقته؟

الرمز- GCIv5: Tech1.1

الأساس المنطقي-GCIv5: تُعنى أفرقة التصدي للحوادث الحاسوبية (CIRT)، فضلاً عن أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) وأفرقة التصدي للطوارئ الحاسوبية (CERT) ومراكز العمليات الأمنية (SOC)، بالحماية من الحوادث الأمنية السيبرانية وكشفها والاستجابة لها. ويعتبر أن كلاً من الفريق CIRT/الفريق CSIRT/الفريق CERT ومركز العمليات الأمنية يعمل بكامل طاقته باستيفائه العناصر التالية:

- تحديد هيكله التنظيمي والموافقة عليه
- توظيف موظفين مدرَّبين ومؤهلين
- تأمين مرافقه (أي تنفيذ تدابير مناسبة لحماية مرافق الكيان من التهديدات المادية والبيئية)
- إعداد وتنفيذ عمليات وإجراءات تفصيلية لعملياته
- اعتماد وتنفيذ التكنولوجيات اللازمة لعملياته
- تنفيذ عمليات التعاون مع أصحاب المصلحة والشركاء الرئيسيين
- تقديم الخدمات إلى عملائه بفعالية وكفاءة.

وقد تتضمن أولى عمليات إنشاء فريق استجابة للحوادث الحاسوبية عملية تقييم (تشمل قياس مدى الجاهزية لإنشاء هذا الفريق، وكذلك إعداد قاعدة أصحاب المصلحة المعنيين الذين تلزمهم أعمال الفريق)، وعملية تصميم (تشمل إعداد وثيقة التصميم التفصيلي للفريق)، ثم عملية الإنشاء (تشمل تنفيذ البنية التحتية، وإنشاء علاقات مع أصحاب المصلحة المعنيين والعملاء، وإنشاء العمليات والخدمات المشمولة بولاية الفريق، وتنفيذ عمليات إطلاق خدماته، وتقديم طلب عضوية في الرابطات الدولية المعنية).

2.1 أنشطة الفريق الوطني CERT/CSIRT/CIRT أو المركز الوطني للعمليات الأمنية

الرمز- GCIv5: Tech1.2

الأساس المنطقي-GCIv5: يُعنى الفريق الوطني للاستجابة للحوادث الحاسوبية (CIRT)، وكذلك الفريق الوطني للاستجابة للحوادث الأمنية الحاسوبية (CSIRT) والفريق الوطني للاستجابة للطوارئ الحاسوبية (CERT) والمركز الوطني للعمليات الأمنية (SOC)، بالحماية من الحوادث الأمنية السيبرانية وكشفها والاستجابة لها. ويشكل كل منها الجهة المركزية للإبلاغ عن الحوادث الأمنية السيبرانية، كما يقدم المعلومات، والمساعدة التقنية، اللازمة لمساعدة المنظمات في منع الحوادث السيبرانية

[5] https://ieeexplore.ieee.org/document/9296846

وتخفيف آثارها والاستجابة لها. ويُعنى الفريق الوطني CIRT أو المركز الوطني SOC، أيضاً، بإجراء أبحاث في القضايا الأمنية السيبرانية واستحداث ممارسات فضلى ومبادئ توجيهية للاستجابة للحوادث السيبرانية.

1.2.1 هل يقوم الفريق الوطني/الحكومي CERT/CSIRT/CIRT أو المركز الوطني/الحكومي للعمليات الأمنية في بلدكم بإعداد وتنفيذ أنشطة توعية في مجال الأمن السيبراني؟

الرمز- GCIv5: Tech1.2.1

الأساس المنطقي-GCIv5: يمكن للأفرقة الوطنية للاستجابة للحوادث الحاسوبية (CIRT) أو المراكز الوطنية للعمليات الأمنية أن تضطلع بدور مهم في تنفيذ حملات توعية في مجال الأمن السيبراني. إذ إن بوسعها بصفتها الهيئات التنسيقية المركزية في هذا المجال اكتساب رؤية متزايدة الوضوح لما هو حالي وما هو ناشئ من تهديدات سيبرانية وتحديات أمنية سيبرانية ومواطن ضعف، وأفكار مفيدة بشأن الاتجاهات الأمنية السيبرانية الرئيسية، ومن تطورات تكنولوجية في مجال الأمن السيبراني، وممارسات فضلى للكشف عن التهديدات السيبرانية والاستجابة لها. ولتعزيز ثقافة الأمن السيبراني والتشجيع على معرفة التدابير الأمنية السيبرانية والممارسات والسلوكيات الرشيدة في هذا الميدان، ينبغي لفريق التصدي للحوادث الحاسوبية/فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)/فريق التصدي للطوارئ الحاسوبية (CERT) أو مركز العمليات الأمنية استحداث و/أو تنفيذ و/أو تنسيق مبادرات وأنشطة توعية في مجال الأمن السيبراني تُكيَّف لتناسب مختلف أصحاب المصلحة، وتستند إلى المعلومات المجموعة عن تطور مشهد التهديدات والاتجاهات الرئيسية وأفضل الممارسات في هذا المجال.

2.2.1 هل يقوم الفريق الوطني/الحكومي CERT/CSIRT/CIRT أو المركز الوطني/الحكومي للعمليات الأمنية في بلدكم بإجراء تمارين أمنية سيبرانية (تمارين سيبرانية) بانتظام؟

الرمز- GCIv5: Tech1.2.2

الأساس المنطقي-GCIv5: التمارين الأمنية السيبرانية هي أحداث يُخطط لتنفيذها، تقوم المنظمة المعنية أثناءها بمحاكاة خلل سيبراني ما بهدف تطوير أو اختبار قدرات من قبيل منع الخلل أو كشفه أو الاستجابة له أو التعافي من آثاره. وإجراء تمارين أمنية سيبرانية بانتظام، بالاشتراك مع أصحاب المصلحة المعنيين، تدبيرٌ استباقي يعزز الجاهزية والمرونة الأمنية السيبرانية. فينبغي لفريق التصدي للحوادث الحاسوبية (CIRT)/فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)/فريق التصدي للطوارئ الحاسوبية (CERT) أو مركز العمليات الأمنية إعداد وإجراء تمارين دورية لإدارة الحوادث/الأزمات السيبرانية، مع إشراك أي من الكيانات العامة أو الخاصة المعنية في جميع أنحاء البلد فيها، لاختبار قدرات هذا الفريق أو المركز في مجال التصدي للحوادث.

3.2.1 هل يقوم الفريق الوطني/الحكومي CERT/CSIRT/CIRT أو المركز الوطني/الحكومي للعمليات الأمنية في بلدكم بإصدار إشعارات أمنية سيبرانية عامة؟

الرمز- GCIv5: Tech1.2.3

الأساس المنطقي-GCIv5: تضمن الإشعارات الأمنية السيبرانية العامة إعلام الوكالات والدوائر بالتهديدات الأمنية السيبرانية المحتملة وتمكينها من اتخاذ احتياطات. إضافةً إلى ذلك، من الممكن أن تساعد هذه الإشعارات في تعزيز تنسيق أنشطة التصدي للتهديدات الأمنية السيبرانية.

3.1 هل الفريق الوطني/الحكومي CERT/CSIRT/CIRT أو المركز الوطني/الحكومي للعمليات الأمنية في بلدكم عضو في منتدى أفرقة الأمن والتصدي للحوادث (FIRST) و/أو مسجَّل لدى فريق المهام المعني بأفرقة التصدي للحوادث الأمنية الحاسوبية (TF-CSIRT)؟

الرمز- GCIv5: Tech1.3

الأساس المنطقي-GCIv5: تستفيد الأفرقة الوطنية للاستجابة للحوادث الحاسوبية (CIRT) أو المراكز الوطنية للعمليات الأمنية (SOC) الأعضاء في منتدى أفرقة الأمن والتصدي للحوادث (FIRST) من ميزة الانضمام إلى شبكة عالمية لأفرقة التصدي للحوادث الحاسوبية واستحقاقات تلقّي التدريب والموارد، واكتساب الخبرة المتخصصة من موظفي المنتدى، والتمتع بفرص التعاون وتبادل أفضل الممارسات. وتشترط معايير أهلية الانضمام إلى منتدى أفرقة الأمن والتصدي للحوادث فاعلية التزام البلدان بأعماله. ويُعتد في إجابة هذا السؤال بالفريق الوطني CIRT أو المركز الوطني SOC الحائز لصفة مسجَّل لدى فريق المهام المعني بأفرقة التصدي للحوادث الأمنية الحاسوبية (TF-CSIRT).

4.1 هل الفريق الوطني/الحكومي CERT/CSIRT/CIRT أو المركز الوطني/الحكومي للعمليات الأمنية المشار إليه أعلاه عضو في فريق إقليمي للتصدي للحوادث الحاسوبية (كفريق آسيا والمحيط الهادئ للتصدي للطوارئ الحاسوبية (APCERT) وشبكة المحيط الهادئ للعمليات الأمنية السيبرانية (PACSON) والفريق الإفريقي للتصدي للطوارئ الحاسوبية (AFRICA CERT) ووكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) وفريق التصدي للطوارئ الحاسوبية التابع لمنظمة التعاون الإسلامي (OIC) وبرنامج الأمن السيبراني لدى منظمة الدول الأمريكية (OAS))؟

الرمز- GCIv5: Tech1.4

الأساس المنطقي-GCIv5: يشمل الانضمام إلى فريق إقليمي للتصدي للحوادث الحاسوبية جميع العلاقات الرسمية أو المنتظمة القائمة مع أي من الأفرقة الإقليمية الأخرى للتصدي للحوادث الحاسوبية. وللانضمام إلى فريق إقليمي للتصدي للحوادث الحاسوبية أو فريق إقليمي للتصدي للطوارئ الحاسوبية مزايا عديدة من بينها تبادل المعارف والخبرات: فغالباً ما تستطيع الأفرقة الإقليمية للتصدي للحوادث الحاسوبية أو الأفرقة الإقليمية للتصدي للطوارئ الحاسوبية تبادل المعارف والخبرات المتصلة بهذا المجال المناسبة لظروف البلدان المعنية.

2 أفرقة التصدي للطوارئ الحاسوبية/أفرقة التصدي للحوادث الحاسوبية/أفرقة التصدي للحوادث الأمنية الحاسوبية أو مراكز العمليات الأمنية، على صعيد القطاعات

الرمز- GCIv5: Tech2

الأساس المنطقي-GCIv5: يخدم الفريق القطاعي للتصدي للطوارئ الحاسوبية (CERT)/الفريق القطاعي للتصدي للحوادث الحاسوبية (CIRT)/الفريق القطاعي للتصدي للحوادث الأمنية الحاسوبية (CSIRT) أو المركز القطاعي للعمليات الأمنية (SOC) العملاء العاملين بقطاع محدد، كالقطاع المالي والقطاع الأكاديمي وقطاعات الطاقة والصحة والاتصالات والمرافق العامة والبنى التحتية الحيوية وغيرها من القطاعات. ويخدم الفريق القطاعي CIRT أو المركز القطاعي SOC عملاءه بتقديم خدمات متخصصة ومكيَّفة بحسب احتياجاتهم تتعلق باستخبار التهديدات وبالتهديدات. وقد تكون لدى البلد أفرقة قطاعية CIRT أو مراكز قطاعية SOC مشتركة مع نظيراتها في بلدان أخرى، بحيث يخدم الفريق أو المركز القطاعي العملاء العاملين بالقطاع المحدد في عدة بلدان. ولا تُقبل لأغراض هذا المؤشر الأفرقة العسكرية للتصدي للحوادث الحاسوبية.

1.2 هل لدى بلدكم أفرقة قطاعية CERT/CSIRT/CIRT أو مراكز قطاعية للعمليات الأمنية؟

الرمز- GCIv5: Tech2.1

الأساس المنطقي-GCIv5: يخدم الفريق القطاعي للتصدي للطوارئ الحاسوبية (CERT)/الفريق القطاعي للتصدي للحوادث الحاسوبية (CIRT)/الفريق القطاعي للتصدي للحوادث الأمنية الحاسوبية (CSIRT) أو المركز القطاعي للعمليات الأمنية (SOC) العملاء العاملين بقطاع محدد، كالقطاع المالي والقطاع الأكاديمي وقطاعات الطاقة والصحة والاتصالات والمرافق العامة والبنى التحتية الحيوية وغيرها من القطاعات. ويخدم الفريق القطاعي CIRT أو المركز القطاعي SOC عملاءه بتقديم خدمات متخصصة ومكيَّفة بحسب احتياجاتهم تتعلق باستخبار التهديدات وبالتهديدات. وقد تكون لدى البلد أفرقة قطاعية CIRT أو مراكز قطاعية SOC مشتركة مع نظيراتها في بلدان أخرى، بحيث يخدم الفريق أو المركز القطاعي العملاء العاملين بالقطاع المحدد في عدة بلدان. ولا تُقبل لأغراض هذا المؤشر الأفرقة العسكرية للتصدي للحوادث الحاسوبية. ويعتبر أن كلاًّ من الفريق القطاعي CIRT/الفريق القطاعيCSIRT/الفريق القطاعيCERT أو المركز القطاعي للعمليات الأمنية يعمل بكامل طاقته باستيفائه العناصر التالية:

- تحديد هيكله التنظيمي والموافقة عليه
- توظيف موظفين مدرَّبين ومؤهلين
- تأمين مرافقه (أي تنفيذ تدابير مناسبة لحماية مرافق الكيان من التهديدات المادية والبيئية)
- إعداد وتنفيذ عمليات وإجراءات تفصيلية لعملياته
- اعتماد وتنفيذ التكنولوجيات اللازمة لعملياته
- تنفيذ عمليات التعاون مع أصحاب المصلحة والشركاء الرئيسيين
- تقديم الخدمات إلى عملائه بفعالية وكفاءة.

وقد تتضمن عملية الإنشاء الجزئي لفريق قطاعي للتصدي للحوادث الحاسوبية عملية تقييم (تشمل قياس مدى الجاهزية لإنشاء هذا الفريق القطاعي، وكذلك إعداد قاعدة أصحاب المصلحة المعنيين الذين تلزمهم أعمال الفريق)، وعملية تصميم (تشمل إعداد وثيقة التصميم التفصيلي للفريق)، ثم عملية الإنشاء (تشمل تنفيذ البنية التحتية، وإنشاء علاقات مع أصحاب المصلحة المعنيين والعملاء، وإنشاء العمليات والخدمات المشمولة بولاية الفريق، وتنفيذ عمليات إطلاق خدماته، وتقديم طلب عضوية في الرابطات الدولية المعنية).

2.2 أنشطة الأفرقة القطاعية CERT/CSIRT/CIRT أو المراكز القطاعية للعمليات الأمنية

الرمز- GCIv5: Tech2.2

الأساس المنطقي-GCIv5: يُعنى الفريق القطاعي للتصدي للحوادث الحاسوبية (CIRT)، أو الفريق القطاعي للتصدي للحوادث الأمنية الحاسوبية (CSIRT) أو الفريق القطاعي للتصدي للطوارئ الحاسوبية (CERT)، أو المركز القطاعي للعمليات الأمنية (SOC)، بالحماية من الحوادث الأمنية السيبرانية وكشفها والتصدي لها.

ويشكل الفريق القطاعي CIRT أو المركز القطاعي SOC الجهة المركزية للإبلاغ عن الحوادث الأمنية السيبرانية في القطاع المعني. كما يقدم المعلومات، والمساعدة التقنية، اللازمة لمساعدة منظمات ذلك القطاع في منع الحوادث السيبرانية وتخفيف آثارها والتصدي لها. إضافةً إلى ذلك، يُعنى الفريق القطاعي CIRT أو المركز القطاعي SOC بإجراء أبحاث في القضايا الأمنية السيبرانية واستحداث ممارسات فضلى ومبادئ توجيهية للتصدي للحوادث السيبرانية.

1.2.2 هل تقوم الأفرقة القطاعية CERT/CSIRT/CIRT أو المراكز القطاعية للعمليات الأمنية في بلدكم بإعداد وتنفيذ أنشطة توعية في القطاعات المعنية في مجال الأمن السيبراني؟

الرمز- GCIv5: Tech2.2.1

الأساس المنطقي-GCIv5: بوسع الأفرقة القطاعية للتصدي للحوادث الحاسوبية (CIRT) أو المراكز القطاعية للعمليات الأمنية أن تضطلع بدور مهم في تنفيذ حملات توعية في قطاعات محددة في مجال الأمن السيبراني. إذ إن لديها بصفتها الهيئات التنسيقية المركزية في هذا المجال في القطاعات المعنية أفكاراً مفيدة بشأن الاتجاهات الأمنية السيبرانية المتصلة بأصحاب المصلحة. فاستناداً إلى استخبارات التهديدات، الخاصة بالقطاع المعني والعامة كذلك، يمكن للفريق القطاعي CIRT المساعدة في إعداد وتنفيذ أنشطة توعية تستهدف مجموعات مختلفة من أصحاب المصلحة المعنيين بالقطاع لتحسين السلوكيات السيبرانية المأمونة.

2.2.2 هل تشارك الأفرقة القطاعية CERT/CSIRT/CIRT أو المراكز القطاعية للعمليات الأمنية في بلدكم في التمارين الأمنية السيبرانية (التمارين السيبرانية) الوطنية بانتظام؟

الرمز- GCIv5: Tech2.2.2

الأساس المنطقي-GCIv5: التمارين الأمنية السيبرانية هي أحداث يُخطط لتنفيذها، تقوم المنظمة المعنية أثناءها بمحاكاة خلل سيبراني ما بهدف تطوير أو اختبار قدرات من قبيل منع الخلل أو كشفه أو التصدي له أو التعافي من آثاره. ومشاركة الأفرقة القطاعية للتصدي للحوادث الحاسوبية (CIRT) في التمارين الأمنية السيبرانية الوطنية تدبير استباقي يُعزز القدرة الأمنية السيبرانية العامة.

3.2.2 هل تُطلع الأفرقة القطاعية CERT/CSIRT/CIRT أو المراكز القطاعية للعمليات الأمنية عملاءها على الحوادث القطاعية؟

الرمز- GCIv5: Tech2.2.3

الأساس المنطقي-GCIv5: إن إطْلاع أصحاب المصلحة في القطاع المعني على معلومات استخبارات التهديدات، المتعلقة بذلك القطاع، يمكن أن يُذكي وعيهم بالتهديدات ومواطن الضعف المتصلة به ويحسِّن زمن التصدي للحوادث، وفعاليتها. إضافةً إلى ذلك، من الممكن أن يساعد ذلك في زيادة تنسيق عمليات التصدي للحوادث الأمنية السيبرانية فيما بين الحكومة والقطاع الخاص والجمهور العام.

3 الإطار الوطني لتنفيذ معايير الأمن السيبراني

الرمز- GCIv5: Tech3

الأساس المنطقي-GCIv5: تشمل الأطر الوطنية لتنفيذ معايير الأمن السيبراني وجود إطار حكومي معتمد (أو مُقرّ) (أطر حكومية معتمدة (أو مُقرَّة)) لإجازة المهنيين واعتمادهم وفقاً لمعايير الأمن السيبراني المعترف بها دولياً. وتتضمن هذه الإجازات والاعتمادات والمعايير، على سبيل المثال لا الحصر، ما يلي: معرفة أمن الحوسبة السحابية (التحالف المعني بأمن الحوسبة السحابية) وCISSP وSSCP وCSSLP CBK والتحليل الجنائي في مجال الأمن السيبراني (ISC^2) وGIAC وGIAC GSSP (SANS) وCISM وCISA و(ISACA) CRISC والرابطة الصناعية لتكنولوجيا الحوسبة (CompTIA) وC|CISCO وCEH وECSA وCHFI (مجلس المجموعة الأوروبية) و(ISECOM) OSSTMM وPCIP/CCISP (معهد البنى التحتية الحيوية) وQ/ISP وشهادة هندسة أمن البرمجيات (جامعة الأمن) وCPP وPSP و(ASIS) PCI وLPQ وLPC (معهد منع الخسائر) ورابطة مفتشي الاحتيال المعتمدين (CFE) ومعالجو حوادث الأمن الحاسوبي المعتمدون (SEI) التابعون لأفرقة التصدي للطوارئ الحاسوبية (CERT) ومعهد التعليم المالي الاستهلاكي (CITRMS) ومعهد الأمن السيبراني (CSFA) و(IAPP) CIPP وABCP وCBCP و MBCP (DRI) وBCCP وBCCS وBCCE وDRCS و(BCM) DRCE وCIA وCCSA (معهد المراجعين الداخليين للحسابات) والرابطة الدولية لمديري المخاطر المحترفين ومعهد إدارة المشاريع (PMP)، والإجازات والاعتمادات الصادرة وفقاً للمعيار 27001 للمتطلبات المعيارية لنظام إدارة أمن المعلومات والمعيار 28000 لأمن إدارة سلسلة التوريد الصادرين عن المنظمة الدولية للتوحيد القياسي (ISO) والمعيار 62443 لأمن أنظمة الأتمتة والتحكم الصناعية، الصادر عن الجمعية الدولية للأتمتة (ISA).

1.3 هل لدى حكومتكم إطار لتنفيذ/اعتماد معايير الأمن السيبراني المعترف بها وطنياً أو دولياً؟

الرمز- GCIv5: Tech3.1

الأساس المنطقي-GCIv5: تشمل الأطر الوطنية لتنفيذ معايير الأمن السيبراني وجود إطار حكومي معتمد (أو مُقرّ) (أطر حكومية معتمدة (أو مُقرَّة)) لتنفيذ/اعتماد معايير الأمن السيبراني المعترف بها وطنياً أو دولياً. ويمكن أن يحدد هذا الإطار خطة أو خريطة طريق لتنفيذ/اعتماد المعايير، وأصحاب المصلحة المعنيين، والعمليات التي ستُتبع في أعمال التحديث المستقبلية، والأساليب التوجيهية الأخرى لعملية التنفيذ.

وتتضمن هذه المعايير، على سبيل المثال لا الحصر، ما يلي: معرفة أمن الحوسبة السحابية (التحالف المعني بأمن الحوسبة السحابية) وCISSP وSSCP وCSSLP CBK والتحليل الجنائي في مجال الأمن السيبراني (ISC^2) وGIAC وGIAC GSSP (SANS) وCISM وCISA و(ISACA) CRISC والرابطة الصناعية لتكنولوجيا الحوسبة (CompTIA) وC|CISCO وCEH وECSA وCHFI (مجلس المجموعة الأوروبية) و(ISECOM) OSSTMM وPCIP/CCISP (معهد البنى التحتية الحيوية) وQ/ISP وشهادة هندسة أمن البرمجيات (جامعة الأمن) وCPP وPSP و(ASIS) PCI وLPQ وLPC (معهد منع الخسائر) ورابطة مفتشي الاحتيال المعتمدين (CFE) ومعالجو حوادث الأمن الحاسوبي المعتمدون (SEI) التابعون لأفرقة التصدي للطوارئ الحاسوبية (CERT) ومعهد التعليم المالي الاستهلاكي (CITRMS) ومعهد الأمن السيبراني (CSFA) و(IAPP) CIPP وABCP وCBCP و MBCP (DRI) وBCCP وBCCS وBCCE وDRCS و(BCM) DRCE وCIA وCCSA (معهد المراجعين الداخليين) والرابطة الدولية لمديري المخاطر المحترفين ومعهد إدارة المشاريع (PMP)، والمعيار 27001 للمتطلبات المعيارية لنظام إدارة أمن المعلومات والمعيار 28000 لأمن إدارة سلسلة التوريد الصادران عن المنظمة الدولية للتوحيد القياسي (ISO) والمعيار 62443 لأمن أنظمة الأتمتة والتحكم الصناعية، الصادر عن الجمعية الدولية للأتمتة (ISA).

2.3 هل يشمل إطار تنفيذ/اعتماد معايير الأمن السيبراني المعترف بها وطنياً أو دولياً البنى التحتية الحيوية؟

الرمز- GCIv5: Tech3.2

الأساس المنطقي-GCIv5: إن شمول البنى التحتية الحيوية بجميع أُطر تنفيذ/اعتماد معايير الأمن السيبراني المعترف بها وطنياً أو دولياً مسألة أساسية لتعزيز حماية البنى التحتية الحيوية ومرونتها ومساعدتها في الحد من مواطن الضعف وفي إدارة المخاطر الأمنية السيبرانية بفعالية.

التدابير التنظيمية

الأساس المنطقي-GCIv5: إن التدابير التنظيمية ضرورية لسلامة إنفاذ الوضع الأمني السيبراني الوطني. إذ يلزم أن تحدد الحكومة أهدافاً استراتيجية في إطار خطة شاملة على مستويات التنفيذ والأداء والقياس. ولا بد أيضاً من إنشاء هياكل إدارية لإنفاذ الوضع

الأمني السيبراني ورصد عمليات التنفيذ وتقييم النتائج، ومن تفعيل هذه الهياكل. وفي غياب شبكة تنظيمية واضحة العناصر من الشركاء العاملين معاً في جميع دوائر الصناعة المعنية، تصبح جهود المجتمع المدني والمؤسسات الأكاديمية المبذولة في شتى القطاعات مشتتة ومبتورة، فيعرقل ذلك جهود تحقيق التنسيق الوطني في سياق تطوير القدرة الأمنية السيبرانية.

ويمكن قياس الهياكل التنظيمية بمدى وجود المؤسسات والاستراتيجيات المنظِّمة لتطوير القدرة الأمنية السيبرانية وطنياً، وعددها. وإنشاء هياكل تنظيمية فعالة ضرورة لتعزيز تطوير القدرة الأمنية السيبرانية، ومكافحة الجريمة السيبرانية، وتعزيز دور عمليات المراقبة والإنذار والتصدي للحوادث في ضمان التنسيق بين المبادرات الجديدة وتلك القائمة على مستويي الوكالات والقطاعات وعبر الحدود. وتتألف مجموعة المؤشرات المتفرعة من دعامة التدابير التنظيمية هذه من مؤشرات الأداء التالية:

1 الاستراتيجية الوطنية للأمن السيبراني

الرمز- GCIv5: Org1

الأساس المنطقي-GCIv5: تقدم الاستراتيجية الوطنية للأمن السيبراني إطاراً لتخصيص الموارد[6] يحدد الأهداف الوطنية المتعلقة بالأمن السيبراني والأولويات من الموارد اللازمة لتنفيذها بهدف تحسين الوضع الأمني في البلد وقدرة البلد على التأقلم[7]. كما تمكّن هذه الاستراتيجية الحكومة من التعاون مع جميع أصحاب المصلحة المعنيين على الصعيد الوطني. إضافةً إلى ذلك، يمكن أن تساعد الاستراتيجية الوطنية للأمن السيبراني في تشجيع الابتكار وحماية الخصوصية والحريات المدنية. وينبغي أن تحدد الاستراتيجية الأهداف الوطنية المتعلقة بالأمن السيبراني بوضوح والهيكل الإداري لتنفيذها[8].

1.1 هل يعتمد بلدكم استراتيجية وطنية للأمن السيبراني (NCS) أو سياسية وطنية للأمن السيبراني، سواء كانت قائمةً بذاتها أو جزءاً من وثيقة أخرى؟

الرمز- GCIv5: Org1.1

الأساس المنطقي-GCIv5: لا ريب في أن الأمن السيبراني قضية فائقة الأهمية لجميع الدول. وتقدم الاستراتيجية الوطنية للأمن السيبراني إطاراً لتخصيص الموارد اللازمة لحماية البنى التحتية الحيوية في الدولة. وتمكّن الحكومة أيضاً من العمل مع القطاع الخاص من أجل تحديد التهديدات السيبرانية وتخفيف آثارها. إضافةً إلى ذلك، يمكن أن تساعد الاستراتيجية الوطنية للأمن السيبراني في تشجيع الابتكار وحماية الخصوصية والحريات المدنية.

2.1 أولويات الاستراتيجية الوطنية للأمن السيبراني

الرمز- GCIv5: Org1.2

الأساس المنطقي-GCIv5: إن اعتماد استراتيجية وطنية محددة الأولويات يتيح تنسيق التصدي للمخاطر السيبرانية. وبالنظر إلى اختلاف التحديات الأمنية السيبرانية التي يواجهها كل بلد، يساعد التركيز على مجالات أمنية سيبرانية محددة البلدان في تحديد الأولويات من الموارد اللازمة وتنسيق التصدي للتهديدات السيبرانية. وقد تركز معظم أدلة إعداد الاستراتيجية الوطنية للأمن السيبراني على أولويات مختلفة، كدليل "إعداد الاستراتيجية الوطنية للأمن السيبراني".[9] وقد يُشار إلى مجالات الأولوية في بعض الاستراتيجيات بعبارة "مجالات التركيز"[10]. وتتضمن الأسئلة من 1.2.1 إلى 4.2.1 مجالات الأولوية التي يمكن أن تشملها الاستراتيجية الوطنية للأمن السيبراني. غير أنه قد تكون لدى البلدان مجالات أولوية أخرى.

---

6 https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained

7 https://www.enisa.europa.eu/topics/national-cyber-security-strategies

8 https://ncsguide.org/the-guide/

9 http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf

10 https://ncsguide.org/the-guide/

1.2.1 هل تشمل استراتيجية بلدكم الوطنية للأمن السيبراني حماية البنى التحتية الحيوية الوطنية؟

الرمز- GCIv5: Org1.2.1

الأساس المنطقي-GCIv5: تشمل البنية التحتية الحيوية الوطنية كل شيء بدءاً من شبكات الكهرباء وأنظمة المياه ووصولاً إلى شبكات المواصلات والمؤسسات المالية. فإن انهارت أي من هذه المرافق، عمَّت الفوضى البلد. ولذلك فمن المهم جداً أن تشتمل الاستراتيجية الوطنية للأمن السيبراني على خطة تضمن حماية هذه المرافق جيداً، ذلك أنه لا غنى عن البنية التحتية الحيوية لحفظ النظام العام والسلامة العامة وهي مهمة لاقتصاد البلد وفائقة الأهمية للأمن القومي.

2.2.1 هل تتضمن استراتيجية بلدكم الوطنية للأمن السيبراني مبادئ إدارة دورة الحياة، وإجراء عمليات رصد وتقييم وتحديث بانتظام؟

الرمز- GCIv5: Org1.2.2

الأساس المنطقي-GCIv5: ينبغي أن تتضمن الاستراتيجية الوطنية للأمن السيبراني (NCS) مبادئ إدارة دورة الحياة[11]، وإجراء عمليات رصد وتقييم وتحديث بانتظام لضمان دوام فعالية الاستراتيجية ودوام ملاءمتها. ويساعد ذلك في تحديد المخاطر المتصلة باستراتيجية محددة ومعالجتها، وإمكانية تكييف الاستراتيجية حسب اللزوم لبيان التغييرات الطارئة على البيئة موضوع الاستراتيجية. كما يساعد نهج إدارة دورة الحياة في ضمان مشاركة أصحاب المصلحة المعنيين كافة في إعداد الاستراتيجية وتنفيذها، وفهم جميع الجهات أدوارها ومسؤولياتها بوضوح. ويساعد ذلك بدوره في تنفيذ الاستراتيجية بفعالية وفي وحدة الغاية التي يعمل الجميع في سبيل تحقيقها. وأخيراً، يُتيح اعتماد مبادئ إدارة دورة الحياة رصد تنفيذ الاستراتيجية، وتقييم نتائجه، الأمر الذي يُتيح تصحيح المسار في الوقت المناسب عند اللزوم ويساعد في ضمان استمرار فعالية وملاءمة الاستراتيجية طوال الوقت.

3.2.1 هل تتضمن استراتيجية بلدكم الوطنية للأمن السيبراني آلية لضمان التشاور بانتظام مع خبراء الأمن السيبراني وأصحاب المصلحة في هذا المجال؟

الرمز- GCIv5: Org1.2.3

الأساس المنطقي-GCIv5: لمَّا كان المشهد الأمني السيبراني دائم التغير، فمن المهم وضع آلية تضمن تحديث الاستراتيجية الوطنية للأمن السيبراني بانتظام. ويستطيع خبراء الأمن السيبراني تقديم مساهمات قيمة بشأن أحدث التهديدات وأفضل سبل التصدي لها. ولا بد أيضاً من مشاورة أصحاب المصلحة كالشركات والمواطنين أثناء عملية الاستراتيجية لضمان نتائج سياساتية أكثر فعالية، إذ يمكنهم تقديم تعقيبات على كيفية سير الاستراتيجية واقتراحات لإجراء تحسينات. فبمشاورة الخبراء وأصحاب المصلحة، يمكن تكييف الاستراتيجية الوطنية للأمن السيبراني لتفي باحتياجات البلد.

4.2.1 هل يعتمد بلدكم خطة عمل/خريطة طريق محددتين لتنفيذ استراتيجيته للأمن السيبراني؟

الرمز- GCIv5: Org1.2.4

الأساس المنطقي-GCIv5: إن اعتماد خطة عمل أو خريطة طريق محددتين لتنفيذ استراتيجية الأمن السيبراني جزء حاسم من جهود حماية البنية التحتية الرقمية والمواطنين في الدولة. فدون خطة، يصعب تخصيص الموارد وقياس التقدم المحرز، فيؤدي ذلك إلى انعدام الفعالية ووجود ثغرات في مستوى التغطية. كما أن اعتماد خطة عمل/خريطة طريق محددة بوضوح يمكن أن يساعد في ضمان إدراك أصحاب المصلحة كافة أدوارهم ومسؤولياتهم في تنفيذ الاستراتيجية، وضمان إمكانية تحقيق الخطة وواقعيتها. ويساعد اعتمادها كذلك في تتبُّع وتقييم آثار تنفيذ الاستراتيجية على مدى الوقت، بحيث يتسنى إخضاعها لما قد يلزم من تعديلات.

11 https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

2 الوكالة المسؤولة

الرمز- GCIv5: Org2

الأساس المنطقي-GCIv5: الوكالة المسؤولة هي السلطة المختصة المنوطة بها مسؤولية إدارة الأمن السيبراني. وينبغي أن تكون هذه السلطة قائدةً (فرداً كانت أو كياناً) رفيعة المستوى ومستقرة في أعلى مستوى حكومي لتقدم التوجيه وتنسق الأعمال وترصد تنفيذ أنشطة الأمن السيبراني وبرامجه. وينبغي أيضاً أن تتصرف هذه السلطة الوطنية المختصة بصفة كيان إداري يعنى بتحديد وتوضيح الأدوار والمسؤوليات والعمليات وحقوق اتخاذ القرار والمهام اللازم تنفيذها لضمان فعالية هيكل الوضع الأمني السيبراني.

1.2 هل ببلدكم وكالة أو وزارة يختصان بالأمن السيبراني على الصعيد الوطني؟

الرمز- GCIv5: Org2.1

الأساس المنطقي-GCIv5: إن وجود وكالة أو وزارة وطنيين يختصان بالأمن السيبراني في البلد يمكن أن يدعم تماسك إدارة التهديدات الأمنية السيبرانية، واستباقية الإجراءات الأمنية السيبرانية. وينبغي أن تعمل هذه الوكالة أو هذه الوزارة مع سائر الدوائر الحكومية ومع القطاع الخاص والمجتمع المدني وسائر الجهات الفاعلة المعنية من أجل إعداد استراتيجية للأمن السيبراني وتنفيذها.

2.2 هل ببلدكم وكالة أو وزارة يختصان بالأمن السيبراني لأغراض حماية البنية التحتية الحيوية الوطنية؟

الرمز- GCIv5: Org2.2

الأساس المنطقي-GCIv5: إن وجود وكالة أو وزارة تُعنيان بالبنية التحتية الحيوية الوطنية يدعم مرونة العمليات واستمراريتها. ويمكن أن تشمل البنية التحتية الحيوية الخدمات الأساسية التي لا غنى عنها لنشاط المجتمع كخدمات المياه والكهرباء والاتصالات. ومن الممكن أن يساعد وجود وكالة أو وزارة وطنيين يعنيان بالبنية التحتية الحيوية في منع تعطل هذه الخدمات أو تخفيف آثار ذلك، بالعمل مع أصحاب المصلحة المعنيين.

3.2 هل ببلدكم وكالة أو وزارة أو فريق مهام أو هيئة أخرى تختص بالإشراف على تطوير القدرة الأمنية السيبرانية وطنياً؟

الرمز- GCIv5: Org2.3

الأساس المنطقي-GCIv5: إن انتهاج نهج منسق وشامل لتطوير المهارات والقدرات الأمنية السيبرانية اللازمة يمكن أن يحد من أرجحية وقوع الحوادث الأمنية السيبرانية ويحسِّن مستوى المرونة. والأمن السيبراني شاغل متعدد الأبعاد يستلزم التنسيق والتعاون من العديد من الوكالات الحكومية والكيانات الخاصة.

4.2 هل يدخل تنسيق مبادرات وأنشطة حماية الأطفال على الإنترنت في نطاق اختصاص أي من الوكالات أو الوزارات أو أفرقة المهام أو الهيئات الأخرى في بلدكم؟

الرمز- GCIv5: Org2.4

الأساس المنطقي-GCIv5: إن التنسيق بين أصحاب المصلحة والفئات المستهدفة، وضمان الإشراف على الأنشطة، مهميْن لضمان تكامل تدخلات حماية الأطفال على الإنترنت (COP). والتنسيق الوطني لمبادرات وأنشطة حماية الأطفال على الإنترنت يمكن أن يكون مسؤولية وكالة أو وزارة أو فريق مهام أو هيئة أخرى مستقلة، أو جزءاً من مجموعة أكبر من المسؤوليات التي تضطلع بها أي من هذه الكيانات.

3 مقاييس الأمن السيبراني

الرمز- GCIv5: Org3

الأساس المنطقي-GCIv5: تشمل مقاييس الأمن السيبراني جميع ما يُعترف بها رسيماً على الصعيد الوطني أو القطاعي من ممارسات للمعايرة القياسية أو مرجعيات تُستخدم لقياس مدى تطور القدرة الأمنية السيبرانية، واستراتيجيات لتقييم المخاطر، وعمليات للتدقيق الأمني السيبراني، وغيرها من أدوات وأنشطة تصنيف أو تقييم الأداء الناتج بهدف إجراء المزيد من التحسينات.

فعلى سبيل المثال، يتعلق المعيار 27004[12] الصادر عن المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC) بقياس إدارة أمن المعلومات.

1.3 هل تُجرى وطنياً أي عمليات تدقيق أمني سيبراني؟

الرمز- GCIv5: Org3.1

الأساس المنطقي-GCIv5: قد تُجرى عمليات التدقيق الأمني السيبراني على الصعيد الوطني لشواغل أمنية أو بموجب اللوائح الأمنية أو غيرها من الوثائق التوجيهية الأمنية. وفي حين يسهم الأمن السيبراني في تدقيق اللوائح، من اللازم أن تُنفذ على الصعيد الوطني عمليات تدقيق فعالة للأمن السيبراني. وقد تصدر نواتج هذه العمليات في هيئة تقارير أو موجزات أو عروض تقديمية أو مذكرات أو ما شابه من مواد.

والتدقيق الأمني السيبراني هو تحديد مواطن الضعف المحتمل وجودها. وحال تحديدها، يمكن تقييمها وترتيبها بحسب الأولوية بغرض تحديد مستوى الخطر الذي تشكله للمنظمة المعنية. وتتنوع الأدوات التي يمكن استخدامها لتقييم مواطن الضعف هذه، ومن بينها ماسحات مواطن الضعف، ومختبرو إمكانية الاختراق، وتمارين الأفرقة الحمراء. ولكل من هذه الأدوات مواطن قوته ومواطن ضعفه، فمن المهم اختيار الأداة المناسبة للمهمة. وبمجرد تحديد مواطن الضعف الأمني السيبراني، من المهم تحديد مستوى الخطر الذي يشكله كل منها للمنظمة.

2.3 هل توجد مقاييس/أدوات لتقييم المخاطر الأمنية السيبرانية على الصعيد الوطني؟

الرمز- GCIv5 Org3.2

الأساس المنطقي-GCIv5: تختلف مقاييس تقييم المخاطر الأمنية السيبرانية على الصعيد الوطني بين البلدان، وينبغي أن تبين التهديدات والقدرات والتحديات الخاصة بكل بلد. ويمكن تحقيق ذلك باستخدام مجموعة متنوعة من المقاييس منها العوامل المؤثرة، وعوامل الاحتمال، وقيم الأصول. فباستخدام هذه المقاييس، يمكن تحديد مستوى الخطر الذي يشكله كل من مواطن الضعف ودرجة شدته، ثم اتخاذ الإجراء التصحيحي المناسب.[13] ويقدم المعيار 27004[14] الصادر عن المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC) تقنيات أمنية يمكن استخدامها لرصد المخاطر الأمنية السيبرانية وقياسها وتحليلها وتقييمها.

3.3 هل تعتمدون تدابير لتقييم مستوى تطور القدرة الأمنية السيبرانية وطنياً باستخدام أدوات من قبيل نموذج اكتمال القدرة الأمنية السيبرانية أو مقياس الجاهزية السيبرانية أو أي أدوات تقييم أخرى تتعلق بذلك؟

الرمز- GCIv5: Org3.3

الأساس المنطقي-GCIv5: يمكن لتقييم مستوى تطور القدرة الأمنية السيبرانية أن يمكّن البلد من إدراك درجة اكتمال وموثوقية بنيته التحتية للأمن السيبراني، وقد تختلف بين البلدان تدابير التقييم المحددة لذلك. ومن الأدوات الشائعة الاستخدام لتقييم مستوى تطور القدرة الأمنية السيبرانية وطنياً نموذج اكتمال القدرة الأمنية السيبرانية[15] ومقياس الجاهزية السيبرانية[16] أو أي تدبير آخر قد يتخذه البلد. وتُستثنى من أدوات التقييم في هذا السؤال مشاركة البلد في الرقم القياسي العالمي للأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات.

4 استراتيجيات ومبادرات حماية الأطفال على الإنترنت

الرمز- GCIv5: Org4

الأساس المنطقي-GCIv5: حماية الأطفال على الإنترنت (COP) هو المصطلح الجامع للاستراتيجيات والمبادرات الرامية إلى حماية الأطفال من التعرض للإيذاء أو الاستغلال عند نفاذهم إلى الإنترنت. ويمكن أن يشمل ذلك ضمان أن يستخدم الأطفال

12 https://www.iso.org/standard/64120.html
13 https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf
14 https://www.iso.org/standard/64120.html
15 https://gcscc.ox.ac.uk/cmm-2021-edition
16 https://www.potomacinstitute.org/images/CRIndex2.0.pdf

برمجيات تناسب أعمارهم وأدوات غربلة، وصولاً إلى تثقيف الوالدين والأطفال بسبل البقاء بأمان على الإنترنت. وتوجد طائفة متنوعة من الاستراتيجيات والمبادرات المنفذة لحماية الأطفال على الإنترنت، والمكيَّفة عادةً لتلبي احتياجات الطفل الخاصة في البلد المستهدف بهذه الاستراتيجيات والمبادرات.

1.4 هل يعتمد بلدكم استراتيجية وطنية لحماية الأطفال على الإنترنت، تقترن بالمبادرات الحالية لحماية الأطفال على الإنترنت؟

الرمز- GCIv5: Org4.1

الأساس المنطقي-GCIv5: توصي المبادئ التوجيهية لحماية الأطفال على الإنترنت بتخصيص استراتيجية شاملة منفصلة لحماية الأطفال على الإنترنت، وبضرورة أن تغطي هذه الاستراتيجية المجالات المتعلقة بالطفل كالصحة والعافية وتنمية المهارات. أما تضمين استراتيجية حماية الأطفال على الإنترنت في مواد أخرى، فغالباً ما يجعلها غير شاملة، بحيث يقتصر تركيزها على قضية الاعتداء الجنسي على الأطفال أو استخدامهم في المواد الإباحية.

2.4 هل تُنفَّذ في بلدكم على الصعيد الوطني أي آليات وقدرات إبلاغ حكومية للمساعدة في حماية الأطفال على الإنترنت؟

الرمز- GCIv5: Org4.2

الأساس المنطقي-GCIv5: إن إتاحة آليات إبلاغ للجمهور العام تسمح بتمييز المسائل المتصلة بالأطفال على الإنترنت وتتبعها ومتابعتها تمكِّن الأفراد من تمييز المشاكل المؤثرة على الأطفال على الإنترنت والإبلاغ عنها. وقد تتضمن هذه الآليات أيضاً قدرات تقنية كالإنذار بالمحتوى. ويمكن لأفرقة التصدي للحوادث الحاسوبية وأجهزة إنفاذ القانون أن تقدم آليات إبلاغ. وفي الوضع الأمثل، ينبغي توفر مجموعة متنوعة من أنظمة الإبلاغ كالخطوط الهاتفية الوطنية للمساعدة، أو البوابات الوطنية على الإنترنت، المزودة بأنظمة إحالة ودعم.

تدابير تنمية القدرات

الأساس المنطقي-GCIv5: تشكل تنمية القدرات جزءاً أصيلاً من التدابير القانونية والتقنية والتنظيمية المشمولة بالرقم القياسي العالمي للأمن السيبراني، وقوة محرِّكة للتنمية الرقمية. وتهدف برامج تنمية القدرات إلى بناء المهارات والمعارف والثقة على الصعيد المحلي، ومن ثم سد الفجوات الرقمية وبناء نظام إيكولوجي للتكنولوجيا أشمل للجميع. علاوةً على ذلك، يتزايد في الوقت الحاضر اعتماد القدرة على تقديم خدمات رقمية شاملة للجميع على وجود قوى عاملة ماهرة. وقد تشمل أطر بناء القدرات لتعزيز الأمن السيبراني التوعية، ويمكن قياس هذه الأطر بمدى وجود برامج البحث والتطوير والبرامج التعليمية والتدريبية والمهنيين المعتمدين وهيئات القطاع العام المعتمدة، وبعدد هذه البرامج والكيانات.

1 حملات التوعية العامة في مجال الأمن السيبراني

الرمز- GCIv5: CapDev1

الأساس المنطقي-GCIv5: إن حملات التوعية العامة في مجال الأمن السيبراني تهدف أساساً إلى الحض على اعتماد سلك سلوكيات مأمونة على الإنترنت. ولتحقِّق هذه الحملات تغييرات سلوكيات هادفة، لا بد من أن تُقنع الناس بأهمية المعلومات المقدمة، وتساعدهم على فهم كيفية الاستجابة، وتحملهم على الرغبة في الاستجابة في ضوء أولويات أخرى.[17] إلا أن حملات التوعية تواجه تحديات متعددة، خاصةً لكونها تتطلب قدراً كبيراً من الجهود والمهارات ولأن "إثارة مشاعر الخوف نادراً ما تُحدث تغييرات سلوكية."[18] ويمكن لحملات التوعية الموجهة أن تكيِّف تدخلاتها لتعالج هذه الشواغل بكيفية أفضل.

1.1 هل تنظم حكومتكم حملات توعية عامة تستهدف الشركات البالغة الصغر والصغيرة والمتوسطة تحديداً؟

الرمز- GCIv5: CapDev1.1

---

17 Rogers, R.W. Attitude change and information integration in fear appeals. Psychological Reports, 56, (1985) 183–188
Witte, K. Message and conceptual confounds in fear appeals: The role of threat, fear and efficacy. The Southern Communication Journal, 58(2), (1993) 147-155 https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8

18 https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8

الأساس المنطقي-GCIv5: تشكل الشركات البالغة الصغر والصغيرة والمتوسطة (SME) جزءاً حيوياً من اقتصاد البلد ويلزمها أن تكون على علم بالتهديدات الأمنية السيبرانية التي قد تؤثر عليها. وتواجه هذه الشركات تحديات خاصة فيما يتعلق بتحسين أمنها السيبراني كنقص الموارد والخبرة التقنية، وبتنفيذ تدخلات موجهة، يمكن معالجة هذه التحديات الخاصة والتركيز على تحقيق أقصى تأثير ممكن لفائدة هذا الشركات. وحملات التوعية في مجال الأمن السيبراني، وبخاصة الموجهة منها إلى الشركات البالغة الصغر والصغيرة والمتوسطة، يمكن أن تزود هذه الشركات بمعلومات عن كيفية حماية أنفسها من الهجمات السيبرانية، وكذلك عن كيفية الاستجابة إن هوجمت.

2.1 هل تنظم حكومتكم حملات توعية عامة تستهدف تحديداً القطاع الخاص إجمالاً؟

الرمز- GCIv5 CapDev1.2

الأساس المنطقي-GCIv5: تواجه جميع الجهات الفاعلة في القطاع الخاص تحديات أمنية سيبرانية. وإلى جانب تلبية الاحتياجات الخاصة للشركات البالغة الصغر والصغيرة والمتوسطة، يمكن أن تساعد حملات التوعية العامة بالمخاطر الأمنية السيبرانية التي يواجهها القطاع الخاص في تحسين السلوك.

3.1 هل تنظم حكومتكم حملات توعية عامة تستهدف تحديداً هيئات القطاع العام على الأصعدة المحلي والبلدي والوطني، والعاملين فيه؟

الرمز- GCIv5 CapDev1.3

الأساس المنطقي-GCIv5: يمكن أن تستفيد هيئات القطاع العام من حملات التوعية في مجال الأمن السيبراني. وتستهدف هذه الحملات تحديداً العاملين في القطاع العام، وتقدم معلومات مهمة عن كيفية حماية المعلومات والبنى التحتية الحساستين.

4.1 هل تنظم حكومتكم حملات توعية عامة تستهدف المجتمع المدني تحديداً؟

الرمز- GCIv5 CapDev1.4

الأساس المنطقي-GCIv5: من الممكن أن تكون منظمات المجتمع المدني أهدافاً للهجمات السيبرانية. وقد تتضمن هذه الهجمات التحرش أو سرقة البيانات أو تزوير المعلومات المالية، عبر الإنترنت. ولا بد لمنظمات المجتمع المدني من أن تعي هذه المخاطر وتحمي أنفسها، وهو ما يشمل تدريب الموظفين واستخدام كلمات سر مأمونة وتحديث برمجيات مكافحة الفيروسات. وبوسع البلدان أن تساعد في حماية هذه المنظمات الحيوية من التضرر بتوعيتها لمساعدتها على الدفاع عن أنفسها وشبكاتها وبيانات المواطنين لديها بأمان.

5.1 هل تنظم حكومتكم حملات توعية عامة تستهدف السكان عموماً؟

الرمز- GCIv5 CapDev1.5

الأساس المنطقي-GCIv5: الأمن السيبراني ليس حكراً على الشركات والحكومات. فالمواطنون هم أكثر الفئات عرضةً على الإطلاق للجريمة السيبرانية، إلا أنه عادةً ما تنقصهم المعرفة والأدوات اللازمتان لحماية أنفسهم. والمجرمون السيبرانيون دائمو البحث عن طرق جديدة لسرقة البيانات أو الأموال أو الهويات، وبإمكانهم تنفيذ ذلك باختراق الأنظمة الحاسوبية أو سرقة كلمات السر أو إنشاء مواقع إلكترونية مزيفة. وعلى الصعيد الوطني، تستطيع الحكومات توعية مواطنيها لحمايتهم، بل ينبغي لها تثقيفهم ليتمكنوا من حماية أنفسهم باستخدام كلمات سر متينة أمنياً، وتوخي الحذر عند فتح الرسائل الإلكترونية، وعدم إعطاء الغير معلومات شخصية بتاتاً عبر الإنترنت. كما ينبغي توعيتهم بنُذُر النصب الإلكتروني أو هجمات التصيد. فينبغي للحكومات أن تلتزم بتوعية مواطنيها كافة في مجال الأمن السيبراني وتحث الجميع على اتخاذ الإجراءات اللازمة لحماية أنفسهم على الإنترنت.

6.1 هل تنظم حكومتكم حملات توعية عامة تستهدف كبار السن (المسنين) تحديداً؟

الرمز- GCIv5 CapDev1.6

الأساس المنطقي-GCIv5: مع استمرار شيخوخة السكان، يتزايد عدد كبار السن الذين سيستخدمون الإنترنت والأجهزة الإلكترونية. ومما يؤسف له أن ذلك يجعلهم هدفاً رئيساً للمجرمين السيبرانيين. فكبار السن أكثر عرضةً من غيرهم للتهديدات السيبرانية لعدة أسباب، وهي أنهم قد لا يعون بنفس الدرجة المخاطر المقترنة باستخدام الإنترنت، وقد تنقصهم المهارات التقنية اللازمة لحماية أنفسهم عليها، وربما من الأرجح أن يقعوا ضحايا للنصب الإلكتروني، بينما من المستبعد أن يبادروا إلى الإبلاغ عن وقوع جريمة سيبرانية.

ولهذه الأسباب، تنظم البلدان حالياً حملات توعية في مجال الأمن السيبراني لسكانها المسنين ليبقوا بأمان على الإنترنت ويتمكنوا من حماية معلوماتهم الشخصية.

7.1 هل تنظم حكومتكم حملات توعية عامة تستهدف الأشخاص ذوي الاحتياجات الخاصة تحديداً بمن فيهم الأشخاص ذوو الإعاقة؟

الرمز- GCIv5: CapDev1.7

الأساس المنطقي-GCIv5: في ظل تزايد التحول من نموذج الإعاقة الطبي إلى نموذجها القائم على حقوق الإنسان، فإن كسر الحواجز المجتمعية التي يواجهها الأشخاص ذوو الاحتياجات الخاصة "كالحواجز الهيكلية وحواجز الاتصال ومواقف المجتمع وبُناه"[19]يمكن أن يحسِّن قدرات الأشخاص ذوي الإعاقة وسلامتهم. وبالتوازي، تزداد كذلك الحاجة إلى تنفيذ أنشطة للتوعية والتدريب في مجال الأمن السيبراني تستهدف هؤلاء الأشخاص تحديداً. فالأشخاص ذوو الإعاقة أكثر عرضة من غيرهم للهجمات السيبرانية لعدد من الأسباب منها نقص درايتهم التكنولوجية، واعتمادهم على مساعدة الآخرين، وإحجامهم أيضاً عن طلب المساعدة. فلا غنى عن تثقيفهم وتوعيتهم، ولا بد من أن تضمن الحكومات شمول كل أفراد المجتمعات بما نبذله من جهود في ميدان الأمن السيبراني. وتلبية احتياجات هذه الفئة من السكان من حملات التوعية العامة مسألة مهمة لتطوير القدرة الأمنية السيبرانية تطويراً فعالاً وشاملاً للجميع.

8.1 هل تنظم حكومتكم أي حملات توعية عامة تستهدف الوالدين والمربين والأطفال، على وجه التحديد، في إطار جهود حماية الأطفال على الإنترنت (COP)؟

الرمز- GCIv5 CapDev1.8

الأساس المنطقي-GCIv5: ينبغي أن تشجِّع الحكومات على استحداث حملات توعية عامة تستهدف الوالدين والمربين تحديداً لتمكينهما من جني مزيد من المعرفة عن المخاطر وصنوف الأذى التي قد يتعرض لها الأطفال والشباب على الإنترنت، وزيادة قدرتهما على التعامل مع المسائل المتصلة بحماية الأطفال على الإنترنت.

9.1 هل تنظم حكومتكم أي حملات توعية عامة تستهدف الأطفال تحديداً في إطار جهود حماية الأطفال على الإنترنت (COP)؟

الرمز- GCIv5 CapDev1.9

الأساس المنطقي-GCIv5: يصبح الأطفال عرضة للتهديدات السيبرانية مع طول المدة الزمنية التي يمضونها على الإنترنت. وهم شديدو العرضة لهذه التهديدات لاحتمال عدم وعيهم بهذه الأخطار وعدم معرفتهم وخبرتهم بالأمن السيبراني بنفس درجة وعي ومعرفة وخبرة الأشخاص البالغين بهما. لذا، ينبغي أن تشجِّع الحكومات على تنظيم حملات توعية عامة تستهدف الأطفال لمساعدتهم في اكتساب المعرفة بمختلف المخاطر التي قد يواجهونها على الإنترنت، بهدف تحسين قدرتهم على تمييز هذه المخاطر وعلى تخفيف آثارها، وتشجيعهم على سلك سلوكيات مسؤولة على الإنترنت.

2 تدريب المهنيين العاملين في مجال الأمن السيبراني

الرمز- GCIv5 CapDev2

الأساس المنطقي-GCIv5: إن تنمية مهارات القوى العاملة المشتغلة بالأمن السيبراني يمكن أن يدعم اقتدارها وحداثتها. ويقتضي تدريب القوى العاملة المشتغلة بهذا المجال جهوداً متواصلة تواكب ما يستجد فيه من تغيرات وتطورات.

1.2 هل تُعِد حكومتكم أو تدعم إعداد دورات تدريبية في مجال الأمن السيبراني للمهنيين العاملين في هذا المجال؟

الرمز- GCIv5 CapDev2.1

الأساس المنطقي-GCIv5: مع تزايد عدد الشركات التي تنقل عملياتها إلى شبكة الإنترنت، أصبحت الحاجة إلى مهنيي الأمن السيبراني أكبر من أي وقت سابق. لكن مع الشائع جداً أن يعوز هؤلاء المهنيين التدريب اللازم لحماية الموظفين من الهجمات

[19] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e777?rskey=sn89T4&result=201&prd=MPIL#

السيبرانية. وتقديم التدريب في مجال الأمن السيبراني مهم لعدة أسباب منها المساعدة في تأسيس مهنيي الأمن السيبراني في هذا المجال، ومساعدتهم في بناء قدرتهم على تطبيق معارفهم عملياً، وفي إدامة إحاطتهم بأحدث الاتجاهات وآخر التطورات في مجال الأمن السيبراني، ومساعدتهم أيضاً في اكتساب المهارات اللازمة لتأمين شبكات وبيانات المنظمات التي يعملون بها.

2.2 هل ببلدكم برامج لاعتماد مهنيي الأمن السيبراني معترف بها محلياً أو دولياً؟

الرمز- GCIv5: CapDev2.2

الأساس المنطقي-GCIv5: تساعد برامج الاعتماد في مجال الأمن السيبراني في ضمان تقيد المهنيين العاملين في هذا المجال بأعلى المعايير. ويمكن أن يساعد ذلك في تحسين نوعية مهنيي الأمن السيبراني إجمالاً وحماية الأفراد والمنظمات من التضرر. إضافةً إلى ذلك، بمقدور البلدان أن تبني الثقة بين مهنيي الأمن السيبراني وعملائهم، إذ إن توفر برنامج اعتماد معترف به عالمياً يمكن أن يساعد في ضمان ثقة جميع الأطراف المعنية في مؤهلات المهنيين الذين تعمل معهم.

3.2 البرامج التثقيفية/الدورات التدريبية الوطنية لقطاعات محددة في مجال الأمن السيبراني المقدمة إلى المهنيين

الرمز- GCIv5: CapDev2.3

الأساس المنطقي-GCIv5: يمكن أن يستفيد المهنيون في شتى القطاعات في البلد من تنفيذ برامج تثقيفية/دورات تدريبية في مجال الأمن السيبراني تعالج ما يؤرقهم من شواغل وما يواجهونه من مواقف محددة، وتُكسبهم المهارات المناسبة اللازمة لهم.

1.3.2 هل تُعِد حكومتكم أو تدعم إعداد برامج تثقيفية أو دورات تدريبية في مجال الأمن السيبراني لموظفي إنفاذ القانون، على الصعيد الوطني؟

الرمز- GCIv5: CapDev2.3.1

الأساس المنطقي-GCIv5: تضطلع الجهات الفاعلة المعنية بإنفاذ القانون كضباط الشرطة وموظفي إنفاذ القانون دوراً حاسماً في المساعدة في حماية البلد من الهجمات السيبرانية. إذ يمكنهم المساعدة في كشف الجرائم السيبرانية والتحقيق فيها والعمل مع الشركات والمنظمات الأخرى لتحسين وضعها الأمني السيبراني. ويلزم تزويد موظفي إنفاذ القانون بالمعارف والأدوات اللازمة للتصدي لهذه التهديدات المتنامية. وتلقّيهم التدريب في مجال الأمن السيبراني يمكن أن يساعدهم في تحسين إدراكهم لأحدث التهديدات، وكشف الأنشطة الضارة، وحماية شبكات الشركات والمنظمات.

2.3.2 هل تُعِد حكومتكم أو تدعم إعداد برامج تثقيفية أو دورات تدريبية في مجال الأمن السيبراني للجهات الفاعلة القضائية الوطنية، على الصعيد الوطني؟

الرمز- GCIv5: CapDev2.3.2

الأساس المنطقي-GCIv5: تؤدي الجهات الفاعلة القضائية الوطنية دوراً فائق الأهمية في ضمان سلامة بلدانها وأمنها، ويلزم تزويدها بالمعارف والأدوات اللازمة للتعامل مع التهديدات الأمنية السيبرانية. فالتخطيط لتقديم دورات تدريبية وطنية في مجال الأمن السيبراني، لا بد من النظر في تقديمها إلى الجهات الفاعلة القضائية والجهات الفاعلة القانونية الأخرى، وتقديم التدريب المهني والتقني دورياً إلى القضاة والمستشارين القانونيين والمحامين بالقضاء العالي والوكلاء القانونيين والمحامين والمساعدين القانونيين وغيرهم من العاملين في المهن القانونية ومهن إنفاذ القانون.

3.3.2 هل تُعِد حكومتكم أو تدعم إعداد برامج تثقيفية أو دورات تدريبية في مجال الأمن السيبراني للشركات البالغة الصغر والصغيرة والمتوسطة؟ [سؤال دون درجات]

الرمز- GCIv5: CapDev2.3.3

الأساس المنطقي-GCIv5: تحتاج الشركات البالغة الصغر والصغيرة والمتوسطة (MSME) إلى التدريب في مجال الأمن السيبراني لأنها تحتفظ بكم كبير من البيانات الحساسة، التي قد تُسرق أو يُعبث بها في حال تعرض هذه الشركات لهجمات سيبرانية. إضافةً إلى ذلك، فغالباً ما لا تدرك هذه الشركات المخاطر المقترنة باستخدام التكنولوجيا وقد لا تمتلك الأدوات أو الموارد اللازمة لحماية بياناتها، وتقديم التدريب إليها في مجال الأمن السيبراني يمكن أن يساعدها في فهم المخاطر المصاحبة لاستخدام التكنولوجيا وكيفية حماية بياناتها. فضلاً عن ذلك، فإن تلقّي هذه الشركات التدريب في هذا المجال يمكن أن يساعدها في تمييز الأنشطة المشبوهة والتصدي للهجمات السيبرانية. وبتزويد الشركات البالغة الصغر والصغيرة والمتوسطة بما يلزمها من أدوات ومعارف لحماية بياناتها، تساعد البلدان بالتالي في حماية تنميتها الاقتصادية.

4.3.2 هل تُعِد حكومتكم أو تدعم إعداد برامج تثقيفية أو دورات تدريبية في مجال الأمن السيبراني للقطاع الخاص بوجه عام؟

الرمز- GCIv5: CapDev2.3.4

الأساس المنطقي-GCIv5: يواجه القطاع الخاص بوتيرة متزايدة مخاطر سيبرانية متنامية الحجم والنطاق والتعقيد تؤثر على مالية الشركات وسمعتها وممتلكاتها. ونظراً إلى أن التكنولوجيا ليست سوى مكوناً واحداً من مكونات الأمن السيبراني، فتنفيذ سياسات وبرامج تستهدف تغيير سلوكيات الأشخاص في القطاع الخاص يمكن أن يحسن مرونته ويحد من تعرضه لمخاطر سيبرانية.

5.3.2 هل تُعِد حكومتكم أو تدعم إعداد برامج تثقيفية أو دورات تدريبية في مجال الأمن السيبراني لموظفي القطاع العام/الحكومة بوجه عام؟

الرمز- GCIv5 CapDev2.3.5

الأساس المنطقي-GCIv5: يقدم القطاع العام إلى المواطنين والشركات خدمات أساسية، ولتقديمها تقديماً مأموناً، يلزم الجهات الفاعلة في القطاع العام التمتع بإدراك أمني سيبراني قوي ومعرفة كيفية حماية أنفسها وعملائها من التهديدات الرقيمة. لذا، يمكن أن يستفيد موظفو القطاع العام/الحكومة من تنفيذ برامج ودورات تدريبية تثقيفية في مجال الأمن السيبراني.

6.3.2 هل تُعِد حكومتكم أو تدعم إعداد برامج تثقيفية أو دورات تدريبية في مجال الأمن السيبراني للجهات الفاعلة في قطاعات المالية و/أو الصحة و/أو الاتصالات و/أو النقل و/أو الطاقة؟

الرمز- GCIv5 CapDev2.3.6

الأساس المنطقي-GCIv5: تختلف الشواغل الأمنية السيبرانية في الغالب باختلاف القطاع. وبالنظر إلى الأدوار الحاسمة التي تؤديها قطاعات المالية والصحة والاتصالات والنقل والطاقة، فإن توجيه دورات تدريبية إلى هذه الجهات الفاعلة يمكن أن يدعم الوضع الأمني السيبراني العام في البلد.

7.3.2 هل تُعِد حكومتكم أو تدعم إعداد برامج تعليمية أو دورات تدريبية في مجال الأمن السيبراني للشباب؟

الرمز- GCIv5 CapDev2.3.7

الأساس المنطقي-GCIv5: عادةً ما تتدخل الحكومات لتصحح المؤثرات الخارجية السلبية في السوق، وتدعم الفئات التي لولا تدخلها لعانت من نقص الخدمات. وإعداد برامج تعليمية ودورات تدريبية، ودعم إعدادها، في مجال الأمن السيبراني ميدان قد لا يحقق فيه القطاع الخاص عائدات كبيرة تشجعه على تحفيز المشاركة فيه. لكنَّ بوسع الحكومات أن تقدم الدعم إلى الشباب في هذا الميدان بسبل منها تقديم المِنح المالية والدعم الدراسي والدعم التدريبي. وقد يكون الشباب الذي يفكر في العمل في مجال الأمن السيبراني أحوج إلى هذا الدعم لافتقارهم إلى رأس المال اللازم للاستثمار في تعليم أنفسهم على حسابهم الخاص.

8.3.2 هل تُعِد حكومتكم أو تدعم إعداد برامج تثقيفية أو دورات تدريبية في مجال الأمن السيبراني للمربين كالبرامج التثقيفية لحماية الأطفال على الإنترنت؟

الرمز- GCIv5 CapDev2.3.8

الأساس المنطقي-GCIv5: يملك المربون غرس السلوكيات الأمنية السيبرانية الإيجابية في الأطفال والشباب بحكم دورهم في تربية الأطفال والشباب. وحرص البلد على تقديم التدريب إلى المربين بشأن قضايا الأمن السيبراني كحماية الأطفال على الإنترنت إنما يبرهن على أنه يعمل في سبيل تنفيذ تدابير أمنية سيبرانية طويلة الأمد، بدعم المربين العاملين مع الجيل المقبل من مستخدمي الإنترنت عند نفاذهم إليها.

3 البرامج التعليمية المتعلقة بالأمن السيبراني في إطار المناهج الأكاديمية الوطنية

رمز-GCIv5 CapDev3

الأساس المنطقي-GCIv5: من أجل تعزيز إلمام السكان بأمور الأمن السيبراني، يتيح إدماجُ المبادئ الأساسية للأمن السيبراني في المناهج الأكاديمية الوطنية تزويدَ الطلاب من جميع الأعمار بالمهارات اللازمة لمواجهة المخاطر المتعلقة بالأمن السيبراني بشكل أفضل.

1.3 هل تقوم حكومتكم بوضع أو دعم أي برامج تعليمية بشأن الأمن السيبراني في إطار المناهج الأكاديمية في التعليم الابتدائي؟

الرمز-GCIv5: CapDev3.1

الأساس المنطقي-GCIv5: يستهلّ أطفال المدارس الابتدائية، أو أولئك الذين هم في المرحلة 1 من التصنيف الدولي الموحد للتعليم (ISCED)، تعليمهم الدراسي، ويقومون عادة بتعلّم المهارات الأساسية في مجال القراءة والكتابة والرياضيات.[20] وإدراج الأنشطة الرامية إلى بناء الأسس اللازمة لانتهاج سلوك يضمن الأمن السيبراني من شأنه أن يساعد على زيادة الوعي والأمن السيبرانيين مدى الحياة. ولكن قد لا يتحلى الأطفال في هذه المرحلة بالمهارات الفكرية النقدية وبالقدرة اللازمة التي تمكّنهم من تقييم مخاطر الأمن السيبراني بشكل مستقل، وبالتالي فإنهم معرّضون للخطر بوجه خاص.[21] ويمكن أن تشمل الأنشطة في هذه المرحلة أنشطة متعلقة بحماية الأطفال على الإنترنت.

2.3 هل تقوم حكومتكم بوضع أو دعم أي برامج تعليمية متعلقة بالأمن السيبراني في إطار المناهج الأكاديمية للتعليم الثانوي؟

الرمز-GCIv5: CapDev3.2

الأساس المنطقي-GCIv5: يشارك تلاميذ التعليم الثانوي، الذين يتبعون البرامج الدراسية المتعلقة بالمستويين 2 و3 من التصنيف الدولي الموحد للتعليم، في الأنشطة التعليمية التي تهدف إلى "إرساء الأساس اللازم للتعلم مدى الحياة وتحقيق التنمية البشرية مما يمكّن أنظمة التعليم من تعزيز نطاق الفرص التعليمية"، كما أنها "مصممة لإنجاز التعليم الثانوي تحضيراً للتعليم العالي أو لتوفير المهارات اللازمة للعمل، أو كلاهما."[22] إن إدراج موضوع الأمن السيبراني في هذه المرحلة من شأنه أن يساعد ليس فقط على تزويد التلاميذ بالمهارات اللازمة لزيادة أمنهم على الإنترنت، وإنما على إثارة اهتمامهم أيضاً مما قد يؤدي إلى انتهاجهم مساراً وظيفياً في مجال التكنولوجيا والأمن السيبراني.

3.3 هل تقوم حكومتكم بوضع أو دعم أي برامج تعليمية متعلقة بالأمن السيبراني في إطار المناهج الأكاديمية للتعليم العالي؟

الرمز-GCIv5: CapDev3.3

الأساس المنطقي-GCIv5: إن الطلاب في مرحلة التعليم العالي، المعروفة أيضاً باسم المستوى 5-8 من التصنيف الدولي الموحد للتعليم، يكونون في غالب الأحيان قد أكملوا دورات التعليم الإلزامي. ويمكن أن تشمل برامج التعليم العالي دورات تدريبية ترمي إلى ما يلي: تزويد المشاركين بالمعارف والمهارات والكفاءات المهنية اللازمة (المستوى 5 من التصنيف)؛ وتزويد المشاركين بالمعارف والمهارات والكفاءات الأكاديمية و/أو المهنية المتوسطة، مما يتيح نيل شهادة من الدرجة الأولى أو على ما يعادلها من مؤهلات (المستوى 6 من التصنيف)؛ وتزويد المشاركين بالمعارف والمهارات والكفاءات الأكاديمية و/أو المهنية المتقدمة مما يتيح نيل شهادة من الدرجة الثانية أو على ما يعادلها من مؤهلات، مثل شهادة ماستر أو مستوى مكافئ (المستوى 7 من التصنيف)؛ أو مما يتيح نيل مؤهلات متقدمة في مجال البحوث، مثل مؤهلات بمستوى دكتوراه (المستوى 8 من التصنيف).[23] إن تناول موضوع الأمن السيبراني في هذه المراحل التعليمية من شأنه أن يدعم إيجاد قوة عاملة ملمّة بالأمور السيبرانية وقادرة على معالجتها، وأن يعزّز تنمية القدرات لأغراض البحث والتطوير.

4 برامج البحث والتطوير (R&D) في مجال الأمن السيبراني

الرمز-GCIv5: CapDev4

الأساس المنطقي-GCIv5: يمكن لأنشطة البحث والتطوير في القطاعات العامة والخاصة والأكاديمية أن تدعم الجهود المبذولة في مجال الأمن السيبراني من خلال تنمية القدرات البشرية وتطوير تقنيات ومنتجات جديدة وتحسين فهم المخاطر وسبل التخفيف منها. ويمكن أن تشمل أنشطة البحث والتطوير حلولاً تقنية وغير تقنية.

---

20 http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

21 https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity/

22 http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

23 http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

1.4 هل تقوم الجهات الفاعلة في القطاع الخاص في بلدكم بأنشطة بحث وتطوير مرتبطة بالأمن السيبراني؟

الرمز-GCIv5: CapDev4.1

الأساس المنطقي-GCIv5: تُظهر أنشطة البحث والتطوير التي يقودها القطاع الخاص استعداد القطاع الخاص للاستثمار في الأنشطة التي تعزز النمو والابتكار في مجال الأمن السيبراني، وفي تحسين حلول الأمن السيبراني المتاحة في السوق.

2.4 هل تقوم الجهات الفاعلة في القطاع العام الوطني في بلدكم بأنشطة بحث وتطوير متصلة بالأمن السيبراني؟

الرمز-GCIv5: CapDev5.2

الأساس المنطقي-GCIv5: إن قيام الجهات الفاعلة في القطاع العام بالمشاركة بصورة فعالة في أنشطة البحث والتطوير المتصلة بالأمن السيبراني يمكن أن يسهم في تحسين تحديد الثغرات التي تعتري البنية التحتية للأمن السيبراني في البلد ومعالجتها. كما يمكن أن يشجّع ذلك على إيجاد حلول الأمن السيبراني التي يمكن اعتمادها لحماية البنية التحتية الحيوية للبلد. ويمكن لأنشطة البحث والتطوير المتصلة بالأمن السيبراني التي يضطلع بها القطاع العام أن تتيح أيضاً الاستعداد للتصدي للهجمات السيبرانية. وتحقيقاً لهذه الغاية، ينبغي أن تكون الجهات الفاعلة في القطاع العام تابعة للحكومة الوطنية وليس لولاية أو حكومة محلية.

3.4 هل تنفذ الهيئات الأكاديمية في بلدكم أنشطة بحث وتطوير متصلة بالأمن السيبراني؟

الرمز-GCIv5: CapDev5.3

الأساس المنطقي-GCIv5: تؤدي الهيئات الأكاديمية دوراً أساسياً في أنشطة البحث والتطوير المتصلة بالأمن السيبراني. وتساهم في أحدث البحوث وفي الأنماط الفكرية الجديدة، وتقوم بتدريب الجيل التالي من المهنيين، وتعمل كصلة وصل مع القطاعين العام والخاص.

4.4 هل يجري في بلدكم تنفيذ برامج/مبادرات لتقييم الأمن السيبراني لمنتجات تكنولوجيا المعلومات والاتصالات، مثل برامج وضع العلامات أو إصدار الشهادات؟

الرمز-GCIv5: CapDev4.2

الأساس المنطقي-GCIv5: يمكن أن تساعد نظم إصدار الشهادات ووضع العلامات، التي يجري بموجبها تقييم الأمن السيبراني لمنتجات تكنولوجيا المعلومات والاتصالات، في تشجيع المصنعين على زيادة معايير الأمن السيبراني، وفي تحقيق المساءلة، وفي تيسير اختيار المستهلكين للمنتجات. وقد تنفّذ البلدان أنواعاً مختلفة من النظم بناء على سياقاتها واحتياجاتها الوطنية.

5 صناعة الأمن السيبراني الوطنية

الرمز-GCIv5: CapDev5

الأساس المنطقي-GCIv5: يمكن أن يؤدي تطوير ودعم صناعة الأمن السيبراني الوطنية إلى تعزيز القدرة المحلية على التصدي للتحديات المتعلقة بالأمن السيبراني وتحسين الأمن السيبراني، ويمكن أن يؤديا إلى إدارة استباقية للأمن السيبراني.

1.5 هل توجد في بلدكم صناعة محلية للأمن السيبراني؟

الرمز-GCIv5: CapDev5.1

الأساس المنطقي-GCIv5: إن وجود بيئة اقتصادية وسياسية واجتماعية مؤاتية تدعم تطوير الأمن السيبراني من شأنه أن يحفز نمو قطاع خاص حول الأمن السيبراني. كما إن شنّ الحملات الرامية إلى توعية الجمهور العام وتنمية القوة العاملة وبناء القدرات وإيجاد حوافز حكومية تؤدي جميعها إلى ظهور سوق لمنتجات وخدمات الأمن السيبراني. ووجود صناعة داخلية للأمن السيبراني يعد شاهداً على هذه البيئة المؤاتية وسيدفع بنمو المشاريع المبتدئة في مجال الأمن السيبراني وأسواق التأمين السيبراني المرتبطة بها.

2.5 هل هناك أي منظمات أو رابطات قُطرية تشجع على تطوير صناعة الأمن السيبراني في بلدكم؟

الرمز-GCIv5: CapDev5.4

الأساس المنطقي-GCIv5: يمكن للمنظمات والجمعيات، من خلال تشجيع تبادل المعرفة وتنمية المواهب والوصول إلى الاستثمار والتمويل، ضمن أمور أخرى، أن تتيح تعزيز الطابع النشط والمشارك لصناعة الأمن السيبراني. ويمكن أن تكون هذه المنظمات والجمعيات مدعومة من دوائر الصناعة أو يمكن أن تستمد الدعم من الحكومات الوطنية أو وكالات أخرى.

6 آليات تقديم الحوافز الحكومية

الرمز-GCIv5: CapDev6

الأساس المنطقي-GCIv5: يمكن أن يكون للاستثمار في مجال الأمن تأثيرات خارجية إيجابية لا يستفيد منها أولئك الذين يقومون بالاستثمار أو يبذلون الجهود. ولمعالجة النقص المحتمل في الاستثمارات أو الجهود في مجال الأمن السيبراني، يمكن أن تتدخّل الحكومات لتقديم حوافز لتحسين الأمن السيبراني، مثل التمويل أو التنظيم أو إيجاد آليات أخرى. ومن شأن ذلك أن يرفع مستوى الأمن السيبراني في بلد ما بما يتجاوز المستوى الذي يمكن أن يصل إليه دون دعم.

1.6 هل هناك أي آليات لتقديم حوافز حكومية من أجل تشجيع بناء القدرات في مجال الأمن السيبراني؟

الرمز-GCIv5: CapDev6.1

الأساس المنطقي-GCIv5: يمكن أن تؤدي آليات تقديم الحوافز الحكومية إلى تحفيز تنمية القدرات في مجال الأمن السيبراني، مثل إجراء الدراسات، أو المشاركة في التعليم المستمر، أو وضع برامج جديدة لتنمية القدرات أو آليات تحفيزية مثل المنح، أو المنح الدراسية، أو دعم دفع الرسوم، أو القروض، أو فرص العمل.

2.6 هل توجد أي آليات لتقديم حوافز حكومية تتيح تطوير صناعة الأمن السيبراني أو زيادة تطويرها؟

الرمز-GCIv5: CapDev6.2

الأساس المنطقي-GCIv5: يمكن أن تَحدث احتكارات نظراً لطبيعة السلع الإعلامية مثل الأمن السيبراني.[24] ومن أجل تعزيز ظهور أفكار وممارسات جديدة في المنظمات الجديدة والقائمة، وتشجيع شتى الجهات الفاعلة وأصحاب المصلحة على المشاركة في مجال الأمن السيبراني، يمكن للحكومات أن تقدم حوافز في شكل منح نقدية، أو إعفاءات من الضرائب أو الرسوم، أو مزايا من حيث السمعة، أو شروط تعاقدية جيدة، أو حوافز تدفع الشركات والمنظمات والأفراد إلى المشاركة في النظام الإيكولوجي للأمن السيبراني.

3.6 هل توجد في بلدكم آليات لتقديم حوافز حكومية تشجّع أنشطة البحث والتطوير المتصلة بالأمن السيبراني؟

الرمز-GCIv5: CapDev6.3

الأساس المنطقي-GCIv5: تُعتبر آليات تقديم الحوافز الحكومية مفيدة عندما لا تولّد قوى السوق الحالية النتائج المرجوة. وبما أن فوائد أنشطة البحث والتطوير المتصلة بالأمن السيبراني يمكن أن تكون لها تأثيرات خارجية إيجابية على المجتمع ككل، فإن على الحكومات أن تشجع أنشطة البحث والتطوير المتصلة بالأمن السيبراني بطرق متنوعة، وذلك مثلاً من خلال المنح، وآليات إعطاء القروض، والبيئة المؤاتية للتجارة والأعمال، والعقود، ودعم أنشطة الجامعات، وغير ذلك.

تدابير التعاون

الأساس المنطقي-GCIv5: يحتاج الأمن السيبراني إلى مدخلات من جميع القطاعات والتخصصات، ولهذا السبب يجب معالجته من خلال نهج متعدد أصحاب المصلحة. ويعزز التعاون الحوار والتنسيق ويمكّن من إيجاد مجال أكثر شمولية لتطبيق الأمن السيبراني. ونظراً إلى أن الأمن السيبراني مرتبط بالقطاعات والجغرافيا وحجم الموارد، ينبغي التعاون على المستويات الخاصة والعامة والإقليمية والدولية. ويمكن أن تؤدي زيادة المبادرات التعاونية إلى تطوير قدرات أقوى بكثير في مجال الأمن السيبراني، مما يساعد في ردع التهديدات المتكررة والمستمرة على شبكة الإنترنت، ويمكن أن تتيح تحسين التحقيقات والقبض على العملاء الضّارّين وملاحقتهم قضائياً.

ويمكن قياس حجم التعاون الوطني والدولي استناداً إلى وجود الشراكات والأطر التعاونية وشبكات تبادل المعلومات وإلى عددها.

[24] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf

1 الاتفاقات الثنائية في مجال الأمن السيبراني

الرمز-GCIv5: Coop1

الأساس المنطقي-GCIv5: تشير الاتفاقات الثنائية (اتفاقات بين طرفين) إلى أي شراكات وطنية معترف بها رسمياً لتبادل أصول الأمن السيبراني عبر الحدود (أي تبادل المعلومات والخبرات والسياسات والتكنولوجيات والموارد الأخرى) بين الحكومة وحكومة أجنبية أخرى أو منظمة إقليمية حكومية من أجل مواجهة خطر اندلاع الأزمات السيبرانية عبر الحدود. ويقيس المؤشر أيضاً ما إذا كان الاتفاق ملزماً قانوناً أو ما إذا كان ينتظر التصديق عليه. ويمكن أن تعني الأصول تبادل المهنيين (الإعارات أو التعيينات أو الأنواع الأخرى من التشغيل المؤقت للموظفين) والمرافق والأجهزة وغيرها من الأدوات والخدمات.

1.1 اتفاق (اتفاقات) ثنائي (ثنائية) مع بلدان أخرى بشأن الأمن السيبراني

الرمز-GCIv5: Coop1.1

الأساس المنطقي-GCIv5: تشير الاتفاقات الثنائية (اتفاقات بين طرفين) إلى أي شراكات وطنية معترف بها رسمياً لتبادل أصول الأمن السيبراني عبر الحدود (أي تبادل المعلومات والخبرات والسياسات والتكنولوجيات والموارد الأخرى) بين الحكومة وحكومة أجنبية أخرى. ويمكن أن يساعد تبادل المعارف والخبرات بين البلدان في بناء قدرات قوية للتصدي للحوادث، فضلاً عن اتخاذ تدابير استباقية لمواجهة المخاطر المتعلقة بالأمن السيبراني.

1.1.1 هل يقوم بلدكم بتبادل المعلومات المتعلقة بالأمن السيبراني مع بلدان أخرى في إطار اتفاق (اتفاقات) ثنائي (ثنائية)؟

الرمز-GCIv5: Coop1.1.1

الأساس المنطقي-GCIv5: تثبت الاتفاقات المتعلقة بالأمن السيبراني التي تتناول تبادل المعلومات أن التزامات البلدان في مجال الأمن السيبراني قد ازدادت، لأن هذه الاتفاقات تسهل مواجهة المخاطر المحتملة، وإجراء تقييمات للتهديدات، والتعاون بشأن الإجراءات المتعلقة بالأمن السيبراني.

2.1.1 هل أبرم بلدكم اتفاقاً (اتفاقات) ثنائياً (ثنائية) مع بلدان أخرى فيها جزء متعلق بتنمية القدرات المتعلقة بالأمن السيبراني؟

الرمز-GCIv5: Coop1.1.2

الأساس المنطقي-GCIv5: تتيح الاتفاقات الرامية إلى تنمية القدرات المتعلقة بالأمن السيبراني على نحو ثنائي تعزيز قدرة البلدان على التصدي بشكل استباقي للمخاطر السيبرانية من خلال تبادل أفضل الممارسات وزيادة مهارات الموظفين وتعزيز التعاون وإذكاء الوعي ووضع إجراءات تشغيلية تتعلق بالأمن السيبراني وتنفيذها.

2.1 اتفاق (اتفاقات) الأمن السيبراني مع المنظمات الدولية والإقليمية

الرمز-GCIv5: Coop1.1.3

الأساس المنطقي-GCIv5: نظراً إلى أهمية المنظمات الحكومية الإقليمية، تعقد البلدان بشكل متزايد اتفاقات تعاونية بشأن الأمن السيبراني من أجل تبادل الأصول المتعلقة بالأمن السيبراني عبر الحدود، مثل تبادل المعلومات والخبرات والتكنولوجيات والموارد الأخرى، سواء كبلدان منفردة أو كأعضاء في منظمة حكومية إقليمية، مع منظمات حكومية إقليمية أخرى مثل الاتحاد الأوروبي ورابطة أمم جنوب شرق آسيا (ASEAN) والجماعة الاقتصادية لدول غرب إفريقيا (ECOWAS) ومنظمة الدول الأمريكية (OAS) والاتحاد الإفريقي (AU) وغيرها.

1.2.1 هل يقوم بلدكم أو المنظمة الحكومية الإقليمية التي يكون بلدكم عضواً فيها بتبادل المعلومات المتعلقة بالأمن السيبراني في إطار اتفاق (اتفاقات) ثنائي (ثنائية) مع منظمات إقليمية ودولية أخرى؟

الرمز-GCIv5: Coop1.2.1

الأساس المنطقي-GCIv5: تُبيّن اتفاقات الأمن السيبراني التي تتناول تبادل المعلومات زيادة التزامات البلدان في مجال الأمن السيبراني، لأنها تسهل مواجهة المخاطر المحتملة وتبادل البيانات المتعلقة بتقييم التهديدات، والتعاون بشأن الإجراءات المتعلقة بالأمن السيبراني.

2.2.1 هل أبرم بلدكم أو المنظمة الحكومية الإقليمية التي يكون بلدكم عضواً فيها اتفاقاً (اتفاقات) ثنائياً (ثنائية) مع منظمات إقليمية ودولية أخرى فيها جزء متعلق بتنمية القدرات المتعلقة بالأمن السيبراني ؟

الرمز-GCIv5: Coop1.2.2

الأساس المنطقي-GCIv5: يمكن للاتفاقات الثنائية المتعلقة بالأمن السيبراني التي تتناول تنمية القدرات في مجال الأمن السيبراني، والمعقودة بين البلدان والمنظمات الحكومية الإقليمية، أن تعزز القدرات المتعلقة بالأمن السيبراني بفضل تبادل أفضل الممارسات، وزيادة مهارات الموظفين، وتعزيز التعاون، وإذكاء الوعي، ووضع إجراءات تشغيلية متعلقة بالأمن السيبراني وتنفيذها.

2 اتفاقات الأمن السيبراني المتعددة الأطراف المعقودة مع بلدان أخرى

الرمز-GCIv5: Coop2

الأساس المنطقي-GCIv5: يقتضي عقدُ اتفاقات خطية متعددة الأطراف الاتفاق على التعاريف والمعلمات الرئيسية المتعلقة بالأمن السيبراني، ويتيح وضع برنامج مشترك للمضي قدماً بشأن الأمن السيبراني. كما يمكن أن تعزز هذه الاتفاقات اتخاذ تدابير لبناء الثقة كجزء من عملية استحداث آليات تلقي التعليقات الإيجابية لبناء علاقات سلمية.

1.2 هل أبرم بلدكم اتفاقاً متعدد الأطراف في مجال الأمن السيبراني يشمل تبادل معلومات بشأن الأمن السيبراني؟

الرمز-GCIv5: Coop2.1.1

الأساس المنطقي-GCIv5: تُبيّن اتفاقات الأمن السيبراني التي تتناول تبادل المعلومات زيادة التزامات البلدان بشأن الأمن السيبراني، لأنها تسهل مواجهة المخاطر المحتملة، وتبادل البيانات المتعلقة بإجراء تقييمات للتهديدات، والتعاون بشأن الإجراءات المتعلقة بالأمن السيبراني.

2.2 هل أبرم بلدكم اتفاقاً متعدد الأطراف بشأن الأمن السيبراني يشمل تبادل أنشطة تنمية القدرات؟

الرمز-GCIv5: Coop2.1.2

الأساس المنطقي-GCIv5: يمكن أن يؤدي عقد الاتفاقات الخطية المتعددة الأطراف التي تشمل تنمية القدرات إلى دعم تنمية القدرات في البلدان التي تعاني من ضعف وضعها فيما يخص الأمن السيبراني، وإلى دعم تدابير بناء الثقة.

3 معاهدات المساعدة القانونية المتبادلة (MLAT)[25] المتعلقة بالأمن السيبراني

الرمز-GCIv5: Coop3

الأساس المنطقي-GCIv5: نظراً إلى الطبيعة العابرة للحدود للأمن السيبراني، يتطلب اتخاذُ الإجراءات بشأن التهديدات التي تؤثر على سيادة دولة أخرى آليات تعاون واضحة، خاصة فيما يتعلق بالمسائل القضائية. ويمكن أن تعطى المساعدة القانونية المتبادلة، التي تكون مثلاً في شكل معاهدات لتبادل المساعدة القانونية، بطرائق متعددة، من خدمة الوثائق وإحالة الأدلة إلى المساعدة في مجال التحقيقات، من بين أشكال أخرى من المساعدة.[26]

1.3 هل يشارك بلدكم في معاهدات تبادل المساعدة القانونية بشأن الأمن السيبراني، سواء من خلال عقد اتفاق (اتفاقات) ثنائي (ثنائية) أو اتفاق (اتفاقات) متعدد (متعددة) الأطراف مع بلدان أخرى أو منظمات إقليمية أو حكومية دولية؟

الرمز-GCIv5: Coop3.1

الأساس المنطقي-GCIv5: نظراً إلى الطبيعة العابرة للحدود للأمن السيبراني، يتطلب اتخاذُ الإجراءات بشأن التهديدات التي تؤثر على سيادة دولة أخرى آليات تعاون واضحة، خاصة فيما يتعلق بالمسائل القضائية. ويمكن أن تعطى المساعدة القانونية

25 https://www.unodc.org/e4j/en/organized-crime/module-11/key-issues/mutual-legal-assistance.html

26 https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL

المتبادلة، التي تكون مثلاً في شكل معاهدات لتبادل المساعدة القانونية، بطرائق متعددة، من خدمة الوثائق وإحالة الأدلة إلى المساعدة في مجال التحقيقات، من بين أشكال أخرى من المساعدة.[27]

4 الشراكات بين القطاعين العام والخاص (PPP)

الرمز-GCIv5: Coop4

الأساس المنطقي-GCIv5: تُعتبر الشراكات المعقودة بين القطاعين العام والخاص جزءاً من اتجاه ولّدته أسباب أيديولوجية ومساع رامية إلى الحصول على قيمة مالية.[28] ويمكن أن تساعد الشراكات المعقودة بين القطاعين العام والخاص، لا سيما في مجال الأمن السيبراني حيث تنشأ الابتكارات الجديدة في كثير من الأحيان في القطاع الخاص، الحكومات على الاستفادة بشكل أسرع من هذه الابتكارات الجديدة ومن التحسّن المحتمل للأمن السيبراني. بيد أن الشراكات المعقودة بين القطاعين العام والخاص تنطوي أيضاً على عدد من التحديات، مثل المشاكل المتعلقة بالوكيل الرئيسي، وإدارة التأثيرات الخارجية، والطابع المعقّد للتفاوض على العقود، ومرونة العقود، والتقييم الفعلي.[29]

1.4 هل تشارك حكومتكم مع شركات محلية في شراكات بين القطاعين العام والخاص في مجال الأمن السيبراني؟

الرمز-GCIv5: Coop4.1

الأساس المنطقي-GCIv5: نظراً إلى الآثار المتأصلة المتعلقة بالشبكات، يمكن أن تؤدي الشراكات المبرمة مع الشركات المحلية في إطار شراكات بين القطاعين العام والخاص بتعزيز النظام الإيكولوجي المحلي للأمن السيبراني، بما يمكّن الجهات الفاعلة المحلية في القطاع الخاص من تطوير وتوسيع مهاراتها وأنظمتها وخدماتها.

2.4 هل تشارك حكومتكم مع شركات أجنبية في بلدكم في شراكات بين القطاعين العام والخاص في مجال الأمن السيبراني؟

الرمز-GCIv5: Coop4.2

الأساس المنطقي-GCIv5: إن الأمن السيبراني، كسلعة إعلامية، يخضع لآثار الشبكات والخبرة المكتسبة على نطاق واسع.[30] ويمكن للجهات الفاعلة الدولية التي اكتسبته خبرتها في مجال الأمن السيبراني من سياقات أو خلفيات وطنية متنوعة، أن توفر فوائد إضافية للحكومات التي تسعى إلى تعزيز الأمن السيبراني الوطني. ويمكن للحكومات التي تبرم شراكات مع جهات فاعلة أجنبية، في إطار شراكات بين القطاعين العام والخاص، أن تستفيد من هذه الخبرة لتحقيق نموها وضمان أمنها.

5 الشراكات بين الوكالات

الرمز-GCIv5: Coop5

الأساس المنطقي-GCIv5: إن الشراكات المحلية الرسمية المعقودة فيما بين الوكالات الحكومية المختلفة في بلد ما من شأنها أن تيسّر استجابة الحكومة للمخاطر المتعلقة بالأمن السيبراني. ويمكن أن تشمل الشراكات تلك الرامية إلى تبادل المعلومات أو الأصول بين الوزارات والإدارات والبرامج وسائر مؤسسات القطاع العام. ولأغراض هذا القسم، لا يُنظر في الشراكات بين وكالات في بلدان مختلفة أو بين منظمات حكومية دولية.

1.5 هل تُجرى في مختلف الهيئات الحكومية الوطنية في بلدكم عمليات تنسيق محددة بين الوكالات بشأن الأمن السيبراني؟

الرمز-GCIv5: Coop5.1

---

27 https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL

28 https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page5

29 https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page66

30 https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf

الأساس المنطقي-GCIv5: إن الشراكات المحلية الرسمية المعقودة فيما بين الوكالات الحكومية المختلفة في بلد ما من شأنها أن تيسّر تصدّي الحكومة للمخاطر المتعلقة بالأمن السيبراني. ويمكن أن تشمل الشراكات تلك الرامية إلى تبادل المعلومات أو الأصول بين الوزارات والإدارات والبرامج وسائر مؤسسات القطاع العام. ولأغراض هذا الفرع، لا يُنظر في الشراكات بين وكالات في بلدان مختلفة أو بين منظمات حكومية دولية.

التعاريف

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
الهيئات الأكاديمية		عالم الدراسات الجامعية	قاموس أكسفورد باللغة الإنكليزية		Tech2؛ وCapDev4.1.3؛ وCapDev6.2
المؤسسات الأكاديمية		المؤسسات المنتمية إلى عالم الدراسات الجامعية	قاموس أكسفورد باللغة الإنكليزية		CapDev4.1.3
الاتفاق		التزامات متبادلة بشكل مكتوب بين دول أو أطراف أخرى وخاضعة للقانون الدولي، سواء وردت هذه الالتزامات في صك واحد أو في اثنين أو أكثر من الصكوك ذات الصلة	مقتبس بتصرّف من اتفاقية فيينا لقانون المعاهدات		
الاتفاق الثنائي		اتفاق مكتوب بين طرفين بما في ذلك الدول أو الهيئات الإقليمية أو المنظمات، يوقّعه صانعو القرارات المختصون	GCIv2		Coop1؛ وCoop1.1؛ وCoop1.1.1؛ وCoop1.1.2؛ وCoop1.1.3
تنمية القدرات		تنمية القدرات هي عملية تغيير. وغالباً ما تُعتبر صنواً لزيادة الموظفين وعقد دورات التدريب وورش العمل. وقد تكون الدورات التدريبية الفردية وورش العمل جزءاً من خطة شاملة لتنمية القدرات، إلا أنها ليست كافية في حدّ ذاتها. وعلى سبيل المثال، فإن تدريب فرد ما لا يضمن بعد ذلك تطبيقه فحوى التدريب في مكان العمل. ويجب أن تكون تنمية القدرات أوسع نطاقاً كي تتناول التحسينات الممكن إدخالها في النظم الصحية لتحسين الأداء وضمان الاستدامة. وينبغي أن تقيّم كيف يعمل النظام حالياً وما هي المجالات التي تحتاج إلى الدعم؛ وعلى سبيل المثال: وضع وتنفيذ أنظمة لتوفير المعلومات الصحية، أو تدريب الموظفين على تحليل البيانات، أو وضع سياسات وإجراءات لإدارة مالية مُحكمة، أو تحسين توفير وتوزيع المنتجات الصحية الرئيسية.	برنامج الأمم المتحدة الإنمائي https://www.undp-capacitydevelopment-health.org/en/capacities/		Org2.3؛ وCapDev1؛ وCapDev6.1؛ وCoop1.1.2
حماية الأطفال على الإنترنت	COP	تهدف حماية الأطفال على الإنترنت إلى حماية الأطفال والشباب من التهديدات والمخاطر التي قد يواجهونها على الإنترنت. ويتضمن مفهوم حماية الأطفال على الإنترنت اتّباع نهج شامل لبناء مساحات رقمية آمنة ومناسبة للعمر وشاملة وتشاركية للأطفال والشباب تتميز بما يلي: ● الاستجابة والدعم والمساعدة الذاتية في مواجهة التهديدات؛ ● ومنع الضرر؛ ● وتحقيق توازن دينامي بين ضمان الحماية وتوفير الفرص للأطفال ليكونوا مواطنين رقميين؛ ● والتمسك بحقوق ومسؤوليات الأطفال والمجتمع على السواء.	https://www.itu-cop-guidelines.com/		Legal1.3.3؛ وTech1.2.4؛ وTech4؛ وOrg1.3؛ وOrg2.4؛ وCapDev6.1

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
البنية التحتية الحيوية (انظر أيضاً: البنية التحتية الحيوية الوطنية)		الأنظمة والخدمات والوظائف الرئيسية التي يؤدي تعطيلها أو تدميرها إلى آثار موهنة على الصحة العامة والسلامة والتجارة والأمن الوطني أو على أي مجموعة من هذه الأمور.	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf	قد تشمل هذه الأنظمة، على سبيل المثال لا الحصر: أنظمة الدفاع والأنظمة المصرفية والمالية وأنظمة الاتصالات والنقل والصحة والطاقة وما إلى ذلك.	Tech1.2
البنية التحتية الحيوية للمعلومات	CII	المعدات والأصول الرقمية والشبكات والخدمات والمنشآت التي يؤدي تعطيلها أو تدميرها إلى آثار جسيمة على الصحة والأمن والرفاه الاقتصادي للمواطنين والعمل السليم لحكومة البلد.	الكتيب الدولي لحماية البنية التحتية الحيوية للمعلومات 2009/2008	قد تشمل هذه الأنظمة، على سبيل المثال لا الحصر: المكالمات الهاتفية والمبادلات عبر الإنترنت والشبكات اللاسلكية والسواتل وما إلى ذلك.	
قانون الجريمة السيبرانية		يحدّد قانون الجريمة السيبرانية قواعد التصرّف ومعايير السلوك لاستعمال الإنترنت والحواسيب والتكنولوجيات الرقمية ذات الصلة، وإجراءات المنظمات العامة والحكومية والخاصة؛ وقواعد الأدلة والإجراءات الجنائية وغيرها من المسائل المتعلقة بالعدالة الجنائية في الفضاء السيبراني؛ والقواعد التنظيمية ...	https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html		Legal1
متطلبات التدقيق الأمني السيبراني		يعني التدقيق الأمني التقييم النظامي والدوري لأمن نظام المعلومات. وقد يشمل التدقيق النمطي تقييم أمن التشكيلة المادية للنظام والبيئة والبرمجيات وعمليات تداول المعلومات وممارسات المستعملين	GCIv4		Legal2.3n
النظام الإيكولوجي للأمن السيبراني		مجتمع من الجهات الفاعلة حول الأمن السيبراني وفيه، ويكون لها أدوار ومسؤوليات تتطوّر معاً	مقتبس بتصرف من *Moore, James. The Death of Competition. 1996*	مثل المهنيين العاملين في المجال القانوني والتقني ومجالي الأعمال والسياسات، الذين يعملون معاً على القضايا المتصلة بالأمن السيبراني	CapDev5.1، وCapDev6.2
القدرة على الصمود في مجال الأمن السيبراني		القدرة على التعافي من الاختراقات أو الهجمات الأمنية. وتضمن الخطة الوطنية للقدرة على الصمود في مجال الأمن السيبراني قدرة البلد على مقاومة واستيعاب التأثيرات الناجمة عن أي أخطار والتكيّف معها والتعافي منها (بما في ذلك الأخطار الطبيعية أو تلك الناجمة عن الأنشطة البشرية) في الوقت المناسب وبكفاءة، بما في ذلك من خلال حفظ واستعادة خدماتها ووظائفها الأساسية بالاعتماد على خدمات خارجية.	https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/website/web-fg-ssc-0090-r7-technical_report_on_ICT_infrastructure_for_resilience_security.doc		Tech1.3

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
المعاهدات والاتفاقات المتعلقة بالأمن السيبراني		معاهدة أو اتفاق بين بلدين أو منظمتين أو مجموعات أخرى تتعلق تحديداً بالأمن السيبراني.	https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478		
الإبلاغ بانتهاك البيانات		قوانين أو لوائح التبليغ عن الانتهاكات هي تلك التي تلزم أي كيان يتعرض لخرق ما بإبلاغ السلطات وعملائها والأطراف الأخرى عن الانتهاك واتخاذ خطوات أخرى لعلاج الأضرار الناجمة عن الانتهاك. وتسنّ هذه القوانين عادة استجابةً للعدد المتصاعد من الانتهاكات لقواعد بيانات المستهلكين التي تتضمن معلومات شخصية تتيح التعرف على هوية أصحابها .	GCIv2		Legal2.2
النفاذ غير القانوني		إذا ما ارتُكب عمداً، هو النفاذ بغير حق إلى كامل النظام الحاسوبي أو إلى جزء منه. ويجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بقصد الحصول على بيانات حاسوب أو بقصد آخر غير شريف، أو فيما يتعلق بنظام حاسوبي متصل بنظام حاسوبي آخر.	GCIv2		Legal1.1.1
الاعتراض غير القانوني		إذا ما ارتُكب عمداً، هو الاعتراض بغير حق، باستخدام وسائل تقنية، لعمليات إرسال غير عمومية لبيانات حاسوبية إلى أو من أو داخل نظام حاسوبي، بما في ذلك ما ينبعث من نظام حاسوبي من موجات كهرمغنطيسية تحمل هذه البيانات.	GCIv2		Legal1.1.3
التدخل غير القانوني		"إذا ما أُرتكب عمداً، هو إتلاف، أو محو، أو إفساد، أو تعديل، أو تدمير بيانات حاسوبية بغير حق." و"إذا ما ارتُكِب عمداً، هو الإعاقة الخطيرة بغير حق لعمل نظام حاسوبي عن طريق إدخال أو إرسال أو إتلاف أو محو أو تغيير أو تبديل أو تدمير بيانات حاسوبية."	GCIv2		Legal1.1.2
الإبلاغ بحادث		إقدام فريق الاستجابة للحوادث الحاسوبية أو غيره على إبلاغ أصحاب المصلحة المعنيين بوقوع حادث متعلق بالأمن السيبراني.			Legal2.2
الشراكات/الاتفاقات المشتركة بين الوكالات		أي شراكات محلية رسمية بين مختلف الوكالات الحكومية داخل بلد ما من شأنها أن تسهّل استجابة الحكومة لمخاطر الأمن السيبراني. ويمكن أن تشمل الشراكات تبادل المعلومات أو الأصول بين الوزارات والإدارات والبرامج ومؤسسات القطاع العام الأخرى. ولأغراض هذا القسم، لا يُنظر في الشراكات بين وكالات في بلدان مختلفة أو بين منظمات حكومية دولية.	GCIv2		Coop5

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
عمليات التنسيق بين الوكالات		التنسيق بين وكالتين حكوميتين أو أكثر بشأن قضايا معيَّنة بغية العمل على تواؤم الأهداف والأنشطة			Coop5.1
الشركات بالغة الصغر والصغيرة والمتوسطة	MSME	قد تختلف تعاريف الشركات بالغة الصغر والصغيرة والمتوسطة باختلاف البلد. وينبغي، حيثما أمكن، استخدام التعاريف التي يعتمدها المنتدى المالي للشركات الصغيرة والمتوسطة.		https://www.smefinanceforum.org/data-sites/msme-country-indicators	CapDev1.1؛ وCapDev2.3.3
الاتفاقات متعددة الأطراف		تشير الاتفاقات متعددة الأطراف (اتفاقات بين طرف وأطراف متعددة) إلى أي برامج وطنية أو قطاعية معترف بها رسمياً من أجل تبادل معلومات أو أصول الأمن السيبراني عبر الحدود بين الحكومة وحكومات أجنبية أو منظمات دولية متعددة (أي التعاون أو تبادل المعلومات والخبرات والتكنولوجيا والموارد الأخرى). وقد تشمل أيضاً التصديق على اتفاقات دولية بخصوص الأمن السيبراني، مثل اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية واتفاقية بودابست بشأن الجريمة السيبرانية وغيرها.	GCIV2		Coop3؛ وCoop3.1.1؛ وCoop3.1.2
البنية التحتية الحيوية الوطنية (انظر أيضاً البنية التحتية الحيوية)		الأنظمة والخدمات والوظائف الرئيسية التي يؤدي تعطيلها أو تدميرها إلى آثار موهنة على الصحة العامة والسلامة والتجارة والأمن القومي أو على أي مجموعة من هذه الأمور.	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf		Legal2.7؛ وOrg1.1.1
الفريق الوطني المعني بالتصدي للحوادث الحاسوبية		فريق التصدي للحوادث الحاسوبية (CIRT) أو فريق التصدي للطوارئ الحاسوبية (CERT) أو فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) كيانات تنظيمية ملموسة مكلّفة بمسؤولية تنسيق ودعم التصدي للأحداث أو الحوادث الأمنية الحاسوبية على الصعيد الوطني. وتتحمّل الأفرقة المسؤولية الوطنية عن توفير القدرات اللازمة لتحديد التهديدات السيبرانية والدفاع عما تُعَرّضه للخطر والتصدي لها وإدارتها وتعزيز أمن الفضاء السيبراني في البلد. ويلزم أن تقترن هذه القدرة بجمع المعلومات الاستخبارية الخاصة بها بدلاً من الاعتماد على التقارير الثانوية عن الحوادث الأمنية سواء من أعضاء الفريق CIRT أو من مصادر أخرى. وقد تكون عسكرية أو مدنية.	من GCI2		
الاعتداء عبر الإنترنت					Legal1.3.2

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
المضايقة عبر الإنترنت		الرسائل المرسلة عبر البريد الإلكتروني أو المراسلة المباشرة أو المواقع الإلكترونية المسيئة التي تهدف إلى ترهيب أو مضايقة فرد أو مجموعة من الأفراد من خلال هجمات ذات طابع شخصي.	GCIv4		Legal1.3.2
السلامة على الإنترنت		تشير إلى تعظيم السلامة على الإنترنت من المخاطر الأمنية المختلفة التي تحيق بالمعلومات الخاصة والشخصية أو المعلومات المرتبطة بالملكية، فضلاً عن تعزيز الحماية الذاتية للمستعملين من الجرائم السيبرانية.	GCIv4		Legal1.3
الأشخاص ذوو الاحتياجات الخاصة		متطلبات خاصة ناتجة عن إعاقة بدنية أو صعوبات في التعلم أو صعوبات سلوكية وما إلى ذلك (لا سيما في السياقات التعليمية).	قاموس أكسفورد باللغة الإنكليزية	"special needs, n. and adj.". OED Online. June 2021. Oxford University Press. https://www.oed.com/view/Entry/253889?redirectedFrom=special+needs (تم تصفح الموقع في 30 أغسطس 2021)	
حماية البيانات الشخصية		البيانات الشخصية هي أي معلومات خاصة بشخص طبيعي محدد أو يمكن تحديده. وحماية البيانات الشخصية هي عملية صون البيانات الشخصية.	https://gdpr-info.eu/issues/personal-data/ تعريف مأخوذ من اللائحة العامة لحماية البيانات (GDPR)	يقدم المعيار الطوعي ITU-T X.1058 | ISO/IEC 29151 نقطة مرجعية قيّمة للحكومات ودوائر الصناعة في تعزيز سعيها إلى ضمان حماية البيانات الشخصية. وتحدد التوصية X.1058 أهداف الضوابط الرامية إلى حماية البيانات، وتوضّح الضوابط اللازمة، وتضع مبادئ توجيهية لتنفيذها. وتُبيّن كيف يمكّن تنظيم هذه الضوابط من تلبية المتطلبات التي حددتها تقييمات المخاطر والآثار التي أجرتها المنظمات فيما يخص حماية البيانات الشخصية.	Legal2.1a
السياسات		السياسات هي القواعد أو المبادئ أو المبادئ التوجيهية أو الهياكل التي اعتمدتها أو صمّمتها منظمة أو بلد ما لتحقيق أهداف طويلة الأجل. وتحدَّد عادة في نسق مكتوب يسهل فهمه. وتصاغ السياسات لتوجيه جميع القرارات الرئيسية التي يتعين اتخاذها	مصطلح جديد		Org1.1

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
		داخل المنظمة والتأثير عليها، ولإبقاء جميع الأنشطة ضمن مجموعة من الحدود المقررة.			
التعليم ما بعد الثانوي غير العالي (المستوى 4 من التصنيف الدولي الموحد للتعليم)	المستوى 4 من التصنيف الدولي الموحد للتعليم	يوفر التعليم ما بعد الثانوي غير العالي تجارب تعلم تستند إلى التعليم الثانوي من أجل الإعداد لدخول سوق العمل والتعليم العالي. وهي تهدف إلى اكتساب الأفراد للمعارف والمهارات والكفاءات دون مستوى التعقيد الذي يتسم به التعليم العالي. وتصمَّم عادة البرامج المتعلقة بالمستوى 4 من التصنيف الدولي الموحد للتعليم أو بمرحلة التعليم ما بعد الثانوي غير العالي من أجل تزويد الأفراد الذين أكملوا المستوى 3 من التصنيف الدولي الموحد للتعليم بالمؤهلات غير العليا اللازمة للوصول إلى التعليم العالي أو لنيل وظيفة عندما لا تتيح مؤهلاتهم المكتسبة في المستوى 3 من التصنيف الدولي الموحد للتعليم مثل هذا النفاذ...	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.4n
التعليم الابتدائي (المستوى 1 من التصنيف الدولي الموحد للتعليم)		البرامج المتعلقة بالمستوى 1 من التصنيف الدولي الموحد للتعليم، أي التعليم الابتدائي، مصمَّمة عادةً لتزويد التلاميذ بالمهارات الأساسية في مجالات القراءة والكتابة والرياضيات (أي أسس القراءة والكتابة والحساب) وإرساء أساس متين للتعلم ولفهم المجالات الرئيسية للمعرفة، وللتنمية الشخصية والاجتماعية، في إطار التحضير للتعليم الثانوي الأدنى. وهي تركّز على التعلم بمستوى أساسي من التعقيد مع قدر قليل من التخصص إن وجد... والعمر هو عادة المتطلب الوحيد للالتحاق بهذا المستوى. ولا يقلّ عموماً العمر المعتاد أو القانوني للالتحاق عن خمس سنوات ولا يتجاوز سبع سنوات.	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.1
حماية الخصوصية		الخصوصية في الإنترنت هي مستوى الخصوصية والأمن للبيانات الشخصية التي تنشر عبر الإنترنت. وهو مصطلح واسع يشير إلى مجموعة متنوعة من العوامل والتقنيات والتكنولوجيات التي تستخدم لحماية البيانات والاتصالات والأفضليات الحساسة والخاصة. ومن أمثلة هذه التشريعات قانون حماية البيانات.	GCIv2		Legal2.1b
الشراكة بين القطاعين العام والخاص	PPP	عقد طويل الأجل بين طرف خاص وكيان حكومي لتوفير أصل عام أو خدمة عامة يتحمّل فيه الطرف الخاص قدراً كبيراً من المسؤولية فيما يخص المخاطر والإدارة، وترتبط الأجور بالأداء. **ملاحظة:** في غياب أي تعريف قانوني رسمي، تحدَّد الشراكات بين القطاعين العام والخاص في كثير من الأحيان بناء على	https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships		

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
		وظيفتها. واقترح الأمين العام للأمم المتحدة شكلين من الشراكات. ويحدد الشكل الأول الوظائف الخمس الرئيسية التالية: أ) التحاور بشأن السياسات، مثل فريق المهام المعني بتكنولوجيا المعلومات والاتصالات، واللجنة العالمية المعنية بالسدود، والتحالف العالمي للقاحات والتحصين؛ وب) التوعية، مثل الشراكة القائمة بين برنامج الأمم المتحدة المشترك المعني بفيروس نقص المناعة البشرية/الإيدز ووسائل الإعلام، من أجل التوعية بفيروس نقص المناعة البشرية/الإيدز؛ وج) تعبئة الأموال الخاصة، مثل مؤسسة الأمم المتحدة وصندوق الشراكات الدولية، ومؤتمر الأمم المتحدة للتجارة والتنمية - مشروع الاستثمار الأجنبي التابع لغرفة التجارة الدولية؛ ود) توفير المعلومات والتعلم، مثل مشاريع البحث والتدريب المشتركة؛ وه) الإنجاز التشغيلي، مثلاً مبادرة الميدان الأولى المشتركة بين الأمم المتحدة وشركة LM Ericsson، ومشروع تسجيل اللاجئين، المشترك بين الأمم المتحدة وميكروسوفت (المبادئ التوجيهية للأمم المتحدة 18-32). ويحدد الشكل الثاني أربع وظائف هي: أ) التوعية، مثل التحالف العالمي لتحسين التغذية، والشراكة العالمية بين القطاع العام والخاص للتشجيع على غسل اليدين بالصابون؛ وب) وضع القواعد والمعايير، مثل مبادرة الإبلاغ العالمية، ومشروع "الفائز من اهتمّ" بشأن المسؤولية المؤسسية في دوائر الصناعة المالية؛ وج) تبادل الموارد والخبرات، مثل الشراكة بين برنامج الأغذية العالمي وTNT بشأن برنامج "الخدمات اللوجستية تحرك العالم"؛ ود) الاستفادة من الأسواق لتحقيق التنمية، مثل مبادرة إنتاج زبدة "الشيا" المشتركة بين صندوق الأمم المتحدة الإنمائي للمرأة وشركة L'Occitane، والمشروع الهندي لقطع غيار السيارات المشترك بين اليونيدو وشركة FIAT (الجمعية العامة للأمم المتحدة، "تقرير الأمين العام عن تعزيز التعاون بين الأمم المتحدة وجميع الشركاء المعنيين، وخاصة القطاع الخاص") *[10 أغسطس 2005]*. وتُحدّد المبادئ التوجيهية للأمم المتحدة عدة طرائق تعاون والترتيبات القانونية الموحّدة المستخدمة في كل منها أو التي تعرَّف ببساطة على أنها مشاريع بين القطاعين العام والخاص. ويمكن قياس مؤشر الأداء هذا بناء على عدد الشراكات الوطنية أو القطاعية المعترف بها رسمياً بين القطاعين العام والخاص لتبادل المعلومات المتعلقة بالأمن السيبراني (المعلومات الاستخباراتية المتعلقة بالتهديدات والأصول (الأشخاص والعمليات والأدوات)	https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1084?rskey=CTIBOr&result=1&prd=MPIL		

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
		بين القطاعين العام والخاص (أي الشراكات الرسمية الرامية إلى التعاون أو تبادل المعلومات و/أو الخبرات و/أو التكنولوجيا و/أو الموارد)، سواء على الصعيد الوطني أو الدولي.			
لائحة تنظيمية		قاعدة أو مبدأ ينظم السلوك أو الممارسة؛ مثل أمر توجيهي تضعه سلطة ما وتحرص على تنفيذه.	قاموس أكسفورد باللغة الإنكليزية	"regulation, n. and adj.". OED Online. June 2021. Oxford University Press. https://www.oed.com/view/Entry/161427?redirectedFrom=regulation (تم تصفح الموقع في 30 أغسطس 2021)	Legal2، وLegal 2.1، وLegal2.2
البحث والتطوير	R&D	تشمل أنشطة البحث والتطوير التجريبي الاضطلاع بأعمال خلاقة منتظمة من أجل زيادة حجم المعارف - بما فيها المعارف المتعلقة بالبشرية والثقافة والمجتمع - واستنباط تطبيقات جديدة للمعارف المتاحة. ويغطي مصطلح البحث والتطوير ثلاثة أنواع من الأنشطة هي: البحوث الأساسية والبحوث التطبيقية والتطوير التجريبي. ولكي يندرج نشاط ما في إطار أنشطة البحث والتطوير، يجب أن يفي بخمسة معايير أساسية. فعلى النشاط أن يكون: ● جديداً (يرمي إلى التوصل إلى نتائج جديدة) ● ابتكارياً (يستند إلى مفاهيم وفرضيات إبداعية لا بديهية) ● غير أكيد (ألا تكون النتيجة النهائية أكيدة) ● نظامياً (أن يتم التخطيط له وتحديد ميزانيته) ● قابلاً للنقل و/أو التكرار (أن يؤدي إلى نتائج يمكن استنساخها).	OECD (2015), Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development http://uis.unesco.org/en/glossary-term/research-and-experimentaldevelopment-rd		CapDev4.1؛ وCapDev4.1.1؛ وCapDev4.1.2؛ وCapDev4.1.3
التعليم الثانوي (المستويان 2 و3 من التصنيف الدولي الموحد للتعليم)	ISCED 2 and 3	تُصمَّم عادة البرامج المتعلقة بالمستوى 2 من التصنيف الدولي الموحد للتعليم، أو التعليم الثانوي الأدنى، بالاستناد إلى نتائج التعلم في المستوى 1 من التصنيف. والهدف في العادة هو إرساء الأساس اللازم للتعلم مدى الحياة وللتنمية البشرية والذي يمكن لأنظمة التعليم أن تستند إليه لزيادة الفرص التعليمية. وقد تقدّم بالفعل بعض أنظمة التعليم برامج تعليمية مهنية على المستوى 2 من التصنيف الدولي الموحد للتعليم من أجل تزويد الأفراد بالمهارات اللازمة للحصول على وظيفة.	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.2

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
		والبرامج المتعلقة بالمستوى 3 من التصنيف الدولي الموحد للتعليم، أو التعليم الثانوي الأعلى، مصمَّمة عادة لإتمام التعليم الثانوي تمهيداً للتعليم العالي أو لتوفير المهارات اللازمة للعمل، أو لتحقيق الغرضين. ويبدأ المستوى 3 من التصنيف الدولي الموحد للتعليم بعد مرور 8 إلى 11 عاماً من التعليم منذ بداية المستوى 1 من التصنيف.			
التعليم العالي (المستويات من 5 إلى 8 من التصنيف الدولي الموحد للتعليم)	ISCED levels 5 to 8	غالباً ما تُصمَّم البرامج المتعلقة بالمستوى 5 من التصنيف الدولي الموحد للتعليم، أي التعليم العالي ذو الدورة القصيرة، لتزويد المشاركين بالمعارف والمهارات والكفاءات المهنية. وتكون عادة مستندة إلى أسس عملية وموجَّهة نحو مهن معيّنة، وتعدّ الطلاب لدخول سوق العمل. بيد أن هذه البرامج قد توفّر أيضاً سبيلاً يفضي إلى برامج أخرى من التعليم العالي. وغالباً ما تصمَّم البرامج المتعلقة بالمستوى 6 من التصنيف الدولي الموحد للتعليم، وهو مستوى البكالوريوس أو مستوى مكافئ، لتزويد المشاركين بالمعارف والمهارات والكفاءات الأكاديمية و/أو المهنية المتوسطة، التي تتيح الحصول على شهادة من الدرجة الأولى أو على ما يعادلها من مؤهلات. وغالباً ما تُصمَّم البرامج المتعلقة بالمستوى 7 من التصنيف الدولي الموحد للتعليم، أي مستوى الماجستير أو مستوى مكافئ، لتزويد المشاركين بالمعارف والمهارات والكفاءات الأكاديمية و/أو المهنية المتقدمة، التي تتيح الحصول على شهادة من الدرجة الثانية أو ما يعادلها من مؤهلات ... والبرامج المتعلقة بالمستوى 8 من التصنيف الدولي الموحد للتعليم، وهو مستوى الدكتوراه أو مستوى مكافئ، مصمَّمة بشكل رئيسي لتتيح الحصول على مؤهل بحثي متقدم. والبرامج المتعلقة بهذا المستوى من التصنيف الدولي الموحد للتعليم مخصَّصة للدراسات المتقدمة والبحوث الأصلية ولا توفرها في العادة إلا مؤسسات التعليم العالي الموجهة نحو البحث مثل الجامعات. وتوجد برامج دكتوراه في المجالين الأكاديمي والمهني على حد سواء.	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.3
كره الأجانب		النفور من الأجانب ومن الثقافات والعادات الأجنبية أو التي يُعتقد أنها أجنبية، وإطلاق أحكام مسبقة عليهم.	قاموس أكسفورد باللغة الإنكليزية	"xenophobia, n.". OED Online. June 2021. Oxford University Press. https://www.oed.com/view/Entry/	Legal1.3.1

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
				230996?redirectedFrom=xenophobia (تم تصفح الموقع في 30 أغسطس 2021).	
المبادرات الوطنية		الأنشطة المضطلع بها على الصعيد الوطني لمعالجة شاغل معيَّن بطريقة منهجية.	GCIv2	عادةً ما تُصمَّم المبادرات القطرية لتناول مجال معيَّن يهمّ المنظمة. ومن الأمثلة على ذلك حقوق الإنسان أو التعليم أو البيئة. ويمكن أن تكون في شكل غايات أو أهداف يُعهد تحقيقها إلى واحد أو أكثر من الأعضاء من خلال الواجهة المخصصة "لإنشاء المشروعات".	
التزوير ذو الصلة بالحاسوب		يشمل التزوير ذو الصلة بالحاسوب انتحال صفة أفراد وسلطات ووكالات وكيانات أخرى مشروعة عبر الإنترنت لأغراض احتيالية.	https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html#:~:text=Computer%2Drelated%20forgery%20involves%20impersonation,entities%20online%20for%20fraudulent%20purposes.		Legal1.2
الاتصالات غير المرغوبة أو الرسائل الاقتحامية		اتصالات إلكترونية لم يرغبها المتلقي، مثل البريد الإلكتروني، أو خدمة الرسائل القصيرة، أو وسائل التواصل الاجتماعي، أو المكالمات الهاتفية. وتشير الرسائل الاقتحامية إلى مثل هذه الاتصالات غير المرغوبة المرسَلة بالجملة.	GCIv2		Legal2.7
التوقيع الإلكتروني		التوقيع الإلكتروني هو تقنية رياضية تستعمل للتحقق من صحة وسلامة رسالة أو برمجية أو وثيقة إلكترونية.	GCIv2		Legal2.6
المعاملة الإلكترونية		المعاملة الإلكترونية هي عملية بيع أو شراء سلع أو خدمات سواء كانت بين شركات تجارية وأسر منزلية وأفراد وحكومات ومنظمات من القطاعين العام والخاص، تجري عبر شبكات حاسوبية؛ وتشمل الأمثلة على هذه النصوص التشريعية قانون التجارة الإلكترونية والقانون الخاص بالتوقيعات الإلكترونية وقانون المعاملات الإلكترونية، وما إلى ذلك، والتي قد تحتوي	GCIv2		

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
		على لوائح بشأن إنشاء إدارة لمراقبة سلطات منح الشهادات.			
معايير الأمن السيبراني		وجود إطار (أطر) معتمد (معتمدة) من الحكومة (أو تحظى (يحظى) بتأييدها) من أجل تنفيذ معايير الأمن السيبراني المعترف بها دولياً داخل القطاع العام (الوكالات الحكومية) وداخل البنى التحتية الحيوية (حتى ولو كان القطاع الخاص هو من يقوم بتشغيلها). وتشمل هذه المعايير، على سبيل المثال لا الحصر، تلك التي تضعها الوكالات التالية: المنظمة الدولية للتوحيد القياسي (ISO)، والاتحاد الدولي للاتصالات (ITU)، وفريق مهام هندسة الإنترنت (IETF)، ومعهد مهندسي الكهرباء والإلكترونيات (IEEE)، وتحالف حلول صناعة الاتصالات (ATIS)، ومنظمة تطوير معايير المعلومات المنظمة (OASIS)، ومشروع شراكة الجيل الثالث (3GPP)، والمشروع 2 لشراكة الجيل الثالث (3GPP2)، ومجلس تصميم الإنترنت (IAB)، وجمعية الإنترنت (ISOC)، ومجموعة السلامة على الإنترنت (ISG)، وISI، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، وISF، وRFC، وISA، واللجنة الكهرتقنية الدولية (IEC)، وNERC، وNIST، وFIPS، وPCI، وDSS، وغيرها. وتنظيم الأمن السيبراني من منظور منح الشهادات/التقييس يلزم الكيانات العاملة داخل أراضي أي بلد بالحصول على البعض أو الحد الأدنى من المتطلبات المتعلقة بالشهادات/التقييس. وقد تختلف هذه المتطلبات باختلاف القطاع المعني من الاقتصاد. وتشمل هذه المعايير، على سبيل المثال لا الحصر، تلك التي تضعها الوكالات التالية: المنظمة الدولية للتوحيد القياسي (ISO)، والاتحاد الدولي للاتصالات (ITU)، وفريق مهام هندسة الإنترنت (IETF)، ومعهد مهندسي الكهرباء والإلكترونيات (IEEE)، وتحالف حلول صناعة الاتصالات (ATIS)، ومنظمة تطوير معايير المعلومات المنظمة (OASIS)، ومشروع شراكة الجيل الثالث (3GPP)، والمشروع 2 لشراكة الجيل الثالث (3GPP2)، ومجلس تصميم الإنترنت (IAB)، وجمعية الإنترنت (ISOC)، ومجموعة السلامة على الإنترنت (ISG)، وISI، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، وISF، وRFC، وISA، واللجنة الكهرتقنية الدولية (IEC)، وNERC، وNIST، وFIPS، وPCI، وDSS، وغيرها.		تعريف GCIv4 وGCIv2	Legal2.5
التمارين المتعلقة بالأمن السيبراني (مثل التدريبات السيبرانية)		حدث مخطط تقوم خلاله منظمة ما بمحاكاة خلل سيبراني من أجل تطوير أو اختبار إمكانات مثل المنع أو الاكتشاف أو التخفيف من الآثار أو الاستجابة أو	GCIv4		Tech1.2.2

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
		الاستعادة فيما يتعلق بحالات الخلل هذه.			
التدريب السيبراني		التدريب السيبراني حدث سنوي تجري خلاله محاكاة هجمات سيبرانية، أو حوادث أمن المعلومات أو أنواع أخرى من الأعطال من أجل اختبار القدرات السيبرانية لمنظمة ما، وذلك من القدرة على الكشف عن حادث أمني إلى القدرة على الاستجابة بشكل مناسب وتقليل أي تأثير ذي صلة. ومن خلال التدريب السيبراني، يتمكن المشاركون من إقرار السياسات والخطط والإجراءات والعمليات والقدرات التي تمكن من إعداد العمليات ومنعها والاستجابة لها واستعادتها واستمراريتها.	تعريف الاتحاد الدولي للاتصالات	https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx	Tech1.2.2
الإشعارات المتعلقة بالأمن السيبراني		إشعارات الأفرقة CIRT: عرض المعلومات على الجمهور العام بشأن التهديدات السيبرانية الناشئة والإجراءات التي يوصى باتخاذها.	GCIv4		Tech1.2.3
الانضمام إلى منتدى أفرقة الأمن والتصدي للحوادث (FIRST)		عضو كامل أو جهة اتصال في منتدى أفرقة الأمن والتصدي للحوادث. www.first.org	GCIv4		Tech1.3
الانضمام إلى أفرقة CIRT/CERT/CSIRT الإقليمية		أي علاقة رسمية أو غير رسمية مع أي فريق CERT آخر داخل أو خارج البلد، كجزء من أي فريق CERT إقليمي. وتشمل أمثلة الأفرقة CERT الإقليمية APCERT وAFRICACERT وEGC وOIC وOAS.	GCIv4		Tech1.4
أفرقة CSIRT/CIRT/CERT القطاعية		إن أي فريق من أفرقة CSIRT/CIRT/CERT القطاعية هو كيان يتعامل مع حوادث أمن الحواسيب أو الأمن السيبراني التي تؤثر على قطاع بعينه. وتشكَّل الأفرقة CERT القطاعية عادةً من أجل القطاعات الحساسة مثل الرعاية الصحية والمرافق العامة وخدمات الطوارئ والقطاع المالي. وخلافاً للفريق CERT الحكومي الذي يقدم خدماته إلى القطاع العام، يقدم الفريق CERT القطاعي خدماته إلى هيئات من قطاع وحيد فقط.	GCIv2		Tech2.1
التعاون الدولي في مجال الأمن السيبراني		التعاون بين حكومتين أو أكثر أو وكالات وطنية أو هيئات تنظيمية وطنية أو أفرقة CIRT وطنية أو منظمات من المجتمع المدني أو هيئات أكاديمية.			Org1.8
آليات وقدرات الإبلاغ		مثل الخطوط الوطنية للمساعدة والخطوط الساخنة الموصولة بنظام الخطوط الدولية للمساعدة. وينبغي توصيل هذه الخطوط بأنظمة الإحالة والدعم.			Org4.3
الحملات العامة للتوعية بالأمن السيبراني		تشمل التوعية العامة الجهود التي تبذل في سبيل تشجيع وصول حملات التوعية إلى أكبر عدد ممكن من المواطنين والاستفادة	GCIv4		CapDev1.

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
		من المنظمات غير الحكومية والمؤسسات والمنظمات وموردي خدمات الإنترنت والمكتبات ومنظمات التجارة المحلية والمراكز المجتمعية وكليات المجتمعات المحلية وبرامج تعليم الكبار والمدارس ومنظمات أولياء الأمور-المعلمين من أجل توصيل الرسالة إلى الجميع بشأن السلوك الآمن من الناحية السيبرانية على. ويتضمن ذلك إجراءات من قبيل إنشاء بوابات ومواقع شبكية لإذكاء الوعي، ونشر مواد الدعم وغيرها من الأنشطة الأخرى.			
مركز العمليات الأمنية	SOC	" مركز العمليات الأمنية هو وحدة تنظيمية تعمل في صميم جميع عمليات الأمن. وعادة ما لا ينظر إليها ككيان أو نظام واحد، بل كهيكل معقّد لإدارة وتعزيز الوضع الأمني الشامل لمنظمة ما. وتتمثل وظيفتها في تحديد وتحليل ومواجهة التهديدات والحوادث المتعلقة بالأمن السيبراني باستخدام الأفراد والعمليات والتكنولوجيا. ويمكن تحديد هذه الأنشطة ضمن سبعة أبعاد أو مجالات وظيفية لمركز العمليات الأمنية. وعلى الرغم من أن هذه المراكز تحظى بقبول واسع النطاق باعتبارها بالغة الأهمية لأمن الشركات، فإنها لا تزال تُعتبر آلية دفاع سلبية قائمة على ردّ الفعل". "فريق التصدي للحوادث الأمنية الحاسوبية: يستخدم هذا المصطلح في كثير من الأحيان بالتبادل مع مصطلح مركز العمليات الأمنية على الرغم من أنه يركز بشكل أساسي على عنصر الاستجابة بعد وقوع هجوم ما. وفريق التصدي للحوادث الأمنية الحاسوبية هو وحدة تنظيمية مسؤولة عن تنسيق ودعم الاستجابة لحادث متعلق بأمن الحواسيب. ويُعتبر فريق التصدي للحوادث الأمنية الحاسوبية إما فريقاً مستقلاً أو جزءاً من أحد مراكز العمليات الأمنية" "مركز العمليات الشبكية: يشرف مركز العمليات الشبكية (NOC) على تحديد المشاكل والتحري عنها وترتيبها من حيث الأولوية وتفاقمها وحلها. غير أن المشاكل التي يتم تناولها في مركز العمليات الشبكية مختلفة لأن هذا المركز يركّز على الحوادث التي تؤثر في أداء شبكة منظمة ما وتيسّرها. وبما أن الحوادث يمكن أن تقع في جميع الأنظمة وليس في الشبكات حصراً، فإنه من المفيد للمنظمات أن تعمل أفرقة مراكز العمليات الأمنية ومراكز العمليات الشبكية معاً" "مركز الاستخبارات الأمني: استُعمِل المصطلح "مركز الاستخبارات الأمني" (SIC) لأول مرة في عام 2017 لوصف الهيئة التي حلت محل مركز العمليات الأمنية. ويهدف مركز الاستخبارات الأمني إلى تقديم رؤية أكثر شمولاً وتكاملاً من مركز العمليات	https://ieeexplore.ieee.org/document/9296846		

المصطلح	المختصر	التعريف	المصدر	أمثلة	الأسئلة المشار إليها (GCIv4)
		الأمنية، ويمكنه أن يرى ويدير المعلومات الاستخباراتية الأمنية بشكل كامل في مكان واحد. وبالتالي، يتم الجمع بين عدة تكنولوجيات (مثل إدارة المعارف المتعلقة بأمن المعلومات (IS) ومعالجة البيانات الضخمة)." "إدارة المعلومات والأحداث الأمنية (SIEM) جزء لا يتجزأ من عمل العديد من مراكز العمليات الأمنية، وتغطي جزءاً كبيراً من المتطلبات التكنولوجية. وهي مسؤولة عن جمع البيانات المتصلة بالأمن بطريقة مركزية. وبالتالي، فإنها توفّر القدرات اللازمة للتحليل الأمني من خلال استنباط الصلات بين الأحداث المسجَّلة. وتمكِّن وظائف أخرى من إضافة بيانات متعلقة بالسياق وتطبيع البيانات غير المتجانسة والإبلاغ والإنذار [73]. ولإتاحة تبادل المعلومات المتعلقة بالتهديدات، تتيح إدارة المعلومات والأحداث الأمنية الدخول إلى منصات تبادل المعلومات الاستخباراتية المتعلقة بالتهديدات السيبرانية، وتشمل محللين في مجال الأمن البشري من خلال توفير قدرات التحليلات الأمنية المرئية. وتشمل قدرات متعلقة بإدارة السجلات من خلال تخزين بيانات الأحداث لفترة طويلة"			