JIU/REP/2021/3

الأمم المتحدة

الأمن السيبراني في مؤسسات منظومة الأمم المتحدة

تقرير وحدة التفتيش المشتركة

من إعداد خورخي فلوريس كاييخاس، وعائشة عفيفي، ونيكولاي لوزينسكي

JIU/REP/2021/3
Arabic
Original: English

الأمن السيبراني في مؤسسات منظومة الأمم المتحدة

تقرير وحدة التفتيش المشتركة

من خورخي فلوريس كاييخاس، وعائشة عفيفي، ونيكولاي لوزينسكي

الأمم المتحدة، جنيف، 2021

فريق المشروع

خورخي فلوريس كاييخاس، وعائشة عفيفي، ونيكولاي لوزينسكي، مفتشون

فنسنت هيرمي، موظف للتقييم والتفتيش

سيلفيا بيسكوف، موظفة مساعدة للتقييم والتفتيش

هيرفي بودات، مساعد بحوث

ديان دينسيك، استشاري

شارلوت كلافو، وألينا داتسي، وبيانكا كانيفاري، متدربون

موجز تنفيذي

الأمن السيبراني في مؤسسات منظومة الأمم المتحدة

في عالم اليوم الرقمي، برز الأمن السيبراني كمسألة ذات أهمية للمنظمات الدولية. والأمم المتحدة ليست استثناء من ذلك. فقد أدى التحول الرقمي والاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات والحلول الممكّنة سيبرانياً، وواقع النمو المتواصل في التهديدات السيبرانية، سواء من حيث التعقيد أو الإمكانات التخريبية، إلى زيادة غير مسبوقة في مخاطر الأمن السيبراني التي تواجه منظومة الأمم المتحدة. ومع أن الأمن السيبراني ظهر في البداية في مجال تكنولوجيا المعلومات والاتصالات، فإنه لم يعد من المجدي الآن أن ننظر إليه من خلال العدسة التقييدية لتكنولوجيا المعلومات والاتصالات وحدها، خاصة بعد أن أصبحت أنظمة إدارة المعلومات متأصلة بعمق في معظم أنشطة الأعمال، وبعد أن تطور مشهد التهديدات بشكل كبير، وأصبح يتطلب أكثر من مجرد دفاعات تحركها التكنولوجيا. ويطرح المفتشون في هذا التقرير الأسباب التي تقضي بإدماج اعتبارات الأمن السيبراني في الأطر الأوسع في المنظمات، من قبيل الإدارة المركزية للمخاطر، والتخطيط لاستمرارية الأعمال، والسلامة والأمن، مما يتطلب تعميم هذه المسألة على المنظمة المعنية ككل.

وقد شهدت منظومة الأمم المتحدة في السنوات الأخيرة فهماً متزايداً لكون الأمن السيبراني يتطلب الاهتمام. فالعواقب المحتملة لضعف حالة الأمن السيبراني تتجاوز فعلاً تعطيل البنية التحتية لتكنولوجيا المعلومات والاتصالات وأنظمتها أو حجم البيانات التي تتعرض للاختراق في نهاية الأمر. فهي تُعرِّض للخطر قدرة مؤسسات منظومة الأمم المتحدة على تنفيذ ولاياتها ومصداقيتها أمام أعضائها والمستفيدين منها. وعلاوة على ذلك، فإن كثيراً من فئات الأشخاص الذين تحتفظ مؤسسات منظومة الأمم المتحدة ببياناتهم يمكن أن يتعرضوا لعواقب ضارة كبيرة في حالة التسرب. ومع أن تأثير الهجمات السيبرانية على المنظمات ذات الولايات والهياكل المتنوعة يمكن أن يتباين، فإن التهديد حقيقي ومشترك. ولا يمكن لأي منظمة أن تتوقع ألا تتعرض أبداً لحادث يتعلق بالأمن السيبراني، بغض النظر عن مدى استعدادها أو يقظتها. وعلاوة على ذلك، يمكن في حال إهمال تلك المخاطر أن تكون الآثار المترتبة على السمعة وعلى الجوانب التشغيلية والقانونية والمالية كبيرة.

أهداف هذا الاستعراض وهيكل التقرير

تتمثل الأهداف الرئيسية لهذا الاستعراض فيما يلي: (أ) تحديد وتحليل تحديات ومخاطر الأمن السيبراني المشتركة التي تواجهها مؤسسات منظومة الأمم المتحدة بشكل فردي، وكذلك استجابات كل منها لها، مع مراعاة المتطلبات السياقية الخاصة للمنظمات (المنظور العمودي)؛ و(ب) دراسة الديناميات الحالية المشتركة بين الوكالات والتي تيسر الأخذ بنهج شامل للمنظومة ككل إزاء الأمن السيبراني من أجل تحسين التنسيق والتعاون وتبادل المعلومات بين مؤسسات منظومة الأمم المتحدة، وعند الاقتضاء، إمكانية إيجاد حلول مشتركة (المنظور الأفقي).

واستناداً إلى التقييم الذاتي الذي وفرته المنظمات المشارِكة، يقدم المفتشون أولاً، في الفصل الثاني، لمحة موجزة عن مشهد الأمن السيبراني الذي تواجهه منظومة الأمم المتحدة، تصف أكثر أنواع التهديدات ووسائل الهجوم انتشاراً، مع تبيان أثرها المبلغ عنه، وتلفت الانتباه إلى مسائل تقنية مختارة تحتاج إلى مزيد من الدراسة. ويتناول المفتشون في الفصل الثالث الترتيبات المؤسسية والممارسات ذات الصلة في مؤسسات منظومة الأمم المتحدة بالإشارة إلى مجموعة عناصر رئيسية محددة في سياق

الاستعراض تساهم في قدرة المنظمة على الصمود في المجال السيبراني وتسلط الضوء على الممارسات الجيدة حيثما ينطبق ذلك. وينصبُّ التركيز في الفصل الرابع على الآلية المشتركة بين الوكالات التي تهدف إلى تعزيز التنسيق والتعاون بين مؤسسات منظومة الأمم المتحدة، وعلى القدرات التشغيلية التي تمكّن من وضع حلول مشتركة في مجال الأمن السيبراني ومن تنفيذها، حيثما تكون هذه الحلول معقولة. وهناك توافق في الآراء بين الخبراء على أن الاستجابة يجب أن تستند إلى الخصائص والمتطلبات المحددة لدى كل منظمة (استناداً إلى ولايتها، والمعلومات التي تمتلكها أو تُديرها، ودرجة التعرض، ومستوى الموارد، وما إلى ذلك). وفي الوقت نفسه، لا تعمل مؤسسات منظومة الأمم المتحدة بمعزل عن بعضها البعض، فهي مترابطة في كثير من النواحي، بما في ذلك من خلال البرامج المشتركة ودرجة من الترابط بين ولاياتها وأنشطتها. ولذا فإن التعرف على مجالات التعرض المشترك يكتسي أهمية بالغة، شأنه في ذلك شأن استكشاف المجالات التي تصلح لاتباع نهج منسق إزاءها.

الأمن السيبراني في منظومة الأمم المتحدة

لا يمكن لأي مؤسسة من مؤسسات منظومة الأمم المتحدة القول بأنها لم تتعرض لشكل من أشكال الهجمات السيبرانية، كبيرها أو صغيرها. وتُعتبر الإجراءات الخبيثة التي تستهدف إما مستخدمي أنظمة المعلومات (من خلال مخططات التصيد الاحتيالي أو سرقة الهوية أو "الرجل الوسيط" وما إليها) أو البنية التحتية (البرمجيات الخبيثة، وهجمات حجب الخدمة الموزع، وما إلى ذلك)، المصدرَ الأكثر شيوعاً للتهديدات المبلغ عنها. وفي حين أن تهديدات الأمن السيبراني ترتبط بشكل عام بالعمليات التقنية المعقدة، فإن مجتمع الخبراء يلاحظ أن هناك تحولاً ملحوظاً من اختراق قراصنة الحواسيب للخوادم والشبكات وأجهزة الاستخدام النهائي إلى قرصنة الأشخاص، وذلك باستخدام طرائق الهندسة الاجتماعية التي تهدف إلى التلاعب بالأفراد لإفشاء المعلومات الحساسة لأغراض احتيالية وغير مشروعة أخرى. وقد أدت جائحة كوفيد-19 إلى تفاقم المخاطر المتعلقة بالهندسة الاجتماعية، إذ أبلغ أكثر من ثلثي المنظمات المشارِكة عن زيادة حادة في تهديدات الأمن السيبراني ونقاط الضعف فيه شهدتها فترات الإغلاق العالمي التي فصلت كثيراً من المستخدِمين عن موارد الأمن السيبراني المدارة مركزياً.

وفي الوقت نفسه، كان الأثر المبلغ عنه والناجم عن الحوادث التي تعرضت لها المنظمات المشارِكة محدوداً، مما يمكن أن يؤدي إلى استنتاج سابق لأوانه بعدم وجود سبب جدي للقلق. على أن ذلك ليس هو الاستنتاج الذي خلص إليه المفتشون. أولاً، تشير البيانات التي تم جمعها بالضرورة إلى بعض النقاط العمياء، ومنها ما ينجم عن إحجام يمكن فهمه عن الكشف عن مستوى الضعف المعروف، فضلاً عما يتأتى عن الطبيعة العتِمة للأنشطة السيبرانية بشكل عام، مما يشير إلى أن الحجم الدقيق للتهديدات والعواقب ذات الصلة قد يكون ببساطة غير معروف. وفي معظم الأوقات، لا سيما في حالة الهجمات الأكثر تعقيداً، ليس لدى الخصوم أي حافز للكشف عن وجودهم أو عن أوجه الضعف التي استغلوها، مما يشير إلى ترجيح أن يكون عدد خروقات الأنظمة وتسرب البيانات أعلى بكثير مما يُبلّغ عنه. فنسبة "المجاهيل المعروفة" مقارنة بما هو معروف عن حجم تهديدات الأمن السيبراني كبيرة، ولكن قد يكون نصيب "المجاهيل المجهولة" مصدر قلق أكبر. لذلك، فإن من الخاطئ أن يُحكَم على جدية التهديد على أساس مدى ما يعرف أنه قد تحقق في الماضي. ويبقى احتمال وقوع الضرر عالياً ويتطلب استمرار الاهتمام به ومنحه الأولوية.

الاختلاف في نضج المنظمات وفي جوانب مختارة من استعدادها التكنولوجي

ليس المقصود من هذا الاستعراض إجراء تقييم شامل لصلابة الترتيبات التشغيلية أو البنية التحتية التقنية لكل منظمة مشاركة، وإنما التوصل إلى فهم للقدرات العامة القائمة وعزل بعض المشاكل المشتركة التي قد تستحق اهتماماً خاصاً. ولأسباب واضحة ترتبط بموضوع هذا الاستعراض، اختار المفتشون عدم إفشاء ترتيبات محددة لدى المنظمات المعنية يمكن أن تعرِّض أمنها للخطر. ومع مراعاة المحدودية المتأصلة في المعلومات التي جُمعت من خلال التقييم الذاتي في المقام الأول، فضلاً عن التباين الكبير في مستوى التفاصيل التي قدمها المجيبون، لاحظت وحدة التفتيش المشتركة وجود اختلافات كبيرة في النهج الذي أخذت به المنظمات المشارِكة في ردودها على تهديدات الأمن السيبراني، ونتيجة لذلك، في نضج حالة الأمن السيبراني لديها. ويمكن تفسير هذه الاختلافات من حيث ما يلي: البيئة التي تعمل فيها كل منظمة؛ والمتطلبات التي يمليها نوع البيانات المحفوظة؛ ومستوى الفهم والأولوية التي تمنحها قيادات تلك المنظمات للأمن السيبراني؛ والمنظور التاريخي لكل من المنظمات؛ وتوفر الموارد؛ والتنوع الكبير في أنظمة تكنولوجيا المعلومات والاتصالات وأدواتها والحلول البرامجية المستخدمة عبر المنظومة.

وترى المنظمات المشارِكة أنها تفهم جيداً الجوانب التقنية الأساسية للأمن السيبراني وأنها استثمرت فيه وفقاً لقدرات كل منها. وفيما يتعلق بالقدرات التكنولوجية والتشغيلية، اقتصر المفتشون في تحليلهم على إبراز سلسلة من المسائل التي قد تستحق مزيداً من الاهتمام المركّز، منها مثلاً إدارة أجهزة الاستخدام النهائي والأدوات التي تيسر العمل عن بُعد، ولا سيما في سياق جائحة كوفيد-19؛ والمخاطر المرتبطة بمخلفات الأنظمة القديمة التي كانت قد اشتُريت في الماضي أو أنشئت داخلياً عبر الزمن، وهي أنظمة يمكن أنها أصبحت غير مدعومة بالفحوصات والإصلاحات الأمنية المعاصرة؛ والتوسع المستمر في استخدام الحوسبة السحابية؛ وترتيبات المنظمات لإدارة مكامن الضعف؛ وممارسات تكنولوجيا معلومات الظلّ (shadow IT) التي تتضمن استخدام وتنفيذ أدوات تكنولوجية خارج إطار العمل المؤسسي لتكنولوجيا المعلومات والاتصالات. وتجدر الإشارة إلى أنه على الرغم من العديد من التحديات المواجَهة، فقد أدى ظهور الجائحة إلى بعض التطورات الإيجابية أيضاً. فقد اضطرت كيانات الأمم المتحدة إلى إلقاء نظرة فاحصة على أطر إدارة الأمن لديها، وبدأت مشاريع تكنولوجيا المعلومات والاتصالات المؤسسية المخطط لها تتحقق بحكم الضرورة العاجلة. ويمكن القول إن التحول الهائل إلى العمل عن بُعد في غضون مهلة قصيرة للغاية أدى بالعديد من المنظمات إلى تسريع جهودها الموجهة لتحسين أمن الوصول عن بُعد، ولعله وفّر زخماً تشتد الحاجة إليه لتحفيز العمل في هذا المضمار.

عناصر تساهم في تحسين القدرة على الصمود في المجال السيبراني

درس المفتشون مجموعة من العناصر التي يرجح أن تؤدي إلى تحسين حالة الأمن السيبراني المؤسسي في مؤسسات منظومة الأمم المتحدة وقدرتها على تحديد التهديدات السيبرانية ومنعها واكتشافها، فضلاً عن الاستجابة للحوادث والتعافي منها. ويتعين الأخذ بنهج متعدد الأوجه يشمل جميع مستويات المنظمة: الهيئات التشريعية والإدارية؛ وآليات الرقابة؛ والادارة التنفيذية؛ والمديرون المتوسطو المستوى في الوحدات الإدارية والفنية أو وحدات الأعمال؛ والقوى العاملة عموماً. بالإضافة إلى ذلك، تتطلب طبيعة هذا الموضوع الجامعة رؤية أوسع تتجاوز تكنولوجيا المعلومات والاتصالات وتدمج الأمن السيبراني بقوة في الإدارة المركزية للمخاطر، فضلاً عن السعي لتحقيق تقارب أكبر بين الأمن

المادي والأمن السيبراني. أخيراً وليس آخراً، تشكل قدرة الموارد البشرية الداخلية المتخصصة المستكملة بخدمات يتم الحصـــول عليها من مقدمي خدمات خارجيين لتلبية احتياجات محددة ومخصـــصـــة، وبتخصيص موارد مالية تتناسب مع احتياجات كل منظمة، العمود الفقري لوضع متين في مجال الأمن السيبراني. وباختصار، تؤثر درجة انعكاس هذه العناصر في نهج المنظمة إزاء الأمن السيبراني بشكل مباشر على قدرتها على الصمود في المجال السيبراني. ولذلك يوصي المفتشون بأن يشرع الرؤساء التنفيذيون في إجراء استعراض على نطاق المنظمة لدراسة مدى إدراج كل عنصر من هذه العناصر، على النحو المفصل أدناه، في سياسات المنظمة وممارساتها، وإبلاغ الهيئات التشريعية والرئاسية لكل من المنظمات بالنتائج بهدف تلقي التوجيهات حول سبل زيادة تعزيز القدرة على الصمود في المجال السيبراني، مع مراعاة أوجه القوة والضعف المحددة في تلك العملية (التوصيتان 1 و2).

على الهيئات التشريعية والرئاسية أن تقدم التوجيه الاستراتيجي وأن توفر الموارد

في منظومة الأمم المتحدة، لا يزال يُنظر إلى الأمن الســـيبراني على أنه مســـألة تقنية في الغالب، مما يمكن أن يفسر سبب محدودية الدعوة الموجهة إلى الهيئات التشريعية والرئاسية، أو قيامها هي بالدعوة، إلى الانخراط في هذا الموضـــوع في معظم المنظمات حتى الآن. ويرى المفتشـــون، في ضوء الأبعاد الأوسع للأمن السيبراني المحددة في هذا التقرير، أنه ينبغي للهيئات التشريعية والرئاسية أن تضاعف انخراطها في هذه المسألة وأن تقدم توجيهات استراتيجية رفيعة المستوى، بما في ذلك من خلال صياغة بيان صريح حول درجة تقبل المخاطر وما يقابل ذلك من تخصيص للموارد للمساهمة في بلوغ مستوى الحماية المطلوب. وعلى الصـعيد الأعم، ينبغي للإدارة التنفيذية أن تفكر في السبل التي يجري من خلالها إبلاغ الهيئات التشريعية والرئاسية بصورة منتظمة حول مسائل الأمن السيبراني، وفي طرق استخدام هذا الإبلاغ لتيسير التفاعل مع تلك الهيئات، في حدود ما يمكن اعتباره ضرورياً وكافياً دون المساس بدفاعات المنظمة. وبالنظر إلى الطبيعة المفاجئة لحوادث الأمن السيبراني والتي يمكن أن تكون عالية الأثر، يشير المفتشون على المنظمات أيضاً بأن تستبق الحاجة إلى تصعيد الحوادث إلى مستوى الهيئات التشريعية والرئاسية، وأن تستبق أيضاً الإجراءات التي يتعين اتباعها في الحالات التي تتطلب ذلك التصعيد، على المستوى الداخلي وبين أعضاء تلك الهيئات أنفسهم.

يساهم اهتمام هيئات الرقابة في تعزيز تدابير الأمن السيبراني

تبين أن آليات الرقابة الداخلية والخارجية في مؤسسات منظومة الأمم المتحدة كانت مهتمة بمسائل الأمن السيبراني حتى في حال عدم وجود إشارات محددة في ولاياتها إلى الموضوع بحد ذاته. وقد صادف المفتشون عدة أمثلة على التحسينات المؤسسية التي أُدخلت على إطار الأمن السيبراني في المنظمات المشارِكة، وهي تحسينات انبثقت عن توصيات الرقابة (من قبيل إنشاء منصب رئيس موظفي أمن المعلومات، والتوصيات الخاصة بالتدريب، ووضع خارطة طريق يمكن تفعيلها، وما إلى ذلك). والواقع أن لجان المراجعة والرقابة تتناول مسائل الأمن السيبراني كجزء من ولايتها التي تغطي الإدارة المركزية للمخاطر وليس في سياق الحوكمة المعنية بتكنولوجيا المعلومات والاتصالات. ومن الجدير بالثناء أن هذه اللجان تبنت هذا الموضوع، ليس لمجرد دعم الإدارة ولكن أيضاً كطريقة لإطلاع الهيئات التشريعية والإدارية على مخاطر الأمن السيبراني ذات الصلة، وتمكينها من المساهمة في التخفيف من المخاطر التي تواجه المنظمات. وللتأكد من أن جميع هيئات الرقابة تضيف قيمة قصوى من وجهة نظر الأمن السيبراني، من الأهمية بمكان أن يسترشد عمل وظيفة الرقابة بما لدى خبراء الأمن السيبراني داخل المنظمة من معرفة وخبرة، وأن تصبّ هذه المعرفة والخبرة في ذلك العمل.

الأطر التنظيمية والامتثال والمساءلة

تشير المنظمات المشارِكة إلى مجموعة واسعة من معايير الصناعة فيما يتعلق بالأمن السيبراني، بل إن هناك في بعض الأحيان أكثر من معيار واحد، وقد حصل معظم المنظمات بالفعل على شهادة بموجب معيار المنظمة الدولية لتوحيد المقاييس رقم 27001، أو هي تخطط للقيام بذلك، أو أنها اختارت مواءمة إطارها طواعية مع ذلك المعيار دون طلب شهادة رسمية. ويمتنع المفتشون عن تأييد معيار صناعي واحد أو الدعوة لاتباع نهج منسق على نطاق المنظومة ككل في هذا الصدد، فالمعايير المختلفة يمكن أن تخدم بشكل سليم أغراضاً مختلفة وأن توفر خيارات تتناسب مع مستويات النضج المختلفة. ومع ذلك، هناك مبرر قوي للاسترشاد – سواء بشكل رسمي أو غير رسمي – بمعايير الصناعة ذات الصلة عند وضع الإطار التنظيمي وإدارته. لذلك يتعين على المنظمات المشارِكة أن تحدد المعيار الملائم، ثم أن تحدّد، ضمن ذلك المعيار، الضوابط الأكثر صلة بأغراضها، استناداً إلى مستوى الحماية المطلوب الذي يتفق مع حالتها، رهناً بالاحتياجات والمخاطر التي يتم تحديدها من خلال تقييم مناسب لمخاطر الأمن السيبراني التي تتعرض لها.

وتتطلب عدة معايير رائدة في هذه الصناعة وجود سياسات محددة للأمن السيبراني وإجراءات موثقة كركيزة أساسية للضوابط التي تدعم نهج الكيان إزاء الأمن السيبراني. ومع استثناءات قليلة، يمكن القول إن المنظمات المشارِكة قد أدركت أهمية وجود إطار مرجعي مفصل يسترشد به نهجها إزاء الأمن السيبراني. وعموماً، تشمل الاستراتيجيات الرفيعة المستوى لتكنولوجيا المعلومات والاتصالات الأمن السيبراني، وإن كان ذلك بدرجات متفاوتة من التفصيل. وقد أنشأ أكثر من ثلثي المنظمات المشارِكة أدوات خاصة بالأمن السيبراني، وهناك ثلاث منظمات تجري حالياً تنقيحاً لإطارها، بينما تعمل أربع منظمات أخرى على وضع سياسات منفصلة. وفي الوقت نفسه، اعتبرت أربع منظمات مشارِكة وظيفة الأمن السيبراني، بما في ذلك الإطار التنظيمي المتصل بتلك الوظيفة، على أنها في مرحلة الولادة على الأكثر. ولا توحي مسألة الامتثال للإرشادات المعمول بها – وخاصة الإنفاذ في حال عدم الامتثال – إلا بدرجة أقل من الثقة بوجود ثقافة للأمن السيبراني المؤسسي في المنظومة ككل. ويرى المفتشون، أن هذا يتطلب نظرة فاحصة ونهُجاً أكثر دقة لتعزيز المساءلة عن الخروقات ولحماية المنظمات بشكل عام.

تتدرج ثقافة الأمن السيبراني من القيادة نزولاً إلى القاعدة

تتمثل الخطوة الأولى نحو غرس ثقافة الأمن السيبراني في أن تكون القيادة العليا نفسها على دراية بالمخاطر المرتبطة به وأن تطور فهماً للآثار المترتبة على ضعف الصحة السيبرانية. ويستلزم ذلك موقفاً أكثر نشاطاً من جانب كبار المديرين في ضمان إنشاء آليات للحوكمة الداخلية بصورة تزودهم بما يحتاجون إليه من معلومات وقاعدة للأدلة. ويتجاوز دور الإدارة التنفيذية في هذا الصدد اتخاذها لقرارات تخصيص الموارد. فأحد العناصر الأساسية لهذا الدور يتمثل في تشجيع قيام ثقافة داخلية لا يُنظر فيها إلى الاعتراف بوقوع الحوادث وتتبعها استباقياً على أنه قبول بالفشل، بل كنقطة انطلاق للمعالجة المشتركة لمشكلة عامة ولتوفير حماية أفضل للمنظمة وأصولها. وهناك طرق إضافية يمكن للإدارة التنفيذية من خلالها إلهام العمل والتأثير بشكل ملموس على العقليات نزولاً عبر سلسلة القيادة من خلال الأخذ بسلوكيات تعتبر نماذج للسلوكيات التي توصي باتباعها، وضمان المساءلة الإدارية عبر المنظمة، والمشاركة في برامج التوعية، والتحلي بأسلوب القيادة الملتزمة في مسائل الأمن السيبراني عموماً. وهناك حاجة إلى تحول ثقافي في منظومة الأمم المتحدة، ولتحقيق ذلك تكتسي مساهمة المديرين التنفيذيين في تحديد التوجه من القمة نزولاً أهمية أساسية.

تعميم الأمن السيبراني كمسعى شامل للمنظمة بأكملها

تماشياً مع الفهم المتزايد بأن المسؤولية عن الأمن السيبراني لا يمكن أن تقع على عاتق إدارات تكنولوجيا المعلومات والاتصالات وحدها، تعترف غالبية المنظمات المشارِكة، بشكل أو بآخر، بأن إدارات الشؤون الإدارية، فضلاً عن الإدارات الفنية، لها دور تؤديه. غير أن المعلومات التي جُمعت في سياق هذا الاستعراض تشير إلى أن الوحدات العاملة في جميع المنظمات ربما لا تزال لا تتقبل على نحو كاف إدراج متطلبات الأمن السيبراني والقدرة على الصمود في تصميم مشاريعها وأنشطتها وتنفيذها. وقد ذُكر أن سياسات وإجراءات الأمن السيبراني تُعتبر في بعض الأوساط عائقاً أمام مرونة التشغيل وكفاءته وليس دروعاً واقية لسمعة المنظمات وأصولها. ويكتسي أهمية خاصة أن يتصدى الرؤساء التنفيذيون بقوة لمثل هذه التصورات. ويمكن لجعل أبعاد الأمن السيبراني في الوظائف البرامجية والإدارية أكثر وضوحاً أن يقلل من سوء الفهم حول الأدوار والمسؤوليات التكميلية للإدارات المختلفة وأن يعالج نقص تولي زمام الأمور الذي لوحظ بين بعض أصحاب المصلحة خلال المراجعة الحالية. وسيكون تعميم اعتبارات الأمن السيبراني في السياسات والممارسات الناظمة لعمل جميع الإدارات في حد ذاته إقراراً بأن لدى كل وظيفة في المنظمة دوراً تساهم به في تحقيق نهج المنظمة بأكملها إزاء هذا الموضوع.

القوى العاملة كخط دفاع أول

يستمر التحدي المتمثل في تثقيف كل فرد من القوى العاملة بشأن دوره في حماية معلومات المنظمة وأصولها الرقمية، فضلاً عن أهمية التقيد بسياسات الأمن السيبراني وإجراءاته وأفضل الممارسات الخاصة به. وقد تزايدت أهمية العامل البشري لا في المشهد العام لتهديدات الأمن السيبراني فحسب، مما ينعكس في القلق العالمي بشأن استهداف المستخدِمين النهائيين الفرديين بشكل متزايد، ولكن أيضاً كعنصر مهم في هيكل الدفاع في المنظمات المشارِكة، شريطة أن يكون هؤلاء المستخدِمون مثقفين بشكل صحيح. وقد أدى إدراك أن مسؤولية الحماية السيبرانية تبدأ بمستخدِمين يتحلون بحسن الاطلاع وباليقظة إلى بذل جهود كبيرة فيما يتعلق بمبادرات التدريب والتوعية، على الرغم من محدودية الموارد ومن سأم المستخدِمين من التدريب والصعوبات في مواكبة تطورات الموضوع المستمرة. على أنه لا يبدو أن البرامج والمبادرات الفردية، على كثرتها، تُتابَع بصورة متسقة أو منهجية أو قائمة على المخاطر. ولذلك فإن المفتشين يشيرون على المنظمات بأن تسعى إلى تطوير برنامج شامل للتدريب والتوعية يُصمَّم كأداة استباقية لتغيير الثقافة الداخلية من خلال وضع أهداف واضحة محددة لكل فئة من أصحاب المصلحة اعتماداً على المخاطر التي قد يمثلونها بالنسبة للمنظمة، بدلاً من تقديم وحدات فردية للجميع لا تسترشد برؤية إستراتيجية. ويكتسي أهمية بالغة الاهتمامُ بالمستخدِمين العرضيين لأنظمة تكنولوجيا المعلومات والاتصالات المؤسسية، بما في ذلك المندوبون في المؤتمرات والمتدربون والزوّار وفئات العاملين الأخرى من غير الموظفين، نظراً لأن هؤلاء المستخدِمين كثيراً ما يدخلون البنية التحتية المؤسسية مستخدِمين أجهزتهم الشخصية. علاوة على ذلك، ولكونهم مستخدِمين غير متواترين للأنظمة المعنية، فإن من غير المرجح أن يكونوا ملمين باستخدامها السليم والآمن وفقاً للسياسات والممارسات المعمول بها في المنظمة.

تحقيق الاستفادة الأمثل من الإنفاق على الأمن السيبراني ومن الاستثمار فيه

يمثل تقدير الموارد المكرسة حالياً للأمن السيبراني تحدياً، وذلك بسبب خصائص أطر المالية والميزنة في مؤسسات منظومة الأمم المتحدة وممارساتها المتعلقة بإدارة هذه الموارد والمحاسبة الخاصة بها. وغني عن القول أن إطار الأمن السيبراني المحمي جيداً له ثمن. وعلى الرغم من الزيادة المبلغ عنها في الموارد المخصصة للأمن السيبراني، لا يزال الممارسون في منظومة الأمم المتحدة يرون أن نقص الموارد يمثل عقبة أمام تمكين منظماتهم من تغطية جميع جوانب القدرة على الصمود في المجال السيبراني. وتتمثل إحدى النقاط المهمة التي يتعين وضعها في الاعتبار أن المبلغ الذي يُنفَق على الأمن السيبراني لا يعكس تلقائياً مستوى الحماية. ويتجاوز الأمر مجرد مناقشة حجم الموارد، فالعنصر الأساسي هو تحديد المجال الذي ينبغي تخصيصها له بحيث تحقق الأثر الأشد جدوى. وبغض النظر عن حجم التمويل المتاح، فإن المعلومات التي جُمِعت لا تشير إلى وجود نهج متسق إزاء تحديد أولويات الإنفاق على الأمن السيبراني في مؤسسات منظومة الأمم المتحدة، مما يزيد من مخاطر ضعف الكفاءة في استخدام الموارد الشحيحة أصلاً. ولتحقيق الاستفادة الأمثل من الإنفاق على الأمن السيبراني، وكذلك من الاستثمار فيه، فإن إجراء تقييم شامل للمخاطر السيبرانية يتوج بعرض مفصل للتكاليف والفوائد والمخاطر والوفورات المتوقعة، بالإضافة إلى الإشارة إلى الآثار المالية المحتملة لعدم القيام بالاستثمار، يُعدُّ شرطاً مسبقاً لحشد دعم الهيئات التشريعية والرئاسية وللحصول فعلاً على مستوى كافٍ من تخصيصها للموارد.

القدرة الداخلية من حيث خبراء مجال الأمن السيبراني

قام أكثر من نصف المنظمات المشارِكة ببناء قدرات داخلية من الموارد البشرية المتخصصة والمكرسة، وهي تتراوح بين خبير واحد لأمن المعلومات، يعمل أحياناً بدوام جزئي فقط، وبين وحدة تنظيمية أكبر يرأسها رئيس لموظفي أمن المعلومات. وفي المقابل، في 10 منظمات مشارِكة، يقوم مسؤولو تكنولوجيا المعلومات والاتصالات أساساً بتنفيذ مهام الأمن السيبراني، إلى جانب مهامهم الأخرى. وهناك في مجال الأمن السيبراني نسبة عالية من استخدام الخبرة الخارجية بسبب طبيعة هذا المجال التقنية المعقدة، فهو مجال يتطور باستمرار ويتطلب درجة كبيرة من التخصص، ويطرح إبقاؤه متاحاً ومحدّثاً على أساس دائم صعوبات وتكاليف باهظة. وعلى هذا فإن اللجوء إلى مقدمي الخدمات الخارجيين لتعزيز القدرات الداخلية واستكمالها أمر لا مفر منه بل ومرغوب فيه، وذلك للاستمرار في التجاوب مع تطورات الفضاء السيبراني السريعة. أما مستوى القيام بذلك فهو يخضع لتقدير كل منظمة، استناداً إلى احتياجاتها وسياقها. على أن من الأهمية بمكان، من وجهة نظر المفتشين، أن تحتفظ المنظمات بدرجة مناسبة من الرقابة والإشراف والقدرة التقنية داخلياً للتمكن من إدارة القدرات التي يساهم بها مقدمو الخدمات الخارجيون ومن التعامل معها بشكل فعال. وفي هذا الصدد، فإن تمكّن المنظمة من الاعتماد على وظيفة يتفرغ لها كبير موظفي أمن المعلومات أن توفر التركيز والضمان اللازمين لهذا الغرض. وتتجاوز الوظائف الأساسية التي تخضع لمسؤولية كبير موظفي أمن المعلومات وضع الضوابط على المستوى التشغيلي، إذ أنها تشمل بحكم الأمر الواقع بُعداً إدارياً لضمان أقصى انعكاس ممكن لاعتبارات الأمن السيبراني كمسألة تخص إدارة المنظمة للمخاطر وقدرتها على الصمود.

ومع ملاحظة ما شهده المفتشون من فوارق في التكوين الداخلي بين المنظمات المشارِكة، وهي فوارق قد تكون أكثر دلالة على القيود المواجَهة وليست نتيجةً لاختيار متعمد أو استراتيجي، يعتقد المفتشون أن توفر خبرة مكرسة ومتخصصة في مجال الأمن السيبراني داخلياً يسهم في تدعيم وضع

المنظمة، بل وفي تعزيز وضع المنظومة ككل، وهو استثمار مجدٍ يستحق أن يُنظر فيه. إضافة إلى ذلك، فإن من الحصافة أن تجري كل منظمة تقييماً لما إذا كانت ستستفيد من القيام بإنشاء مركزٍ للعمليات الأمنية، حتى في أكثر أشكاله بساطة، على أن يستند ذلك إلى تحليلٍ للتكلفة والفائدة، وفقاً لظروف المنظمة تحديداً، يشمل معايير من قبيل مستوى تعقيد هيكل البنية التحتية لتكنولوجيا المعلومات والاتصالات في المنظمة، وعدد ونوع الأصول والعمليات الحيوية التي تديرها، والحجم الإجمالي لتدفقات البيانات فيها وبالتالي تواتر التهديدات التي تتعرض لها، وعواملَ أخرى. ويتمثل أحد الجوانب المهمة لإنشاء مركز رسمي للعمليات الأمنية، بغض النظر عن حجمه وقدرته، فيما يوفره من تركيز في رصد العمليات على أساس يومي، وما يؤديه من دور مهم في التنسيق والمزامنة، فضلاً عن التوعية على مستوى المنظمة، مما يمكن أن يُحدث فرقاً كبيراً فيما يتعلق بكفاءة تخصيص الموارد والقدرات الداخلية.

هل يُعتبر الأمن السيبراني أولوية على نطاق المنظومة ككل؟

على مر السنين، دأبت الدول الأعضاء والإدارات التنفيذية على حد سواء على القول بأولوية تعزيز وضع الأمن السيبراني لمنظومة الأمم المتحدة من خلال تعميق التنسيق والتعاون بين المنظمات على المستوى الاستراتيجي ومن خلال تعزيز القدرة التشغيلية على نطاق المنظومة ككل. ومع ذلك، وعلى الرغم من وجود عدة موارد وآليات ومبادرات هامة متاحة ضمن المنظومة، ومنها الإرادة السياسية الواضحة، فإن التقدم في جعل هذه الأقوال التطلعية حقيقة واقعة كان أقل من واضح. فحتى الآن، لا يوجد كيان واحد مكلف رسمياً بخطة للأخذ بنهج منسق إزاء الأمن السيبراني، والجهود المبذولة على نطاق المنظومة بشأن الأمن السيبراني تتركز مؤسسياً على آليات التنسيق بين الوكالات في إطار مجلس الرؤساء التنفيذيين في منظومة الأمم المتحدة المعني بالتنسيق، ويدعمها من الناحية التشغيلية، إلى حد ما، مركز الأمم المتحدة الدولي للحوسبة بصفته مقدماً لخدمات الأمن السيبراني المشتركة لعدد من مؤسسات منظومة الأمم المتحدة. وقد وجد المفتشون، في سياق هذا الاستعراض، أنه لا توجد روابط كافية بين التوجه الاستراتيجي على نطاق المنظومة والقدرات التشغيلية، الأمر الذي أثر على دينامية التفاعل بين هذه الهياكل ومن المرجح أن يكلف المنظومة غالياً من حيث مكاسب الكفاءة غير المحققة بسبب إضاعة فرص المزيد من التعاون المباشر.

تحديد مستوى أساسي من الحماية ما يلزم من متطلبات الدفاع الدنيا المتفق عليها

هناك قبول عام للفكرة القائلة بأن ضعف الحماية من التهديدات السيبرانية في إحدى المنظمات يزيد من تعرض المنظومة بأكملها للخطر. وعلى هذا، يمكن القول إن قوة منظومة الأمم المتحدة تقاس بقوة أضعف حلقاتها. غير أن المبادرات السابقة التي رمت إلى إدخال معايير مشتركة أو تقييمات للنضج تقارن بين المنظمات لم تلق دعماً كافياً، إذ يشير منتقدوها إلى تنوع البنى الهيكلية والسياقات التي تعمل فيها المنظمات كعقبة تحد من قيمة تلك النهُج الجماعية أو التراكمية. علاوة على ذلك، لم تبدِ المنظمات المشارِكة، على المستويات العليا، إلا ما قلّ من التقبُّل لتبادل معلومات الأمن السيبراني الداخلية الخاصة بها، وذلك لأسباب تتعلق بالسرية وبالتخوف من الكشف عن أوجه الضعف حتى بين المنظمات. ويمكن التخفيف من حدة هذه المخاوف باستخدام اتفاقات لتبادل المعلومات يمكن أن توفر ضمانات مناسبة. على أن محاولات إنشاء قدرة تشغيلية على مستوى المنظومة لمنع التهديدات السيبرانية واكتشافها والتصدي لها لم تسفر عن نتائج ملموسة حتى الآن. وقد سدّ مركز الأمم المتحدة الدولي للحوسبة بعض الثغرات في هذا الصدد، حيث اجتذبت حقيبة خدمات الأمن السيبراني التي

يقدمها قاعدة كبيرة من العملاء، وإن كان ذلك على أساس اختياري لا يفي بالتالي باحتياجات المنظومة إلا على نحو جزئي. وعلى الرغم من محدودية ما تحقق حتى الآن من نجاح في المساعي المبذولة على نطاق المنظومة نحو نهج مشترك أو منسق، سواء على المستوى المفاهيمي أو التشغيلي، يعتقد المفتشون أن تحديد مستوى أساسي من الحماية ومتطلبات دفاع دنيا لمنظمات الأمم المتحدة، وبالتالي للمنظومة ككل، يبقى هدفاً صالحاً لا يزال يستحق المتابعة.

الآليات المشتركة بين الوكالات بشأن الأمن السيبراني

تبين أن الآلية المشتركة بين الوكالات للتعامل مع الأمن السيبراني راسخة منذ زمن وأنها تعمل بشكل عام، مع أن بعض الأهداف الطموحة التي حددتها لنفسها لم تترجم بعد إلى نتائج ملموسة تتجاوز المستوى المتين لتبادل المعلومات ولما تم تمكينه بالفعل من تبادل مهني على نطاق المنظومة. وتقدم محاضر الشبكة الرقمية والتكنولوجية واللجنة الإدارية الرفيعة المستوى دليلاً على أن الأمن السيبراني، خلال فترة لا تقل عن 30 عاماً، اكتسى بعض الأهمية في جدول الأعمال على نطاق المنظومة. ومنذ عام 2011، كان الفريق المختص بأمن المعلومات الذي يعمل في إطار الشبكة الرقمية والتكنولوجية، هو الآلية الرئيسية لتعزيز التعاون بين الوكالات ولتحسين أمن المعلومات داخل المنظمات الأعضاء فيه. ووفقاً لاختصاصات الفريق، فإن الغرض الرئيسي منه يتمثل في تبادل المعرفة، على أن التركيز، بعد تنقيح تلك الاختصاصات في عام 2018، بات ينصب أيضاً على دور الفريق في تنفيذ المشاريع المشتركة – وهو تطلع أبرزته دعوة الشبكة الأم التي يتبعها الفريق لكي يزيد نشاطه في مجالات تصميم وتقديم الحلول والابتكارات المشتركة. ومع الاعتراف بالمصداقية المهنية والكم الهام من العمل الذي أنجزه الفريق على مر السنين، وجد المفتشون أن الحلول المشتركة الواسعة النطاق للمنظومة لم تتحقق على النحو المحدد في الولاية. وكهيئة تنسيقية، يواجه الفريق نفس التحديات التي تواجهها أية آلية أخرى مشتركة بين الوكالات تفتقر إلى سلطة اتخاذ القرار لفرض الإجراءات بصورة مباشرة على مستوى المنظومة، ولهذا السبب فإن من غير الواقعي أن ننتظر أن يتحقق التنفيذ ضمن هذا المنتدى. فتأثير الفريق محدود نوعاً ما بسبب اعتماده على المشاركة والمتابعة الفردية للمنظمات التي يجمع بينها، والتمكين غير المتكافئ لهذه المنظمات الأعضاء ضمن هيكلها المؤسسي، والواقع المتمثل في أن الفريق لا يتمتع بصفة تشغيلية تمكنه من تنفيذ الاتفاقات التي يتوصل إليها أو التوصيات التي يقدمها. بالإضافة إلى ذلك، يعتبر الفريق مسؤولاً أمام الشبكة الرقمية والتكنولوجية، وهو بالتالي يعكس البنية السائدة الملحوظة لدى معظم المنظمات حيث يتبع رئيس موظفي أمن المعلومات رئيس إدارة تكنولوجيا المعلومات والاتصالات في منظمته، مع ما يرافق ذلك من مزايا ومحدودية تنطوي عليها جميعاً تلك البنية.

مركز الأمم المتحدة الدولي للحوسبة كمقدم رئيسي لخدمات الأمن السيبراني للمنظومة

دأب مركز الأمم المتحدة الدولي للحوسبة على تقديم خدمات الأمن السيبراني لنحو ثلثي مؤسسات منظومة الأمم المتحدة خلال عدد من السنوات، مع أن قاعدة العملاء لكل خدمة من خدماته الثلاث عشرة ذات الصلة مختلفة إلى حد كبير. وقد شهد هذا المجال من قائمة خدمات المركز نمواً كبيراً ومتنوعاً، مع أنه لا يزال يمثل جزءاً بسيطاً فقط من أعمال المركز من حيث الميزانية. وقد ظهر أن تقييم خدمات الأمن السيبراني التي يقدمها المركز يتباين بين المنظمات المشارِكة، وهناك اعتراف بأن خدمة المعلومات الاستخبارية للتهديدات، التي يتيحها "الأمان المشترك" ("Common Secure")، هي الخدمة الرئيسية التي يقدمها. وكانت وحدة التفتيش المشتركة قد دعت فعلاً، في عام 2019، إلى تحسين الاستفادة من إمكانات المركز غير المفعّلة، وتحديداً فيما يتعلق بخدماته في مجال الأمن السيبراني.

وتُشجَّع مؤسسات منظومة الأمم المتحدة والمركز على إيجاد قدر أكبر من الأرضية المشتركة لتكميل القدرات الداخلية الحالية لدى المنظمات بمزيد من الخدمات المشتركة. وبهذه الروح، فإن الرؤساء التنفيذيين للمنظمات المشاركة مدعوون إلى إعادة النظر في الترتيبات المؤسسية الحالية والعودة إلى التفكير في الفرص المتاحة للاستفادة من خدمات المركز في مجال الأمن السيبراني. ونظراً لأن المركز يعمل كمرفق مشترك بين الوكالات بموجب قواعد منظمة الصحة العالمية وإطارها الإداري، فإن نموذج أعماله يستند إلى نموذج استرداد التكلفة والخدمة المشتركة. وقد ظهر أن هذا المزيج يشكل عامل تمكين، وهو في الوقت نفسه عقبة، أمام جعل المركز مجمعاً للأمن السيبراني للمنظومة ككل. فقد أوجد وضعاً يعتمد فيه ما يعرضه المركز من خدمات على العملاء الذين يقدمون تمويلاً أولياً لتغطية تكاليف تطوير أي خدمة جديدة حسب الطلب، في حين أن جهات كثيرة لا يمكنها إلا أن تشتري الخدمة المطورة على هذا النحو بعد بلوغ كتلة حرجة من العملاء الذين اشتركوا في تلك الخدمة بالفعل. وبالنظر إلى التحديات التي يفرضها الأمن السيبراني والمخاطر التي تواجهها المنظمات، فقد اعتُبر أن الوقت مناسب لاستكشاف استخدام التبرعات كآلية تمويل تكميلية لتوفير المزيد من الموارد المباشرة لحماية وضع المنظومة العام في مجال الأمن السيبراني. ويرى المفتشون أن من شأن إنشاء صندوق استئماني يستكمل آليات التمويل القائمة بتبرعات مخصصة لحلول الأمن السيبراني المشتركة التي تعود بالنفع على المنظومة ككل أن يغير قواعد اللعب فيما يتعلق بمعالجة بعض العقبات في هذا الصدد. فالصندوق الاستئماني يمكن الدول الأعضاء الراغبة في المساهمة بشكل مباشر في تعزيز الأمن السيبراني عبر المنظومة من القيام بذلك، ليس هذا فحسب، بل إنه سيوفر أيضاً فرصة، من خلال آلية للحوكمة للصندوق يستنبطها أصحاب المصلحة المعنيون، لتحسين الروابط بين التوجه الاستراتيجي الذي يمكن أن يوفره الفريق المختص بأمن المعلومات والقدرة التشغيلية التي يقدمها مركز الحوسبة (التوصية 3). والجمعية العامة مدعوة إلى الإحاطة علماً بالتوصية وإلى دعوة المانحين إلى تقديم التبرعات للصندوق الاستئماني (التوصية 4).

نحو مواءمة أوثق بين اعتبارات الأمن المادي والأمن السيبراني

من المعروف جيداً أن لدى إدارة شؤون السلامة والأمن ولاية على نطاق المنظومة لوضع السياسات وتوجيه الترتيبات التشغيلية في مجال السلامة المادية والأمن عبر الكيانات على مستوى العالم ككل. وعلى الرغم من الالتقاء بين الحيز المادي والفضاء السيبراني عندما يتعلق الأمر بحماية الموظفين وأصول المنظمات، فإن ولاية إدارة شؤون السلامة والأمن على النحو الذي حددته الجمعية العامة تركز على تهديدات محددة للسلامة والأمن تقع ضمن اختصاصها، وهي بالتالي لا تتضمن أي إشارة صريحة إلى الأمن السيبراني أو إلى البعد السيبراني للمخاطر والتهديدات. ومن الواضح أن الحاجة إلى تنسيق أوثق بين الأمن المادي والأمن السيبراني قد ألهمت المناقشة لسنوات في عدة هيئات مشتركة بين الوكالات، لكن هذه المناقشة لم تنضج بعد لتأتي باستنتاجات قابلة للتنفيذ بالنسبة للمنظومة. وللمساعدة في توضيح الفرص والمخاطر المرتبطة بتوسيع نطاق النهج السائد القائم على المخاطر ليشمل العالم السيبراني والاستجابة المنهجية المرتكزة على المساءلة التي تدعم نظام إدارة الأمن في الأمم المتحدة، يوصي المفتشون بأن يقدم الأمين العام تقريراً إلى الجمعية العامة يسلط الضوء على السبل التي تمكن من توفير حماية أكثر شمولاً لموظفي الأمم المتحدة وأصولها، ويشير إلى التدابير اللازمة لتعزيز الهياكل القائمة تبعاً لذلك، مع إيلاء اهتمام خاص لدور إدارة شؤون السلامة والأمن في هذا المضمار. وينبغي أن يسترشد التقرير بنتائج المشاورات بين آليات التنسيق المشتركة بين الوكالات ذات الصلة التي تتعامل مع الأمن السيبراني والشبكة المشتركة بين الوكالات لإدارة الأمن، مع مدخلات من مركز الأمم المتحدة الدولي للحوسبة حسب الاقتضاء (التوصية 5).

التوصيات

التوصية 1

ينبغي للرؤساء التنفيذيين لمؤسسات منظومة الأمم المتحدة أن يُعدّوا، على سبيل الأولوية وفي موعد لا يتجاوز عام 2022، تقريراً شاملاً عن إطار عملهم الخاص بالأمن السيبراني وأن يقدموه إلى هيئاتهم التشريعية والإدارية في أقرب فرصة، على أن يغطي العناصر التي تسهم في تحسين القدرة على الصمود في المجال السيبراني على النحو المطروح في هذا التقرير.

التوصية 2

ينبغي للهيئات التشريعية والإدارية في مؤسسات منظومة الأمم المتحدة أن تنظر في التقارير المتعلقة بالعناصر التي تسهم في تحسين القدرة على الصمود في المجال السيبراني والتي أعدها الرؤساء التنفيذيون، وأن تقدم توجيهات استراتيجية بشأن ما يتعين تنفيذه من تحسينات أخرى في منظماتهم، حسب اللزوم.

التوصية 3

ينبغي لمدير مركز الأمم المتحدة الدولي للحوسبة أن يعمل على إنشاء صندوقٍ استئماني لتبرعات المانحين، في موعد أقصاه نهاية عام 2022، من شأنه أن يكمل قدرة المركز على تصميم وتطوير وتقديم خدمات وحلول مشتركة لتعزيز وضع الأمن السيبراني في مؤسسات منظومة الأمم المتحدة.

التوصية 4

ينبغي للجمعية العامة للأمم المتحدة أن تحيط علماً، في موعد لا يتجاوز دورتها السابعة والسبعين، بالتوصية الموجهة إلى مدير مركز الأمم المتحدة الدولي للحوسبة بإنشاء صندوق استئماني لحلول الأمن السيبراني المشتركة، وأن تدعو الدول الأعضاء الراغبة في تعزيز وضع الأمن السيبراني لمؤسسات منظومة الأمم المتحدة إلى المساهمة في ذلك الصندوق الاستئماني.

التوصية 5

ينبغي للأمين العام أن يقدم تقريراً إلى الجمعية العامة للأمم المتحدة، في موعد لا يتجاوز دورتها الثامنة والسبعين، يستكشف المزيد من الفرص للاستفادة من التقارب بين الأمن المادي والأمن السيبراني لضمان توفير حماية أكثر شمولاً لموظفي الأمم المتحدة وأصولها، ويبين التدابير اللازمة لتعزيز الهياكل القائمة تبعاً لذلك، على أن يولي اهتماماً خاصاً لما يُمكن أن تضطلع به إدارة شؤون السلامة والأمن من دور في هذا المضمار.

وتُستكمل هذه التوصيات الرسمية بخمسٍ وثلاثين توصية غير رسمية أو مقترحة تظهر بالبنط العريض في متن هذا التقرير كاقتراحات إضافية يمكنها، في رأي المفتشين، أن تعزز وضع الأمن السيبراني لمنظومة الأمم المتحدة.

المحتويات

أولاً- مقدمة

ألف- السياق

1- **أهمية الأمن السيبراني في العصر الرقمي.** برز الأمن السيبراني في عالم اليوم الرقمي كمسألة ذات أهمية بالنسبة للمنظمات الدولية، ولا تُستثنى من ذلك مؤسسات منظومة الأمم المتحدة. وقد أدى التحول الرقمي، والاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات والحلول الممكّنة سيبرانياً، والواقع المتمثل في النمو المستمر في تهديدات الأمن السيبراني، من حيث درجة تعقيدها وما تنطوي عليه من إمكانات التعطيل، إلى زيادة غير مسبوقة في مخاطر الأمن السيبراني التي تواجه مؤسسات منظومة الأمم المتحدة. فالحوادث التي كانت تعتبر في يوم من الأيام استثنائية أصبحت أكثر تواتراً وشيوعاً. ويشير المفتشون إلى رسالة موجهة إلى الأمين العام في عام 2017، أعدها ممثلو لجان الرقابة في منظومة الأمم المتحدة بمناسبة أول اجتماع مشترك لهم على الإطلاق، إلى شواغل أساسية ثلاثة لدى مؤسسات المنظومة، أحدها الحاجة لأن تولي الإدارة الاعتبار الواجب للمخاطر الجديدة والناشئة، ولا سيما التهديدات العالمية والتهديدات الحرجة التي يتعرض لها الأمن السيبراني في مجال تسيير الأعمال، والمخاطر الناشئة عن طرق العمل الجديدة المواكبة لتسارع وتيرة التحول الرقمي[(1)]. وإزاء هذه الخلفية، أيدت المنظمات المشارِكة في وحدة التفتيش المشتركة قيام الوحدة بدراسة لسياسات الأمن السيبراني وممارساته المعمول بها في منظومة الأمم المتحدة، وقد أجرتها الوحدة كجزء من برنامج عملها لعام 2020، وهي الأحدث في سلسلة من الاستعراضات في موضوع التكنولوجيا تناولت موضوعات من قبيل الحوكمة الخاصة بتكنولوجيا المعلومات والاتصالات وإدارة مواقع الإنترنت واستخدام خدمات الحوسبة السحابية[(2)].

2- **منظومة الأمم المتحدة كهدف للهجمات السيبرانية.** لا يختلف مشهد تهديدات الأمن السيبراني الذي تواجهه مؤسسات منظومة الأمم المتحدة عن تلك التي تؤثر على الكيانات الأخرى، فمرتكبو الهجمات هم نفسهم، كما أن الوسائل المتبعة والأهداف المتوخاة – والتي تتراوح بين المالية والرمزية – مماثلة. ويمكن ملاحظة الفارق، إن وجد، في الطرق التي يمكن من خلالها اعتبار الأمم المتحدة هدفاً مفضلاً مقارنة بغيرها من كيانات القطاع العام والقطاع الخاص. أولاً، قد تكمن الجاذبية في بروز كيانات الأمم المتحدة ونطاقها العالمي، مما يجعلها هدفاً أكثر ظهوراً للقراصنة الحاسوبيين الباحثين عن الشهرة، مقارنة بما يمكن اكتسابه من دعاية من خلال مهاجمة حكومة وطنية وحيدة أو قطاع عام واحد. بالإضافة إلى ذلك، وعلى خلاف كثير من أهداف القطاع الخاص، فقد تكون كيانات منظومة الأمم المتحدة أكثر جاذبية أيضاً لدى "نشطاء القرصنة الحاسوبية" الذين يسترشدون بدوافع أيديولوجية ويحتجون ضد القيم التي تدافع عنها، أو تروج لها، مؤسسات المنظومة، أو يعارضونها. ونظراً للبيئة الحكومية الدولية التي تعمل فيها المنظمات، هناك أيضاً بُعد سياسي لا يمكن إنكاره، وتكتفي المنظمات نفسها بالتلميح إليه، مع أنها جميعاً، دون استثناء، تعترف به كأمر مسلم به. وباختصار، فإن الهجمات قد تختلف من حيث دوافعها في حين أن أساليبها تبقى متماثلة. ومن الواضح أن هناك زيادة هائلة في الهجمات، كبيرها وصغيرها، طرأت ضد المنظمات المشارِكة في وحدة التفتيش المشتركة على مدى السنوات الخمس الماضية، وهو ما يتضح من أرقام المصادر المختلفة التي رجع إليها المفتشون.

3- **تتجاوز حوادث الأمن السيبراني تعطيل المنظومة إذ أن تأثيرها يمكن أن يصل إلى تنفيذ الولايات.** بالنسبة لمؤسسات منظومة الأمم المتحدة، تتجاوز العواقب التي يمكن أن تنجم عن ضعف الأمن

(1) رسالة موجهة إلى الأمين العام، 26 كانون الثاني/يناير 2017.

(2) JIU/REP/2008/5؛ وJIU/REP/2008/6؛ وJIU/REP/2011/9؛ وJIU/REP/2019/5.

السيبراني تعطيل قدرات العمل الإداري والبنية التحتية لتكنولوجيا المعلومات والاتصالات وأنظمتها، وينبغي ألا تقاس فقط بحجم المعلومات والبيانات المتأثرة في نهاية الأمر. ويمكن لانتهاك واحد أن يكون مدمراً للمنظمة إذا أثر على بيانات حساسة من قبيل معلومات التعريف الشخصية، أو السجلات الطبية للموظفين، أو بيانات الملكية الفكرية، أو المحفوظات التاريخية والسياسية، أو ما شابه ذلك. وعلاوة على ذلك، فإن قدرة المنظمات على تنفيذ ولاياتها، فضلاً عن مصداقيتها أمام الدول الأعضاء والمستفيدين، هي على المحك. وفي المجال الذي تعمل فيه هذه المنظمات، يمكن حتى للحوادث البسيطة من الناحية التكنولوجية أن تحدث آثاراً متتابعة قد تتدخل في العمليات الدبلوماسية والحكومية الدولية، أو التدخلات الإنسانية، أو حتى في مجال السلم والأمن الدوليين في أسوأ الأحوال. وفي حين أن تأثير الهجمات السيبرانية على مؤسسات المنظومة ذات الولايات والهياكل المتنوعة قد يتباين، فإن التهديد حقيقيٌ ومشترك[3]. ولا يمكن لأي منظمة أن تتوقع ألا تتعرض أبداً لحادث أمن سيبراني، بغض النظر عن مستوى استعدادها ويقظتها. على أن الآثار المترتبة على السمعة والجوانب التشغيلية والقانونية والمالية يمكن أن تكون كبيرة في حال إهمال المخاطر.

4- **اعتراف المجتمع الدولي والأمم المتحدة بأهمية الأمن السيبراني.** توثق تقارير الهيئات التشريعية والإدارية وآليات التنسيق الداخلي ذات الصلة، منذ أوائل التسعينيات على الأقل، أن هناك فهماً لأن الأنشطة العدائية في الفضاء السيبراني تشكل تهديداً للمجتمع الدولي، وبشكل أكثر تحديداً لمنظمات الأمم المتحدة. وقد أخذ النقاش الموضوعي حول هذه المسألة مسارات متوازية. فهو، من ناحية، يُتابَع بين الحكومات في سياق عملها، كأعضاء في الهيئات التشريعية والإدارية للأمم المتحدة، على تطوير استجابة عالمية لنشوء الجريمة السيبرانية والتهديدات السيبرانية (مما يشكل البعد "المواجه للخارج" لعمل الأمم المتحدة في مجال الأمن السيبراني، والذي يقع اختصاص تنسيقه في المنظومة ككل على عاتق اللجنة الرفيعة المستوى المعنية بالبرامج التابعة لمجلس الرؤساء التنفيذيين في منظومة الأمم المتحدة المعني بالتنسيق)، في حين أنه، من ناحية أخرى، يُتابَع بين مؤسسات منظومة الأمم المتحدة في سعيها إلى تعزيز مستوى استعدادها الداخلي المؤسسي واستجابتها للتحديات ذات الصلة، سواء بشكل جماعي أو فردي (وهو ما يشكل البعد "المواجه للداخل"، الذي يخضع لاختصاص اللجنة الإدارية الرفيعة المستوى). ويدلل على الاعتراف بالدور المزدوج لمنظومة الأمم المتحدة في هذا الصدد بيانٌ ختامي أدلى به الأمين العام في سياق مجلس الرؤساء التنفيذيين مؤخراً في عام 2019، يشير إلى "ضرورة اضطلاع منظومة الأمم المتحدة بدور قيادي وتطوير موقف موحد بشأن الأمن السيبراني والتهديدات ذات الصلة، مع العمل في الوقت نفسه كمنصة تجمع الدول الأعضاء وأصحاب المصلحة الآخرين لمناقشة الأمن السيبراني بأبعاده المختلفة"[4].

5- **تشمل مسؤولية الدول عن حماية أصول الأمم المتحدة الأصول الرقمية في الفضاء السيبراني.** فيما يتعلق بالحماية القانونية الخاصة بالأمن السيبراني، تعتمد مؤسسات منظومة الأمم المتحدة على الامتيازات والحصانات التي تنطبق على ممتلكاتها وأصولها ومحفوظاتها ووثائقها واتصالاتها عموماً[5]. ويفرض وجود هذه الامتيازات والحصانات على الدول الأطراف التزاماً بأن تكون، بموجب قوانينها، في

(3) للاطلاع على معلومات أساسية عن التحديات التي تواجهها مؤسسات منظومة الأمم المتحدة، انظر كتيب الأمم المتحدة الرقمي "الخوذ الزرقاء" الذي أصدره مكتب الأمم المتحدة لتكنولوجيا المعلومات والاتصالات.

(4) CEB/2019/2، الفقرة 39.

(5) المادة 105 من ميثاق الأمم المتحدة؛ واتفاقية امتيازات وحصانات الأمم المتحدة المؤرخة 13 شباط/فبراير 1946؛ واتفاقية امتيازات الوكالات المتخصصة وحصاناتها المؤرخة 21 تشرين الثاني/نوفمبر 1947؛ واتفاق امتيازات وحصانات الوكالة الدولية للطاقة الذرية المؤرخ 17 آب/أغسطس 1959.

وضـــع يمكنها من توفير الحماية والأمن اللازمين لتحقيق أغراض الكيان الذي يتمتع بهذه الامتيازات والحصـانات، وعلى وجه الخصـوص، في وضـع يمكنها من ضـمان حرمة المباني والمحفوظات والوثائق "أينما كان مكانها وأياً كانت الجهة الحائزة لها". وبعبارة أخرى، يقع على عاتق الدول، ولا ســـيما البلدان المضيفة، واجب حماية المنظمات من الهجمات العدائية، سواء في المجال المادي أو في المجال الرقمي. وقد أكد مكتب الشـؤون القانونية هذا التفسـير للمفتشـين وهو تفسـير يحسـم مسـألة ما إذا كانت البيانات الإلكترونية والأصـــول الرقمية مشـــمولة بالأحكام القانونية القائمة. وفي الواقع، في أحدث اتفاقات المقر واتفاقات الدول المضيفة المبرمة ثنائياً بين المنظمات والدول التي تستضيفها على أراضيها، أوضح مكتب الشـؤون القانونية أن مصـطلح "المحفوظات" يُعرّف صـراحة على أنه يشـمل رسـائل البريد الإلكتروني والسجلات الحاسوبية، فضلاً عن أية مواد مماثلة تعود ملكيتها للمنظمة المعنية أو تحتفظ بها تلك المنظمة للتمكن من أداء وظيفتها. وبالمثل، تُعتبر الاتصـالات المحمية شـاملة لاتصـالات البيانات الإلكترونية، في حين أن الاتفاقات الأخرى تنص بصـورة أوسـع على حرمة أية وسـيلة من وسـائل الاتصـالات المسـتخدمة. وبالمعنى الأعم، يعني ذلك أن هناك مســؤولية تتحملها الدول بموجب القانون الدولي عن حماية أصـــول الأمم المتحدة، بما في ذلك في الفضاء السيبراني.

6- **التطور من تكنولوجيا المعلومات والاتصالات إلى منظور أوسع.** تقليدياً، ظهرت اعتبارات الأمن السـيبراني وجرى التعامل معها، لأول مرة، في مجال تكنولوجيا المعلومات والاتصـــالات، وهو مجال كان يحتل، في الأيام الأولى للحوسبة، دوراً أقل بروزاً في الأنشطة المؤسسية بالمقارنة بما هي عليه اليوم. وقد جاء هذا الفهم للأمن السـيبراني، الذي يركز على تكنولوجيا المعلومات والاتصـالات كتخصـص مسـتقل، كمنتج منطقي لزمن اقتصـرت فيه التهديدات في الغالب على البنية التحتية للحوسـبة وأثرت على مجموعة من أصول المعلومات والعمليات المؤسسية أضيق بكثير. أما الآن، وبعد أن أصبحت تكنولوجيا المعلومات والاتصـالات متأصـلة بعمق في معظم الأنشـطة المؤسـسية، وبعد أن تطور مشـهد التهديدات بشـكل كبير ليتجاوز مجرد التعرض لتعطلات تقنية تتطلب حلولاً أبسـط ودفاعات تسـتند إلى التكنولوجيا، فإنه لم يعد من العملي النظر إلى الأمن السـيبراني من خلال العدسـة التقييدية لتكنولوجيا المعلومات والاتصـــالات وحدها. **وفي الواقع، يرى المفتشـون أنه ينبغي تأطير الأمن السـيبراني من خلال منظور أوسـع بكثير يشمل عدداً من مجالات عمل المنظمة واختصاصاتها، بما في ذلك الإدارة المركزية للمخاطر، والسلامة والأمن الماديين، وحماية البيانات والخصوصية، والخبرة القانونية، وأمن المعلومات في السياق الأوسع لإدارة المعلومات والمعرفة.**

7- **تخطيط اسـتمرارية الأعمال كمفتاح للأخذ بنهج يقوم على المخاطر إزاء الأمن السـيبراني.** بدأت بعض المنظمات بالفعل في تبني مفهوم إدارة قدرة المنظمة على الصـمود الذي يشمل الأمن السيبراني كواحد من الجوانب الكثيرة. ويتمثل الشاغل المركزي لمجال قدرة المنظمة على الصمود في التقييم المناسب للمخاطر السـيبرانية بغية اعتماد تدابير وقائية تخفف من المخاطر والدفاع ضـــد التهديدات من ناحية، وإدخال بروتوكولات مناسـبة لتوجيه العمل والحفاظ على اسـتمرارية الأعمال في حال تحقق هذه المخاطر والتهديدات من ناحية أخرى. ولا يعتبر تخفيف المخاطر في مجال الأمن السـيبراني مطلقاً في أي وقت كان، فالمسـألة تتعلق بالدرجة، ويجب الحكم على فعاليته ليس فقط من خلال نجاحه في تجنب التهديدات، ولكن أيضـــاً من خلال مدى ما يقدمه من مساعدة على استعادة العمليات بعد هجوم ناجح. ولذا فإن من الضـروري عند وقوع حوادث خطيرة أن يكون هناك إجراءٌ للتعافي بعد الكوارث تم اختباره جيداً لجميع أنظمة المعلومات. ولا يمكن تحقيق ذلك إلا إذا أُخضـــعت بروتوكولات التعافي لاختبار منتظم صـــارم كجزء من التخطيط الروتيني لاســـتمرارية الأعمال. ومن الناحية المثالية، يُســـتخدم في هذا الصـــدد اختبار الاختراق كأداة قوية لإدارة المخاطر. وفي حين أن إجراءات التعافي من الكوارث لها بُعدٌ تقني قوي، إلا أنه ينبغي تطويرها ضـــمن المعايير الاســـتراتيجية التي تحددها قيادة المنظمة (بما في ذلك درجة تحمل المخاطر وتقبلها، والموارد

المتاحة، وما إلى ذلك) والقيود التشـــغيلية المعمول بها (مثل الوقت المقبول للتعافي) لكي تكوم مؤثرة بالفعل. وعلى هذا فإن تخطيط اســـتمرارية الأعمال، إلى جانب إدارة المخاطر، يصـــبح ركيزة لا غنى عنها لقدرة المنظمة على الصمود في مواجهة التهديدات المادية والتهديدات السيبرانية على حد سواء[6].

باء- الأهداف والنطاق والمنهجية

الأهداف

8- تتمثل الأهداف الرئيسية لإجراء هذا الاستعراض فيما يلي:

(أ) تحديد وتحليل التحديات والمخاطر المشـتركة في مجال الأمن السـيبراني التي تواجهها مؤسـسـات منظومة الأمم المتحدة واسـتجابة كل منها لها، مع مراعاة القواسـم المشـتركة والاختلافات ذات الصلة في متطلبات السياق المحدد لكل من المنظمات والقدرة على حماية أصولها الرئيسية مع الحفاظ في الوقت نفسه على قدرتها على تنفيذ ولاياتها؛

(ب) تحديد الترتيبات الحالية المشـتركة بين الوكالات ودراسـة ما إذا كانت فعالة في تيسـير الأخذ بنهج للمنظومة ككل إزاء الأمن السيبراني، فضـلاً عن تحديد فرص تحسين التنسيق والتعاون وتبادل المعلومات بين مؤسسات منظومة الأمم المتحدة، عند الاقتضاء.

النطاق

9- **التغطية على نطاق المنظومة ككل.** أُجري هذا الاســتعراض على نطاق المنظومة ككل وشــمل جميع المنظمات المشـارِكة في وحدة التفتيش المشـتركة، أي الأمانة العامة للأمم المتحدة، وإداراتها ومكاتبها، وصـــنـاديق الأمم المتحدة وبرامجها، وهيئـات وكيـانـات الأمم المتحدة الأخرى، ووكـالات الأمم المتحدة المتخصـصـة، والوكالة الدولية للطاقة الذرية. ولم يشـارك مركز التجارة الدولية في عملية الاسـتعراض وهو بالتالي غير مدرج في الأرقام الإجمالية التي يتضـــمنها هذا التقرير. بالإضـــافة إلى ذلك، درســـت الوحدة مركز الأمم المتحدة الدولي للحوسبة، نظراً لما له من دور في توفير خدمات الأمن السيبراني لعدة منظمات في منظومة الأمم المتحدة.

10- **التركيز على الترتيبات الداخلية للأمن السـيبراني.** يركز هذا التقرير على الترتيبات المؤسـسـية المتعلقة بإدارة أطر الأمن السيبراني ضمن مؤسسات منظومة الأمم المتحدة، وهي ترتيبات صممت لحماية أصـــولها في الفضـــاء الســـيبراني ولتمكين تنفيذ الأنشـــطة المنوطة بها (البعد "المواجه للداخل" للأمن الســـيبراني)[7]. ويرد في المرفق الأول عرض موجز للعمل الحكومي الدولي الذي تقوم به منظومة الأمم المتحدة لدعم الدول الأعضـــاء، بما في ذلك من خلال المســـاعدة التقنية لبناء القدرات الوطنية في مجال الأمن السـيبراني أو الاسـتجابة للجرائم السـيبرانية، وذلك توضـيحاً للسـياق ولكن دون جعله محوراً لهذا الاسـتعراض. ويتضـمن المرفق لمحة تاريخية مقتضـبة عن تطورات المسـألة في مختلف مسـارات عمل الجمعية العامة والهيئات الحكومية الدولية الأخرى.

11- **جوانب تقنية لم يجرِ تقييمها بالتفصـيل.** مع أن الأمن السـيبراني ليس مسـألة تقنية بحتة، فإنه لا يمكن معالجته دون الرجوع إلى البُعد الخاص بتكنولوجيا المعلومات والاتصالات فيه. على أن المفتشين

(6) يتضمن برنامج عمل وحدة التفتيش المشتركة لعام 2021 استعراضاً لاستمرارية الأعمال تحديداً.

(7) يُستكمل هذا التقرير برسالة إدارية موجهة إلى الرؤساء التنفيذيين للمنظمات المشاركة في وحدة التفتيش المشتركة تركز على المخاطر المرتبطة بصون وحماية الوثائق والبيانات القانونية والمعيارية والإدارية والسياسية والتاريخية للمنظمات (JIU/ML/2021/1).

لم يحاولوا إجراء تحليل متعمق للتدابير التي نفذتها المنظمات من حيث جدواها التكنولوجية أو سلامتها. ولأغراض دراستهم للاعتبارات التقنية التي ظهر أنها لا غنى عنها لإكمال هذا التقرير، استفاد المفتشون من الدراية الخارجية، واكتفوا بإبراز مجالات مختارة للنظر فيها ولما يمكن من مزيد من الدراسة لها. وعلى وجه الخصوص، لا يدعي المفتشون أنهم يقدمون في هذا التقرير تقييماً شاملاً، مقارناً أو غير مقارن، لنضج كلٍ من مؤسسات منظومة الأمم المتحدة. فقد اعتبروا أن تقييماً من ذلك القبيل يقع خارج نطاق هذا التقرير، كما أن فائدته محدودة بالنسبة للمنظمات المعنية، سواء جماعياً أو لكل منها بمفردها.

12- **مجالات ذات صلة تتمحور حول البيانات وتهمّ الأمن السيبراني ولكنها لا تدخل في نطاق التقييم.** تتقاطع مع الأمن السيبراني مجموعة متنوعة من مجالات إدارة المعرفة والمعلومات، فضلاً عن مجالات حماية البيانات، والخصوصية، والمجالات ذات الصلة، ولكنها تتجاوز نطاق هذه الدراسة. وقد كان بعض هذه المجالات بالفعل موضوعاً لتقارير أعدتها وحدة التفتيش المشتركة (من ذلك مثلاً تصنيف المعلومات كموضوع فرعي لإدارة السجلات والمحفوظات)[8]، في حين أن بعضها الآخر يُدرس حالياً على مستوى فرادى المنظمات استناداً إلى توجيهات خاصة بالمنظومة ككل (مثل ترجمة مبادئ حماية البيانات الشخصية والخصوصية التي اعتمدها مجلس الرؤساء التنفيذيين عام 2018 كسياسات وكإصدارات إدارية للمنظمات). بالإضافة إلى ذلك، فإن التحديات والتعقيدات المرتبطة باعتماد اللائحة الأوروبية العامة لحماية البيانات في نفس العام ومحاولات إنفاذها فيما يتعلق بمؤسسات منظومة الأمم المتحدة تطرح مجموعة منفصلة من الأسئلة تؤثر على الأمن السيبراني وتتجاوز نطاق هذه الدراسة. ولا تمثل هذه المسائل قائمة شاملة، ولكنها توضح النطاق الواسع للأمن السيبراني كمجال جامع لا يمكن التطرق إليه إلا بشكل سريع في هذا التقرير. **على أن المفتشين يودون أن يلاحظوا أن مجال حماية البيانات وخصوصية المعلومات الشخصية، على وجه الخصوص، يشكل مسألة ملحة اليوم تثير كثيراً من الشواغل، وأن الوقت مناسب ومبرر لإجراء استعراض نقدي مكرس لسياسات مؤسسات منظومة الأمم المتحدة وممارساتها في هذا الصدد.**

المنهجية

13- وفقاً لمعايير وحدة التفتيش المشتركة وإجراءات عملها الداخلية، استخدم المفتشون مجموعة من طرائق جمع البيانات النوعية والكمية من مصادر مختلفة لضمان اتساق نتائجهم وصحتها وموثوقيتها. والمعلومات المستخدمة في إعداد هذا التقرير حديثة حتى أيار/مايو 2021.

- **الاستبيانان والاستعراض المكتبي.** جمعت وحدة التفتيش المشتركة المعلومات من خلال استبيانين وجهتهما إلى المنظمات المشارِكة. وقد فحص المفتشون المكونات ذات الصلة من الأطر التنظيمية المعمول بها (قرارات الهيئات الإدارية، والاستراتيجيات المؤسسية بشأن تكنولوجيا المعلومات والاتصالات، والسياسات المحددة ووثائق التوجيهات الإجرائية بشأن أمن المعلومات والأمن السيبراني حيثما وجدت)، ورجعوا إلى تقارير هيئات الرقابة الداخلية والخارجية. وتمكن المفتشون، من خلال عدة جولات من الاستفسارات الموجهة إلى مركز الأمم المتحدة الدولي للحوسبة، من إجراء استعراض نقدي لولايته وقائمة خدماته وقدراته المؤسسية والتشغيلية في مجال الأمن السيبراني. وقدم مكتب الشؤون القانونية توضيحاً خطياً بشأن سلسلة من الجوانب القانونية. وساعد تحليل تقارير لجان وشبكات مجلس الرؤساء التنفيذيين، ولا سيما الشبكة الرقمية والتكنولوجية وفريقها المختص بأمن المعلومات، على توفير مزيد من المعلومات حول

(8) JIU/REP/2013/2.

الديناميات المشـتركة بين الوكالات والمبادرات الحالية والسـابقة على نطاق المنظومة. كما رجع المفتشـون إلى معايير الصـناعة ذات الصـلة والكتابات المتعلقة بالأمن السيبراني باعتبارها وثائق معلومات أساسية.

- **المقابلات**. اسـتناداً إلى الردود على الاسـتبيانين، أجرى المفتشـون 45 مقابلة مع المسـؤولين عن تكنولوجيا المعلومات والاتصـالات، وبشـكل أكثر تحديداً عن الأمن السـيبراني، وكذلك مع كبار المسـؤولين لتقديم منظور أوسـع عن المنظمات. وأجريت مقابلات لاحقة مع ممثلي هيئات الرقابة، وإدارة شـؤون السـلامة والأمن، فضـلاً عن منظمات مختارة غير مشاركة. وقدمت المقابلات التي أجريت مع رئيس الفريق المختص بأمن المعلومات وممثلي أمانة مجلس الرؤسـاء التنفيذيين مزيداً من التبصـر في المبادرات المشـتركة بين الوكالات بشـأن الأمن السـيبراني. وأجريت مقابلات مع ممثلي مركز الأمم المتحدة الدولي للحوسـبة أتاحت تفاصـيل عن القدرات التي يقدمها المركز في مجال الأمن السيبراني. كما حضـر المفتشون مؤتمر الأمان المشـترك لعام 2020، الذي اسـتضـافه مركز الحوسـبة وعُقد افتراضـياً بسـبب جائحة فيروس كورونا الحالية (كوفيد-19)، للحصـول على انطباع عن التطورات والتحديات الحالية التي ناقشـها المشـتركون في خدمة الأمان المشـترك التي يوفرها المركز. بالإضـافة إلى ذلك، من خلال مجموعة للتركيز، استفاد المفتشون من آراء وخبرات عدد من رؤساء موظفي أمن المعلومات المشـاركين كأعضـاء في شـبكة عالمية غير رسـمية لحكومات المدن التي تواجه تحديات مماثلة، وتعرفوا من خلال ذلك على سـياسـات حكومات تلك المدن وممارسـاتها والدروس المسـتفادة منها، وذلك كمرجع عن أعمال القطاع العام يمكن لكيانات الأمم المتحدة أن تستفيد منه.

14- **القيود من حيث توافر المعلومات وسريتها**. واجه المفتشـون قيوداً تتعلق في المقام الأول بما يلي: (أ) توافر المعلومات (نظراً لأن قياسات حوادث الأمن السيبراني لم تُسجل بشكل منهجي أو لم تأخذ، في حال تسـجيلها، بمنهجية متفق عليها عموماً، مما حدّ أيضـاً من إمكانية مقارنة البيانات)؛ و(ب) سـرية البيانات المتعلقة بالتهديدات والحوادث، ولا سـيما بتدابير الاسـتجابة، حيث رأت المنظمات أن تقديم هذه المعلومات يؤدى إلى تعرض لا ضـرورة له لأنها تحدد أوجه الضـعف في بنيتها التحتية الأمنية وتكشـفها، ولهذا السبب، عُرضت المعلومات في المقام الأول بشكل إجمالي في المتن السردي للتقرير، دون إسنادها إلى كيانات محددة ما لم يكن لذلك ما يبرره على أسـاس كل حالة على حدة؛ و(ج) أثر جائحة كوفيد-19 على عملية جمع البيانات، مما أدى إلى تأخيرات واسـتلزم إجراء المقابلات من خلال التداول بالفيديو حصـرياً، مما يُحتمل أن يكون قد أثر على الوصـول إلى بعض المحاورين، وكذلك على رغبتهم في تقديم معلومات حسـاسـة كان من الممكن تقديمها من خلال تفاعلات شـخصـية. بالإضـافة إلى ذلك، ومع أن المفتشـين سـعوا إلى دراسـة وعرض سـبل تأثير اسـتجابات المنظمات المشـارِكة للجائحة على الاعتبارات الخاصـة بالأمن السيبراني، فإن بعض الترتيبات والتدابير المنفذة في هذا السياق يمكن أن تكون قد شهدت مزيداً من التطورات، ولذا فإنها ربما لم تؤخذ في الاعتبار بشكل كامل أثناء عملية الاستعراض.

15- **شكر وتقدير**. يود المفتشون أن يعربوا عن تقديرهم لجميع المسؤولين في مؤسسات منظومة الأمم المتحدة وممثلي المنظمات الأخرى الذين سـاعدوا في إعداد هذا التقرير، ولا سـيما أولئك الذين شـاركوا في المقابلات وقدموا معارفهم وخبراتهم بكل طيب خاطر. وقد اسـتُخدمت، لأغراض ضـمان الجودة، طريقة اسـتعراض الأقران الداخلي لالتماس التعليقات من مفتشـي وحدة التفتيش المشـتركة على مشـروع التقرير،

الذي عُمم لاحقاً على المنظمات المعنية لإبداء تعليقات موضوعية على النتائج والاستنتاجات والتوصيات، وكذلك لتصحيح أية أخطاء في الوقائع.

16- **التوصيات.** يتضمن هذا التقرير خمس توصيات رسمية، واحدة منها موجهة إلى الجمعية العامة، وواحدة إلى الهيئات التشريعية والإدارية، وواحدة إلى الرؤساء التنفيذيين للمنظمات المشاركة في وحدة التفتيش المشتركة، وواحدة إلى الأمين العام، وواحدة إلى مدير مركز الأمم المتحدة الدولي للحوسبة. وتيسيراً للتعامل مع هذا التقرير وتنفيذ توصياته ورصدها، يحتوي المرفق العاشر على جدول يوضح ما إذا كان التقرير مقدم إلى المنظمات ذات الصلة لاتخاذ إجراء أو للعلم ويحدد ما إذا كانت التوصيات تتطلب اتخاذ إجراء من قبل الهيئات التشريعية والإدارية أو من جانب الرؤساء التنفيذيين. وتُستكمل التوصيات الرسمية بـ 35 توصية غير رسمية مبينة بالبنط العريض في النص، باعتبارها اقتراحات إضافية يمكنها، في رأي المفتشين، أن تعزز وضع الأمن السيبراني لمنظومة الأمم المتحدة.

جيم- التعاريف

17- **عدم وجود تعريف مقبول عالمياً للأمن السيبراني.** غالباً ما تتضمن معايير الصناعة الدولية والوطنية الخاصة بأمن المعلومات تعريفاً للأمن السيبراني. على أنه لا يوجد تعريف مقبول عالمياً أو إجماع عالمي حول ما يشمله المصطلح بدقة. وفي سياق الأمم المتحدة، لاحظ المفتشون أنه لا توجد أية توجيهات على نطاق المنظومة من المنتديات المشتركة بين الوكالات ذات الصلة توصي بالإجماع بتعريف معين باعتباره موثوقاً للمنظومة[9]، كما أن الأطر التنظيمية لدى المنظمات لا تحاول بشكل منهجي فرض تعريف للأمن السيبراني. ولأغراض هذا التقرير، قرر المفتشون استخدام تعريف الأمن السيبراني الذي وضعه الاتحاد الدولي للاتصالات، والذي يرد في الإطار 1. وقد أكدت الغالبية العظمى من المنظمات المشارِكة في وحدة التفتيش المشتركة أن التعريف يعكس نهجاً إزاء هذا الموضوع، مع استكماله في كثير من الأحيان باستخدام المنظمات لمعايير الصناعة ذات الصلة كمرجع.

الإطار 1

الأمن السيبراني وفقاً لتعريفه لدى الاتحاد الدولي للاتصالات

"الأمن السيبراني هو مجموعة من الأدوات، والسياسات، والمفاهيم الأمنية، والضمانات الأمنية، والمبادئ التوجيهية، ونُهُج إدارة المخاطر، والإجراءات، والتدريب، وأفضل الممارسات، والضمان، والتقنيات، التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدِمين. وتشمل أصول المنظمة والمستخدِمين أجهزة الحوسبة المترابطة، والموظفين، والبنية التحتية، والتطبيقات، والخدمات، وأنظمة الاتصالات، ومجموع المعلومات المنقولة و/أو المخزونة في البيئة السيبرانية. ويسعى الأمن السيبراني لضمان تحقيق وحفظ الخصائص الأمنية لأصول المنظمة والمستخدِمين ضد المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتتألف الأهداف الأمنية العامة مما يلي: التوافر؛ والسلامة، والتي يمكن أن تشمل المصداقية وعدم التنصل؛ والسرية. "

توصية الاتحاد الدولي للاتصالات ITU-T X.1205، نظرة عامة على الأمن السيبراني.

(9) تضمّن الإطار الشامل للأمم المتحدة بشأن الأمن السيبراني والجريمة السيبرانية (انظر CEB/2013/2) وخطة التنسيق الداخلي لمنظومة الأمم المتحدة بشأن الأمن السيبراني والجريمة السيبرانية (2014، المرفق)، تعاريفَ للتوصل إلى فهم مشترك لمصطلحات الجريمة السيبرانية والأمن السيبراني، مع التنبيه إلى أن تلك التعاريف تبقى مجرد تعاريف عملية وظيفية ولم تقرّها منظومة الأمم المتحدة بهذه الصفة.

18- **أمن المعلومات في مقابل الأمن السيبراني.** تستخدم العديد من المنظمات مصطلح "أمن المعلومات"، الذي يهتم بأمن المعلومات بجميع أشكالها وحيثما يتم تخزينها، وليس فقط البيانات الإلكترونية في المجال الرقمي. وعلى خلاف ذلك، يمكن للأمن السيبراني أن يكون أكثر ارتباطاً بالمعلومات الرقمية الخالصة وبحماية مجموعة أوسع من الأصول المتصلة أو المتأثرة بالفضاء السيبراني، على النحو الموضح في تعريف الاتحاد الدولي للاتصالات. وعلى الرغم من التباين المفاهيمي الطفيف بين المصطلحين، إلا أنهما يتداخلان إلى حد كبير، لا سيما فيما يتعلق بالأهداف الأساسية لحماية توافر المعلومات وسلامتها وسريتها (مما يُعرف أيضاً باسم "ثالوث أمن المعلومات"، على النحو المبين في الشكل الأول). وتستخدم بعض المنظمات مصطلح "الأمن السيبراني" بشكل تبادلي كلياً مع مصطلح "أمن المعلومات". ويعتبر البعض الآخر أن "الأمن السيبراني" قد حل محل مصطلح "أمن المعلومات" الأكثر تقليدية، مع أنه تنازل عن بعض دلالاته المتعلقة بالإدارة الأوسع للمعرفة والمعلومات ليأخذ بدلاً عنها مزيداً من الخصائص التي تركز على تكنولوجيا المعلومات والاتصالات. على أن آخرين أيضاً يستخدمون "الأمن السيبراني" كمصطلح شامل يشمل كلاً من "أمن المعلومات" والمصطلح الأضيق (والأكثر استخداماً) "أمن تكنولوجيا المعلومات والاتصالات"، والذي يشير تحديداً إلى أمن البنية التحتية لتكنولوجيا المعلومات والاتصالات (مثل الأجهزة والبرمجيات والشبكات والعمليات التقنية).

الشكل الأول

نموذج ثالوث أمن المعلومات[10]

المصدر: المعهد الوطني الأمريكي للمعايير والتكنولوجيا.

19- ولوحظ وجود غموض مشابه في تسميات الوظائف القيادية التي يُدرج الأمن السيبراني تحتها عادة في السياق التنظيمي. فعلى سبيل المثال، قد يكون "رئيس موظفي أمن المعلومات" مسؤولاً أمام "رئيس موظفي تكنولوجيا المعلومات" أو "رئيس موظفي المعلومات"، حيث تُستخدم التسميتان الأخيرتان كمترادفتين تشيران إلى رئيس إدارة تكنولوجيا المعلومات والاتصالات، أو تُستخدم تسمية "رئيس موظفي المعلومات" لتشمل أيضاً إدارة المعرفة والسجلات أو وظائف الاتصالات والعلاقات العامة. ولم يتمكن

(10) وفقاً لما حدده مركز أمن الإنترنت، فإن ثالوث السرية والسلامة والتوافر هو نموذج لقياس أمن المعلومات مصمم للتحكم في سبل تعامل المنظمة مع البيانات عند تخزينها أو إرسالها أو معالجتها، ولتقييم هذه السبل. وتمثل كل صفة من الصفات الثلاث مكوناً مهماً لأمن المعلومات، على النحو التالي. السرية تعني أنه لا ينبغي الوصول إلى البيانات أو قراءتها دون إذن. وهي تضمن ألا تتمكن من الوصول إليها إلا الأطراف المأذون لها بذلك. وتُعتبر الهجمات ضد السرية هجمات لإفشاء المعلومات. أما السلامة فهي تعني أنه لا ينبغي تعديل البيانات أو المساس بها بأي حال من الأحوال. ويُفترض بقاء البيانات على حالتها المقصودة ولا يمكن تعديلها إلا من قبل الأطراف المأذون لها بذلك. وتُعتبر الهجمات على السلامة هجمات لتحريف المعلومات. وأما التوافر فهو يعني أن البيانات يجب أن تكون متاحة عند الطلب المشروع. ويضمن ذلك تمكن الأطراف المأذون لها بذلك من الوصول دون عائق إلى البيانات عند الحاجة. وتُعتبر الهجمات ضد التوافر هجمات لتدمير المعلومات.

المفتشون من تمييز نمط ثابت من شأنه أن يفيد بوجود قصد أو صرامة على المستوى المفاهيمي لتحديد الفوارق في نطاق الوظائف المرتبطة بكل مصطلح.

20- ويستخدم المفتشون في هذا التقرير كله مصطلح "الأمن السيبراني" على النحو المحدد أعلاه. وعندما يرد مصطلح "أمن المعلومات"، فإن استخدامه يتم عن عمد توخياً للدقة عند عرض اقتباسات مباشرة مأخوذة من وثائق مرجعية أو ضماناً لصحة استخدام مصطلحات تقنية من قبيل "رئيس موظفي أمن المعلومات" أو "نظام إدارة أمن المعلومات". فالمفتشون لم يجدوا أن هناك حاجة إلى تنقيح تلك الاقتباسات أو المصطلحات الفنية أو مواءمة استخدامها، لأنها لا تمثل عائقاً أمام نقل المعلومات ذات الصلة أو تبادلها عبر المنظمات.

ثانياً- لمحة سريعة عن الأمن السيبراني في منظومة الأمم المتحدة

ألف- اهتمام متزايد بالأمن السيبراني، بيد أن مستويات النضج مختلفة عبر المنظومة

21- **تزايُد إدراك أن الأمن السيبراني يتطلب الاهتمام.** شهدت السنوات الأخيرة فهماً متزايداً لكون الأمن السيبراني يتطلب الاهتمام، وإن كان هذا الفهم متفاوتاً بين مؤسسات منظومة الأمم المتحدة. ولا جدال في انكشاف مؤسسات منظومة الأمم المتحدة وجاذبيتها كهدف للمهاجمين السيبرانيين، مع أن درجة ذلك يمكن أن تختلف رهناً بولاياتها أو مستوى بروزها. ويمكن القول إن الولاية أو نموذج العمل، بالإضافة إلى المعلومات التي تملكها أو تديرها المنظمات، أثرت على سرعة اعترافها بالأمن السيبراني كمسألة ذات أهمية. ويبدو أن المنظمات التي تتعامل مع البيانات الحساسة سياسياً ذات الآثار المترتبة على الأمن الدولي أو المصالح الوطنية أو الاقتصادية، وكذلك تلك التي تدير كميات كبيرة من البيانات الحساسة قانونياً، بما في ذلك البيانات الشخصية للفئات السكانية المستفيدة المعرضة للخطر أساساً، شرعت قبل غيرها في مسيرة الارتقاء بتأهب الأمن السيبراني لديها، في حين أن المنظمات التي لديها ولايات غير مثيرة للجدل نسبياً كانت سرعتها أكثر اعتدالاً في لحاقها ببناء الدفاعات السيبرانية. بالإضافة إلى ذلك، كان على بعض المنظمات التي أصبحت في بؤرة اهتمام الجمهور نظراً للأهمية الآنية لولاياتها، أن تكثف جهودها بشكل كبير في غضون مهلة قصيرة (مثل منظمة الصحة العالمية)، وهو ما فعلته المنظمات الكبيرة التي أدى تعرضها لهجمات سيبرانية واسعة النطاق أو بارزة للغاية إلى تسريع الحاجة إلى اتخاذ إجراءات فورية وتعزيز قدرتها على الصمود في المجال السيبراني (كما في حال منظمة الطيران المدني الدولي). على أنه إجمالاً، لا توجد منظمة مشاركة في وحدة التفتيش المشتركة لم تدرك، بشكل ما، أهمية إبقاء أمنها السيبراني في وضع قوي يتناسب مع متطلباتها التشغيلية.

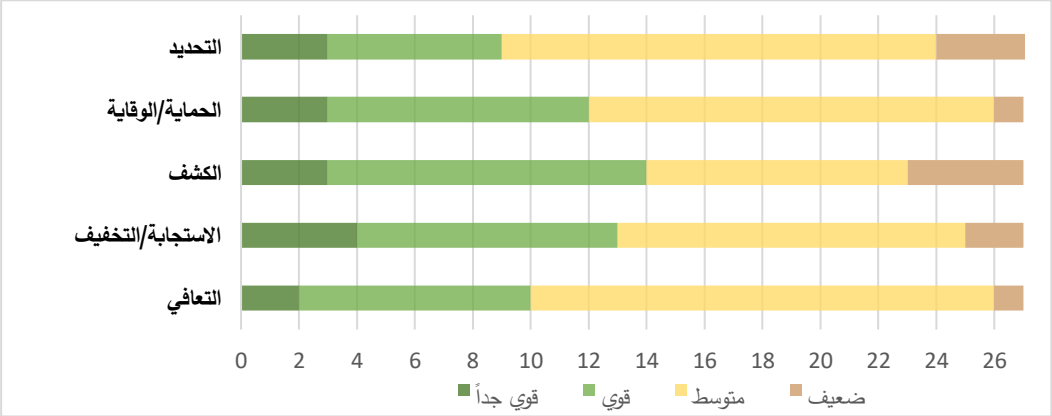
22- **اختلاف مستويات النضج بين منظمات الأمم المتحدة.** بينما لم يجد المفتشون أية منظمة من المنظمات المشارِكة في وحدة التفتيش المشتركة غافلة عن ضرورة الاستثمار في أمنها السيبراني، فقد لوحظت اختلافات كبيرة في الأساليب التي لجأت إليها المنظمات المختلفة في استجابتها للتهديدات السيبرانية. وحتى مع عدم وجود معايير مشتركة أو معايير مستخدمة بشكل موحد يمكن أن تيسر إجراء مقارنة موثوقة منهجياً قائمة على الأدلة، فقد ظهر أن مستوى نضج أطر الأمن السيبراني بين مؤسسات منظومة الأمم المتحدة متباين إلى حد كبير. ويمكن تفسير هذا التباين بالرجوع إلى بيئة عمل كل منظمة؛ والمتطلبات التي يمليها نوع البيانات المحفوظة؛ ومستوى فهم القيادة للأمن السيبراني وما تمنحه له من أولوية؛ وتوافر الموارد؛ والتفاوت في أنظمة تكنولوجيا المعلومات والأدوات والحلول البرمجية المستخدمة، والتي غالباً ما تعكس سنوات من عدم تنسيق قرارات الاستثمار وكذلك خيارات الباعة عبر المنظومة. وعلى الرغم من القواسم المشتركة الهيكلية وغيرها مما لا شك في وجوده في معظم المنظمات التي نظرت فيها وحدة التفتيش المشتركة، إن لم يكن جميعها، فإن محاولات تقديم تقييم حاسم لنضج الأمن السيبراني عموماً في منظومة الأمم المتحدة ككل لم تكن لتنصف التنوع الذي يميز أعضائها. وعلاوة على ذلك، فقد اعتُبر أن القيمة العملية لمثل ذلك التقييم ستكون محدودة، لأن المقارنات مع المنظمات الأخرى أو تحديد "متوسط" النضج على نطاق المنظومة لن يقدم ما يُذكر من المعلومات حول حماية فرادى المنظمات.

23- **توحي الردود التي تم جمعها بوجود مجال للتحسين.** في محاولة لتقديم صورة سريعة تقريبية للوضع الراهن، يوضح الشكل الثاني كيف قيَّمت المنظمات المشارِكة ذاتياً إطار الأمن السيبراني الشامل لديها استناداً إلى فئات عريضة من المجالات الوظيفية التي حددها استبيان وحدة التفتيش المشتركة. ومع ملاحظة التحديات الواضحة في تفسير الاستجابات المتلقاة في غياب إطار مرجعي مشترك أو معيار للمقارنة، فإن الصورة العامة مع ذلك لا توحي بوجود موقف أمن سيبراني واثق عبر المنظومة ككل، حتى

بالمعايير الذاتية. وقد قدم مركز الأمم المتحدة الدولي للحوسبة، في تقييمه الخاص للأداء العام لمؤسسات منظومة الأمم المتحدة في سياق الرد على نفس السؤال، وبقدر ما كان في وضع يسمح له بتقديم نظرة متعمقة حول عملائه، درجات تتراوح من "المتوسط" إلى "الضعيف"، مما يؤكد أيضاً أن هناك مجالاً للتحسين على مستوى المنظومة بأكمله.

الشكل الثاني

التقييم الذاتي للأداء في مجالات عريضة من الأمن السيبراني، حسب نوع الضوابط وعدد المنظمات المشارِكة في وحدة التفتيش المشتركة



المصدر: استبيان وحدة التفتيش المشتركة 2020.

ملاحظة: مفهوم فئات التقييم الذاتي مستوحى من الفئات المستخدمة في الأطر والمعايير المرجعية المعترف بها في مجال الأمن السيبراني. وتقسّم مجالات الأمن السيبراني المشار إليها في استبيان وحدة التفتيش المشتركة على النحو التالي: التحديد (العمليات الحرجة، والأصول، والموارد، والمخاطر، وما إلى ذلك)؛ والحماية/الوقاية (إدارة الوصول، والوعي، والتدريب، والإجراءات، والتكنولوجيا، وما إلى ذلك)؛ والكشف (الحالات الشاذة والأحداث، والرصد المستمر، وعملية الكشف، وما إلى ذلك)؛ والاستجابة/التخفيف (التخطيط، والاتصالات، والتحليل، والتخفيف، وما إلى ذلك)؛ والتعافي (التخطيط، والاستعادة، والاتصالات، والتحسينات، وما إلى ذلك).

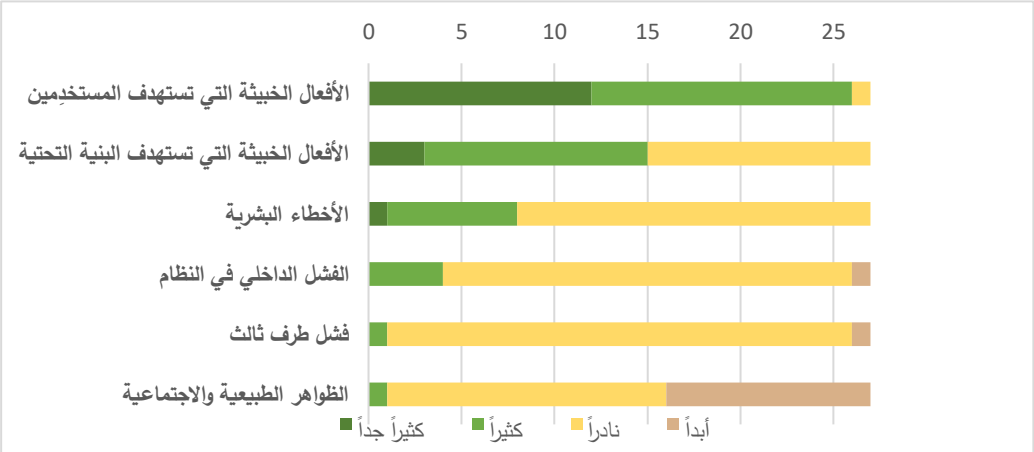
24- **المخاطر على نطاق المنظومة تتزايد بفعل ضعف وضع فرادى المنظمات.** تتجاوز مسألة المستوى المناسب من الاستعداد للأمن السيبراني تعرُّض كل منظمة على حدة. وخلال المقابلات، أكد خبراء الأمن السيبراني الرأي القائل بأن هشاشة أو ضعف دفاعات أي منظمة تمثل خطراً على الكيانات الأخرى في المنظومة. إذ أن من الممكن للمهاجم، بعد أن يستولي على الامتيازات الإدارية ويحصل على وصول أعمق إلى أنظمة معلومات إحدى المنظمات، أن يستغل هذا الوصول لاختراق المجال الرقمي لكيان آخر. كما قد يصعب اكتشاف الحركة الجانبية الخبيثة من منظمة إلى أخرى (المعروفة باسم التحرك جانبياً "pivoting") ومكافحتها، لأنها يمكن أن تظهر كحركة معتادة. واستناداً إلى المعلومات التي يجمعها القراصنة الحاسوبيون في سياق البنية التحتية لمنظمة واحدة، يمكنهم أن يكيفوا طريقة الهجوم وأن يستخدموا مجموعة من التقنيات والأدوات مهيأة بصورة أفضل لتحقيق هدفهم. وعلى هذا، فإن المنظمات التي يخلص تقييمها الذاتي الفردي إلى أن أمنها السيبراني "ضعيف" تمثل مشكلة جماعية. ومن ثم يمكن القول إن قوة منظومة الأمم المتحدة تقاس بقوة أضعف حلقاتها. ويجري استكشاف هذا البعد بمزيد من التفصيل في الفصل الرابع من هذا التقرير.

باء- مشهد تهديدات الأمن السيبراني

25- **مصادر التهديد ووسائل الهجوم الأكثر شيوعاً.** يقدم الشكل الثالث لمحة عامة عن التعرض الحالي لتهديدات الأمن السيبراني، ويعكس الردود التي قدمتها المنظمات المشارِكة في وحدة التفتيش المشتركة بشأن تواتر الحوادث التي أثرت عليها في السنوات الخمس الماضية، مصنفة حسب مصدر التهديد. وقد كانت الإجراءات الخبيثة التي تستهدف مستخدمي أنظمة المعلومات (من خلال التصيد الاحتيالي، أو سرقة الهوية، أو مخططات "الرجل الوسيط"، وما إلى ذلك) أو تستهدف البنية التحتية (البرامج الضارة، وهجمات حجب الخدمة الموزع، وما إلى ذلك) هي أكثر أنواع التهديدات المبلغ عنها شيوعاً إلى حد كبير. وقد أكد المسؤولون الذين تمت مقابلتهم أن الأفعال الخبيثة التي تستهدف المستخدِمين النهائيين كانت أكثر أنواع الهجمات شيوعاً والأسرع نمواً في الماضي القريب. وتعزز ذلك بسبب وضع الجائحة، الذي أجبر كثيراً من المستخدِمين النهائيين على العمل من مواقع بعيدة، غالباً باستخدام أجهزتهم الخاصة التي تفرض، في كثير من الحالات وبدرجات متفاوتة، ضغوطاً إضافية على تدابير حماية الأمن السيبراني المؤسسي (الفقرات 39-41).

الشكل الثالث

التعرض لتهديدات الأمن السيبراني في السنوات الخمس الماضية، حسب فئة مصدر التهديد وعدد المنظمات المشارِكة في وحدة التفتيش المشتركة



المصدر: استبيان وحدة التفتيش المشتركة 2020.

ملاحظة: توصف مصادر التهديد بمزيد من التفصيل على النحو التالي: الأفعال الخبيثة التي تستهدف المستخدِمين (التصيد الاحتيالي، وسرقة الهوية، ومخططات "الرجل الوسيط"، وما إلى ذلك)؛ والأفعال الخبيثة التي تستهدف البنية التحتية (البرمجيات الخبيثة، وهجمات حجب الخدمة الموزع، والإجراءات الفنية الأخرى، وما إلى ذلك)؛ الأخطاء البشرية (الخطأ في التكوين، والخطأ التشغيلي، وعدم الامتثال للإجراءات، وفقدان المعدات، وما إلى ذلك)؛ والفشل الداخلي في النظام (عطل في الجهاز أو النظام أو فشل في المعدات، وانقطاع التيار الكهربائي، وفشل وصلة الاتصال، وما إلى ذلك)؛ وفشل طرف ثالث (مزودو خدمات الإنترنت، وشبكة الكهرباء، وإدارة الأجهزة عن بُعد، وما إلى ذلك)؛ والظواهر الطبيعية والاجتماعية (الفيضانات، والزلزال، والقصف، والاضطرابات المدنية، والحرائق، وما إلى ذلك).

26- **زيادة هجمات الهندسة الاجتماعية، ولا سيما أثناء جائحة كوفيد-19.** في حين أن تهديدات الأمن السيبراني ترتبط عموماً بالعمليات التقنية المعقدة التي تستهدف البنية التحتية، أبلغ مجتمع الأمن السيبراني في الأمم المتحدة عن تحول ملحوظ من اختراق الخوادم والشبكات وأجهزة الاستخدام النهائي إلى اختراق الأشخاص، وذلك باستخدام طرائق الهندسة الاجتماعية التي تهدف إلى التلاعب بالأشخاص

لإفشاء المعلومات الحساسة لأغراض احتيالية. وأدت جائحة كوفيد-19 إلى تفاقم المخاطر المتعلقة بالهندسة الاجتماعية. وقد أبلغ أكثر من ثلثي المنظمات المشارِكة عن زيادة حادة في تهديدات الأمن السيبراني وفي أوجه الضعف خلال عمليات الإغلاق العالمية التي فصلت بشكل فعال العديد من المستخدِمين عن موارد الأمن السيبراني المدارة مركزياً، مما أضعف الصفة المباشرة للاتصال بالمهنيين المدربين للحصول على المشورة بشأن رسائل البريد الالكتروني والمواقع الشبكية المشبوهة، وذلك بسبب الانتقال المفاجئ إلى العمل عن بعد. ووفقاً لمركز الأمم المتحدة الدولي للحوسبة، استفاد مجرمو الفضاء السيبراني والخصوم من الارتباك وزيادة الاهتمام بالمحتوى المرتبط بالجائحة عن طريق إرسال رسائل بريد إلكتروني في موضوع كوفيد-19 بقصد التصيد الاحتيالي، وإنشاء مواقع شبكية مزيفة محملة ببرمجيات خبيثة يزُعم أنها توفر معلومات عن المرض. وكانت هجمات التصيد الاحتيالي ناجحة بشكل خاص خلال هذه الفترة، والتي تميزت أيضاً بنشر مستويات غير مسبوقة من المعلومات المضللة، أحياناً بقصد استغلالي.

27- **التحديات المحددة المتعلقة بتقنيات الهندسة الاجتماعية.** على خلاف الهجمات التي تركز على البنية التحتية، والتي تستهدف بشكل مباشر عدداً محدوداً من موارد الحوسبة التي قد تكون حمايتها أكثر سهولة، تعتبر الهندسة الاجتماعية تحدياً من عدة جوانب. ففي حين أن هذه التقنيات سهلة التطبيق من الناحية التقنية، فإنها تصمم بحيث تستطيع الوصول إلى عدد كبير من المستخدِمين في آن واحد، مما يزيد من احتمال وقوع الخرق. بالإضافة إلى ذلك، ومع أن الهندسة الاجتماعية تستهدف المستخدِمين النهائيين، إلا أنها غالباً ما تكون مجرد نقطة دخول توفر ممراً للانتقال إلى أصول أخرى في غاية الأهمية. ويمكن أن يستمر الاقتحام، الذي ييسره أفراد من القوى العاملة عن غير قصد، لسنوات دون أن يكتشف، مما يوفر للخصوم وصولاً مطولاً إلى بنية الأمن الداخلي والمعلومات السرية، مما يتيح بدوره فرصاً إضافية للهجوم. ويمكن أن يشمل ذلك التحركَ جانبياً، وهو طريقة تستخدم للانتقال بشكل جانبي من البيئة السيبرانية لإحدى المنظمات إلى البيئة السيبرانية لمنظمة أخرى بعد الاختراق الأولي، بالاستفادة من البنية التحتية المشتركة أو المرتبطة. ويثير هذا التكتيك الأخير قلق مؤسسات منظومة الأمم المتحدة بشكل خاص، حيث يشترك العديد منها في أماكن عمل أو مراكز بيانات أو خوادم مشتركة، لأنه يجعل دفاعات المنظمات، حتى أكثرها تقدماً وأفضلها حماية، مماثلة في الضعف لتلك التي تعتبر الحلقة الأضعف في السلسلة. ولذا فإن من المهم بشكل خاص ضمان التدريب المناسب والوعي بين جميع المستخدِمين فيما يتعلق بتعزيز الممارسات الصحية.

28- **التهديدات الأخرى.** حددت المنظمات أيضاً الأخطاء البشرية كمصدر لا يمكن تجاهله للضعف الناشئ عن أخطاء التكوين أو الأخطاء التشغيلية أو عدم الامتثال للإجراءات أو فقدان المعدات أو الضرر غير المقصود الناجم عن نقص الوعي عموماً. ونادراً ما تطرأ إخفاقات الطرف الثالث، وهو أمر مشجع لأنه يشير إلى أن المنظمات تبذل ما يكفي من العناية الواجبة في اختيار شركائها التجاريين. كما أن الكوارث الطبيعية فضلاً عن الأخطار الأخرى، بما في ذلك الاضطرابات الناجمة عن النزاع أو النشاط الإرهابي، كانت أقل شيوعاً، مع أنها تشكل مجالاً مهماً يتعين فيه أن تسير اعتبارات الأمن المادي والأمن السيبراني جنباً إلى جنب للتخفيف من الأثر.

29- **منشأ التهديدات.** في سياق الأمم المتحدة وكذلك بشكل عام، يمكن أن تنشأ حوادث الأمن السيبراني من مجموعة واسعة من المهدِّدين (الإطار 2)، الذين يمكن أن يكونوا من داخل الكيان أو من خارجه، والذين قد يتصرفون طواعية (هجوم متعمد) أو بصورة غير طوعية (عن طريق الأفعال أو الإغفالات غير المقصودة أو من خلال استغلالهم دون علمهم). وتقدم بعض الجماعات الإجرامية قدراتها لجهات فاعلة أخرى بالأجرة، أي أنه يستعان فعلاً بمصادر خارجية للقيام بالهجمات من خلال ممارسة يمكن تسميتها "الجريمة السيبرانية كخدمة". وبناءً على ذلك، فإن الإجابة على السؤال عمّن يقف

وراء هجوم معين (إسناد التهديد) تمثل تحدياً، لأسباب ليس أقلها وجود آليات لا تعد ولا تحصى تُستخدم للتعتيم على المنشأ الفعلي للهجوم (على سبيل المثال من خلال الانتحال أو المسح الروبوتي وما إلى ذلك). وبالفعل، اعترف عدد من المسؤولين الذين تمت مقابلتهم بأن مؤسسات منظومة الأمم المتحدة لا تفتقر فقط إلى القدرة على تحديد مصادر الهجوم على نحو موثوق، ولكنها تتردد أيضاً في السعي إلى إسناد المنشأ، لأن التكاليف التي تنطوي عليها محاولة القيام بذلك تفوق كثيراً الفائدة أو المنفعة من معرفة الجهة الكامنة وراء الاقتحام. وأعرب كثيرون عن أنهم يركزون جهودهم على الوقاية والكشف والاستجابة بدلاً من استثمار الوقت والموارد في ملاحقة الخصوم، لأن ذلك يتطلب جهوداً كبيرة، ولأنه حتى إذا تم إيقاف الخصوم بنجاح، فإن المشكلة لا تنتهي بذلك نظراً لأن المنظمات ستستمر في التعرض لخصوم آخرين. وينطبق هذا أيضاً على ظاهرة التهديدات المستمرة المتقدمة، والتي أكدت المنظمات أنها حدث لا يستهان به وتميل إلى أن تتخذ شكل الاقتحام والرصد والفعل المتأخر، مما يتطلب مستوى من الموارد والتعقيد يرتبط عادة بالهجمات التي ترعاها إحدى الدول.

الإطار 2

الأنواع الرئيسية لجهات التهديد في البيئة السيبرانية

- **القراصنة الحاسوبيون.** أفراد أو جماعات يخترقون الشبكات لإحداث اضطراب أو أذى أو فوضى وذلك في الغالب من أجل الشهرة أو الرغبة في التحدي.
- **نشطاء القرصنة الحاسوبية.** قراصنة حاسوبيون لديهم دوافع محددة ويرون في نشاطهم شكلاً من أشكال العصيان المدني أو وسيلة للتعبير عن الذات سياسياً أو أيديولوجياً.
- **مجرمو الفضاء السيبراني.** جهات فاعلة تنخرط في نشاط إجرامي ممكّن سيبرانياً (الجرائم الشائعة مثل الاحتيال والسرقة والابتزاز وما إلى ذلك، بمساعدة الوسائل الحاسوبية) أو في نشاط إجرامي معتمد على الفضاء السيبراني (مثل نشر الفيروسات أو البرمجيات الخبيثة وغيرها من الأنشطة التي لا يمكن ارتكابها إلا من خلال الوسائل المحوسبة). ووفقاً لمستوى التطور التقني والقدرة التنظيمية، يمكن أن تتراوح هذه الجهات الفاعلة بين الجماعات الصغيرة عموماً إلى شبكات الجريمة المنظمة الكبيرة.
- **جواسيس الصناعة.** تُعتبر هذه الفئة أحياناً فئة فرعية من الجماعة الإجرامية، وأهدافها محددة بالحصول على الأسرار التجارية، أو الابتزاز لأسباب تتعلق بالمصلحة الاقتصادية، أو تخريب المنافسة، وغالباً ما تشاهَد في عالم الشركات.
- **الدول أو المجموعات التي ترعاها دولة.** جهات فاعلة متطورة للغاية وذات موارد جيدة يصعب عادة اكتشاف أنشطتها أو تعقبها أو تحديدها، ويمكن أن تلتمس بطريقة خفية أهدافاً معقدة، غالباً ما تكون غير مباشرة وغير واضحة، وهي تُستخدم بشكل مباشر من قبل كيانات حكومية أو عسكرية أو بتمويل غير مباشر منها. وفي الماضي، طورت الدول قدرات في مجال التحقيق في المقام الأول، ولكن في السنوات الأخيرة أصبح من الحقائق المقبولة على نطاق واسع أن بعضها قد اكتسب قدرات هجومية إضافية.
- **المطلعون.** جهات فاعلة لا تعتبر، بحكم علاقتها التعاقدية مع المنظمة المعنية، جهات خارجية ولكنها تعرّضها للخطر من الداخل. ويمكن أن تشمل هذه الفئة الموظفين الساخطين والموظفين المدربين تدريباً سيئاً أو مقدمي الخدمة المتعاقد معهم والمدربين تدريباً سيئاً، إلى جانب جهات أخرى.

جيم- الأثر المعروف وغير المعروف لحوادث الأمن السيبراني

30- **الإبلاغ عن أثر محدود.** من أجل فهم أفضل لمدى ترجمة المخاطر إلى حوادث أمن سيبراني أثرت على المنظمات المشارِكة في وحدة التفتيش المشتركة، طلبت الوحدة من المنظمات تقييم أثر الحوادث السابقة حسب شدتها (من أثر غير هام إلى أثر بالغ) وفئة الأثر (المالي أو التشغيلي أو الرقمي أو السياسي أو المتصل بالسمعة، أو المادي أو البدني أو المتصل بالإنتاجية). ومن المثير للاهتمام، ولعله من المفاجئ، أن المنظمات المشارِكة جميعها أفادت في ردودها بأن أثر حوادث الأمن السيبراني التي واجهتها كان طفيفاً أو غير هام، بغض النظر عن نوعه. في الوقت نفسه، يُسلّم بأن عدد وتواتر ما تم تجنبه من حوادث الأمن السيبراني كبير يصل إلى الآلاف شهرياً، وقد نما بشكل كبير في السنوات الأخيرة. ويؤكد ذلك حجم التهديدات السيبرانية التي تتعرض لها المنظمات والبنية التحتية الخاصة بها اليوم. على أنه، وللوهلة الأولى، ومراعاة للافتقار نسبياً لجمع البيانات بشكل منهجي في هذا المضمار، يبدو أن هذا الحجم يشير إلى أثر محدود نسبياً بشكل عام.

31- **المجالات الأشد تضرراً.** أفادت المنظمات أن المجالات الأشد تضرراً من الهجمات السيبرانية (والتي يصنف أثرها على أنه "معتدل" من قبل عدد أكبر نسبياً ولكنه محدود من المنظمات، و"رئيسي" من قبل منظمة واحدة أو منظمتين، بيد أن أياً من المنظمات لم تصنف الأثر عليها على أنه "حاد")، هي المجال الرقمي (بشكل رئيسي تسرب البيانات) يليه الإضرار بالسمعة والضرر السياسي (معلومات مضللة، واهتمام إعلامي غير موات، وتدخل غير مبرر في العمليات الحكومية الدولية، إلى ما هنالك). وحتى من الناحية المالية، فإن الخسائر المباشرة (مثل التحويلات الاحتيالية للأموال) لم تتطوِ إلا على مبالغ صغيرة، مما يشير بحذر إلى أن تدابير الرقابة كانت فعالة في هذا الصدد. على أن المفتشين يرغبون في تسليط الضوء على العواقب المالية الأخرى المرتبطة بالهجمات السيبرانية (مثل وقت الموظفين وتكاليفهم في التحقيق فيما حدث وتحديد مدى الضرر الناجم، وتكاليف استرداد الأصول أو المعدات، ورسوم الاستشارات المتعلقة بالقدرات الخارجية المطلوبة لمعالجة الخروقات، والخسائر في الإنتاجية أثناء تعطل النظام، أو تكاليف الاستثمار في منع المشاكل في المستقبل)، مما قد يكون قياسه أكثر تعقيداً بكثير، ولكنها عواقب كبيرة بلا شك. وبشكل عام، على الرغم من أن غالبية المنظمات المشارِكة قد قيّمت ذاتياً قدرتها على الاستجابة للأمن السيبراني على أنها "متوسطة" (اعتبر ثلث المنظمات فقط أن هذه القدرة "قوية" أو "قوية جداً")، فإن أثر حوادث الأمن السيبراني التي تتعرض لها منظومة الأمم المتحدة اليوم، على النحو المبلغ عنه، لا يشير في حد ذاته إلى وجود سبب خطير للقلق.

32- **الواقع غير المعروف.** على أن هناك عدة عوامل تشير إلى أن الأولوية في الاهتمام بالأمن السيبراني لها ما يبررها. أولاً، تشير البيانات التي تم جمعها إلى وجود بعض نقاط تنعدم فيها الرؤية، مما يؤكد أن الحجم الدقيق للتهديدات وما يتصل بها من عواقب غير معروف، وهو ما أقرت به عدة منظمات في ردودها. وفي معظم الأوقات، وخصوصاً في حالة الهجمات الأكثر تعقيداً، لا يوجد لدى الخصوم أي حافز للكشف عن وجودهم أو أوجه الضعف التي استغلوها، مما يشير إلى احتمال أن يكون ما لا يُكتشف من خروقات الأنظمة وتسريبات البيانات أعلى بكثير من المستوى المبلّغ عنه. وفي هذا السياق، أشار عدة محاورين إلى أن نسبة "المجاهيل المعروفة" مقارنة بما هو معروف عن حجم تهديد الأمن السيبراني كانت كبيرة، غير أن نسبة "المجاهيل المجهولة" قد تكون مصدر قلق أكبر. ثانياً، يمكن أن تقلل الاستجابات من الأثر (عن قصد أو دون قصد)، نظراً إلى أنه في ثقافة مؤسسية تحركها تقارير الأداء والشعور الحاد بالاعتماد على الموارد المرتبطة بتلك التقارير، فإن الاعتراف الصادق بأوجه الضعف لم يصبح بعد هو القاعدة في سياق ثقافة المنظمات. ويمكن نتيجة لذلك تحريف النتائج. وكمثال على ذلك، فإن 11 منظمة مشاركة أكدت رسمياً، في ردها على استبيان وحدة التفتيش المشتركة، أنها تعرضت لهجوم سيبراني رئيسي

واحد على الأقل كان له تأثير على عملياتها في الماضـــي القريب. غير أن هناك كيانات من المعروف عموماً أنها تعرضـت لمثل هذه الهجمات ولكنها لم تفصـح عن ذلك في سـياق تفاعلها مع وحدة التفتيش المشـتركة. ولذلك يمكن للمرء أن يفترض أن التهديد الفعلي، وكذلك أثره، يتجاوزان ما هو معروف وما قد تكون المنظمات مستعدة للإفصاح عنه.

33- **التهديدات السـابقة لا تعتبر مؤشـراً على ما يمكن أن يقع من حوادث في المسـتقبل.** بغض النظر عما ورد أعلاه، يبدو أن هناك إجماعاً بين الخبراء على أن من المضـلّل أن نحكم على خطورة التهديد من خلال مدى ما عُرف أنه قد تحقق في الماضـي. فإمكانية وقوع ضـرر تبقى مرتفعة وينبغي استباقها باستراتيجيات مضادة توضع في المكان الصحيح. وعلى سبيل المثال، يبدو أن مؤسسات منظومة الأمم المتحدة، مع بعض الاسـتثناءات، قد نجت حتى الآن من التهديد المتزايد المتمثل في اسـتخدام برمجيات الفدية لأغراض ابتزاز الأموال مقابل البيانات المسروقة. وتؤكد التقارير الإعلامية أن عدة كيانات معروفة، منها شـركات كبرى في القطاع الخاص وحتى كيانات حكومية محلية، أُجبرت على دفع الفدية لاسـتعادة قدرتها على الوصـول إلى أنظمة بياناتها ومعلوماتها. ويلاحظ المفتشـون أن هناك، في الوقت الحاضر، موقفاً واضـحاً اتخذته المنظمات المشارِكة ضـد دفع أي فدية للمجرمين. وعلى الشاكلة نفسها، تجدر الإشـارة إلى أن مؤسـسـات منظومة الأمم المتحدة حتى الآن لم تبلغ عن تعرضـها لأي هجمات سيبرانية ضد الأجهزة المتصلة بشبكات، مثل المصاعد أو أنظمة التهوية أو المركبات ذاتية القيادة أو أية معدات مماثلة يتم التحكم فيها عن بعد. ويعدّ اسـتهداف الأجهزة المتصـلة بشـبكات مجالاً جديداً من مجالات مخاطر الأمن السـيبراني، ولكن ينبغي على الكيانات الانتباه إذ أن خبراء الصـناعة يتوقعون حدوث زيادة كبيرة في هذا النوع من التهديد في المستقبل. ويُبين هذان المثالان أهمية استباق مخاطر ربما لم يكن لها إلا سابقات محدودة في سياق الأمم المتحدة حتى الآن، ووجوب إدراج اعتبارات الأمن السيبراني استباقياً في عملية الإدارة الشاملة للمخاطر في المنظمات.

34- **التأمين السـيبراني.** لزيادة الحماية الاسـتباقية ضـد التهديدات الناشـئة، يتمثل أحد الخيارات في شراء التأمين السيبراني لتغطية الأضرار التي تسببها الهجمات السيبرانية، بل ويمكن القول أيضاً للتهرب من الاضطرار إلى التعامل مع البعد الأخلاقي لمسألة دفع الفدية أو الامتناع عن دفعها. ويمكن أن يطلب العملاء من الباعة التجاريين، في كل حالة على حدة، توفير تأمين سيبراني. وأثناء الاسـتعراض، لم تُشـر أية مؤسـسـة في منظومة الأمم المتحدة إلى أنها اختارت تأميناً كهذا لتغطية المخاطر السـيبرانية، مع أن بعضـها ذكر أنها تفكر في ذلك. واعترافاً بالموقف السـائد بين كيانات الأمم المتحدة، لا يعتبر المفتشـون التأمين السيبراني أداة فعالة للتصدي الاستباقي للمخاطر ذات الصلة في معظم السياقات التشغيلية، خاصة وأنه لا يشكل سوى استراتيجية للتخفيف الجزئي تسهم في تقليل الخسائر المالية التي قد يتسبب فيها هجوم سـيبراني، دون أن يحقق إلا القليل من حيث معالجة الضـرر التشـغيلي أو الإضـرار بالسـمعة. على أن **المفتشين يرون أن من المحبذ أن تستعد الإدارة التنفيذية لاحتمال وقوع تهديدات كهذه، وهو احتمال من المرجح أن يزداد في المستقبل.**

دال- العمل والتعاون مع السلطات الوطنية

35- **تفاوت الممارسـات والتقبل المحدود لفكرة إبلاغ السـلطات الوطنية.** لدى المنظمات المشـارِكة ممارسات مختلفة عندما يتعلق الأمر بإبلاغ السلطات الوطنية عن انتهاكات الأمن السيبراني، مع أن هذه السـلطات قد تكون في وضـع يمكنها من التحقيق واتخاذ إجراءات إدارية أو قضـائية بخصـوص الهجوم السيبراني. وذكر حوالي ثلث المنظمات المشارِكة أنها أبلغت سلطات إنفاذ القانون الوطنية بالحوادث، لكن

قلة منها فعلت ذلك بشـــكل منهجي أو روتيني. ومن بين المنظمات التي أشـــارت إلى أنها عملت مع السلطات الوطنية في مسائل الأمن السيبراني في الماضـي، أكد معظمها أنها فعلت ذلك على أساس كل حالة على حدة وليس اسـتناداً إلى سـياسـة أو ممارسـة ثابتة لدى المنظمة. واسـتخدمت منظمات كثيرة علاقات العمل غير الرسـمية بدلاً من القنوات الرسـمية حيثما أمكن، على أنها لم تفعل ذلك إلا عند وقوع هجمات كبيرة توحي إما باحتمال وجود أثر على البلد المضـيف أو تعريض سـمعة المنظمة لخطر كبير. وحتى في الحالات التي تتجاوز فيها قدرات التحقيق الوطنية المتعلقة بملاحقة المهاجمين المشـــتبه بهم القدرات الداخلية لدى المنظمات – وهي قدرات غالباً ما تكون محدودة للغاية – وبالتالي يمكن أن تكملها بشكل مفيد، لم تعرب إلا قلة من المنظمات عن رغبتها في التفاعل المنهجي مع السلطات الوطنية، أو في زيادته، فيما يتعلق بانتهاكات الأمن السيبراني، أو عن حاجتها إلى إضفاء طابع رسمي على ذلك التفاعل أو زيادته. وتشير الصورة الإجمالية إلى تقبل محدود لفكرة التعامل مع السلطات الوطنية وإلى تفضيل إبقاء التفاعل على شكله غير الرسمي واللجوء إليه "حسب الضرورة".

36- **العوامل التي تؤثر على ممارســـات المنظمات.** هناك عوامل مختلفة قد تدفع المنظمات إلى التردد في الاتصـــال بالســـلطات الوطنية. أحدها هو الوضـــع القانوني للمنظمات بحكم ما تتمتع به من امتيازات وحصـانات، لا سـيما من حيث سـرية بياناتها وحرمتها، ووجوب خلوها من أي تدخل ذي طابع تشـريعي أو تنفيذي أو قضـــائي. وكثيراً ما تكون حدود الالتزام القانوني في هذا المجال غير مفهومة جيداً من جانب ممارسـي الأمن السيبراني. والواقع أنه، في حين أن الدول ملزمة قانونياً بتقديم الحماية، فإن المنظمات لا تُلزم إلا بالتعاون مع السـلطات الوطنية بحدود عدم تعارض هذا التعاون مع قدرتها على ممارسـة وظائفها بشـكل مسـتقل. ولذا فإن هذا التعاون طوعي دائماً. وقد تكون هذه الصـيغة خطأً رفيعاً بالفعل للتعامل مع المسـألة على صـعيد الممارسة العملية غير أنها ينبغي ألا تعيق التعاون الطوعي عند الضـرورة، بعد إجراء تقييم كامل للمخاطر التي يُحتمل أن تترتب على ذلك التعاون. وعلى أي حال، لا يوجد واجب لإبلاغ السـلطات الوطنية عن الحوادث أو الكشـف عن أية بيانات تعتبر حسـاسـة. وتشـغل الإدارات القانونية الموقع الأفضـل لتقديم المشورة لصـانعي القرار في هذا الصـدد. وهناك عامل آخر يتعين النظر فيه عند البتّ فيما إذا كان سـيجري الاتصـال بالسـلطات الوطنية أم لا وهو يتصـل بمستوى النضـج في جهاز الأمن السـيبراني في البلد المعني، بالإضـــافة إلى تعامله مع مرتكبي الجريمة السـيبرانية بعد إحالتهم إلى الولاية القضـــائية الوطنية. ويمكن أن تتعقد هذه المخاوف في حال تورط موظفي المنظمة نفســها في تعريض أمنها الســيبراني للخطر (التهديدات الداخلية). وفي مثل هذه الحالات، تتوخى الإجراءات المعتادة رفع الامتيازات والحصـانات وتسـليم الشـخص إلى دولة جنسيته لإجراء مزيد من التحقيق وما يُحتمل من مقاضاة. على أن هذا لا يزال نادر الحدوث نسبياً، لا سيما فيما يتعلق بسوء السلوك عبر الفضـاء السيبراني. وقد بدأ في عام 2007 تجميع الإحصـاءات ذات الصـلة ونشرها، ومنذ ذلك الحين أحيل موظف واحد في حالة سوء سلوك عن طريق مكتب الشؤون القانونية إلى السـلطات الوطنية لإجراء مزيد من التحقيق بشـأن انتهاك أمن المعلومات[11]. بالإضـافة إلى الاعتبارات الموضـــحة أعلاه، كانت العوامل المتمثلة بشـــدة الحادث، وفائدة واحتمال النجاح في عزو الهجمات إلى مرتكبها، واحتمال الكشف غير المبرر عن معلومات سرية أو حساسة، والأثر المحتمل للتحقيق على الأنشطة التشغيلية، من بين أكثر العوامل التي يُذكر أنها تُراعى عند اتخاذ قرار بالاتصال بالسلطات الوطنية أو عدمه. كما أقر بعض المسؤولين بأن خيار إبلاغ السلطات الوطنية غالباً ما كان يتعرض للإهمال.

37- **عملية صـــنع القرار المتعلق بإبلاغ النظراء الوطنيين.** كما هو موضـــح أعلاه، فإن القرار بشـــأن الاتصـــال بالسـلطات الوطنية أو عدمه ينطوي على أبعاد تتجاوز اختصـــاص خبراء الأمن السـيبراني. فهناك مجموعة من الاعتبارات السياسية والقانونية والاستدلالية والعملية التي ينطوي عليها الأمر، وعلى هذا فإن القرار

(11) A/75/217، المرفق الأول.

ينبغي أن يشمل مجموعة من أصحاب المصلحة. وفي المنظمات التي وجد المفتشون فيها دليلاً على وجود نهج أكثر رسوخاً في التعامل مع السلطات الوطنية، عكس توزيع المسؤوليات مجموعة الاعتبارات ذات الصلة، مما يُعتبر ممارسة جيدة. وبشكل أكثر تحديداً، يقوم مكتب البرنامج المتضرر أو الوحدة الفنية المعنية بتقييم شدة الاقتحام، وموازنة المخاطر البرنامجية، وفوائد الاتصال بالسلطات الوطنية. ويُجري المكتب القانوني تقييماً للتداعيات المحتملة ذات الطابع القانوني، ويسدي المشورة بشأنها، على ضوء المركز الخاص للمنظمات وموظفيها في الولايات القضائية المعنية، بما في ذلك احتمال وجوب رفع الامتيازات والحصانات، ويحيل عند الاقتضاء الموظفين المتورطين إلى بلد جنسيتهم. ويتمثل دور إدارة تكنولوجيا المعلومات والاتصالات أو خبراء الأمن السيبراني في تقديم الأدلة الجنائية على الانتهاك إلى الحد المتاح. ويعود إلى الإدارة التنفيذية قرار المضي قدماً في إثارة المسألة مع البلد المضيف، ويساهم فيه جميع أصحاب المصلحة المذكورين أعلاه. وعند اتخاذ قرار بالعمل مع السلطات الوطنية فيما يتعلق بحادث ما، فإن آليات القيام بذلك تتمثل عادة في خطوط الاتصال القائمة بين المكاتب ذات الصلة في منظمات الأمم المتحدة، والبعثة الدائمة للدولة المعنية، والسلطات ذات الصلة في البلد المضيف المعني. وبالنظر إلى بعض الملاحظات النقدية المدلى بها بشأن فعالية العملية القائمة، فقد يكون هناك مجال لدراسة بعض السبل البديلة أو التكميلية، ويرد وصفٌ لبعضها في مكان آخر في هذا التقرير (الفقرات 161-163).

هاء- الاستعداد التكنولوجي - مسائل مختارة للاهتمام بها

38- **القدرات التقنية الأساسية الحسنة التطوير، وتسليط الضوء على مجالات تتطلب اهتماماً أوثق.** طرح المفتشون سلسلة من الأسئلة على المنظمات المشارِكة بهدف فحص الحالة العامة لاستعدادها التكنولوجي لدرء التهديدات السيبرانية. ولم يكن القصد من ذلك إجراء تقييم شامل لمدى متانة ترتيباتها التشغيلية أو بنيتها التحتية التقنية، بل التوصل إلى فهم القدرات العامة الموجودة وعزل بعض القضايا المشتركة التي قد تستحق اهتماماً خاصاً. ومع مراعاة القيود المتأصلة في المعلومات التي تُجمع أساساً من خلال التقييم الذاتي، فضلاً عن التباين الكبير في مستوى التفاصيل المعروضة على المفتشين، تُظهر الردود أن المنظمات المشارِكة تعتبر الجوانب التقنية الأساسية للأمن السيبراني مفهومة ومستثمر فيها جيداً وفقاً لقدرات كل منها. وعلى سبيل المثال، أشار ثلثا المنظمات المشارِكة إلى وجود أدوات لرصد الشبكات. بالإضافة إلى ذلك، تشير معظم المنظمات إلى أنها أقامت جدران حماية نارية للحماية أو أنها استخدمت أنظمة أخرى لمنع الاقتحام، بينما أبلغت 13 منظمة عن تنفيذها لنظامٍ لإدارة المعلومات والحوادث. على أن الصورة في المجالات التي خضعت لمزيد من التطور التكنولوجي الدينامي في الماضي القريب تبدو أكثر تنوعاً في تفاصيلها وقد تتطلب بعض الاهتمام من جانب المنظمات المشارِكة. ولا يحدد هذا القسم من التقرير، لأسباب أمنية، أية ترتيبات بعينها لدى المنظمات، وذلك لتجنب التوصل إلى استنتاجات قد تعرض أمن الكيانات المعنية للخطر.

إدارة أجهزة الاستخدام النهائي، والأدوات التي تيسر العمل عن بُعد

39- **أدت جائحة كوفيد-19 إلى التركيز على إدارة أجهزة الاستخدام النهائي.** فقد فرضت الجائحة تنفيذ ترتيبات عمل بديلة ومرنة على نطاق أوسع بكثير مما شهدته الممارسة سابقاً في جميع الفئات المهنية تقريباً، سواء في المقر الرئيسي أو على المستوى الميداني. وفي ظل هذه الخلفية، خضعت قدرة المنظمات على العمل خارج أماكن العمل، وما ارتبط بذلك من محدودية الوصول المادي إلى المباني والمعدات الحاسوبية المتصلة مركزياً، إلى اختبار للإجهاد غير مسبوق، كما تعرضت الأدوات التي تسهّل العمل عن بُعد لمزيد من التدقيق من منظور الأمن السيبراني. ومن ناحية، يشمل ذلك قدرة الموظفين على الوصول الآمن إلى موارد الحوسبة عن بُعد، وقد أشار ثلثا المنظمات إلى أنها يسّرت ذلك الوصول من خلال استخدام شبكات افتراضية خاصة، بينما استخدمت المنظمات المتبقية خدمات سحابية يتم الوصول

إليها من خلال بروتوكولات الإنترنت المشفرة على الشبكة العامة دون الحاجة إلى شبكات افتراضية خاصة. ومن ناحية أخرى، تتضمن القدرة على العمل خارج الموقع إدارة أجهزة الاستخدام النهائي (أجهزة الحاسوب المكتبية والمحمولة بالإضافة إلى الأجهزة المحمولة الأخرى)، والتي تشير الردود إلى مستوى تغطية أكثر تنوعاً.

40- **تخلف إدارة أجهزة الاستخدام النهائي عن الركب.** في حين أن غالبية المنظمات تشير إلى توفر درجة ما من الإدارة المركزية للأجهزة، فإن عدداً منها يبدو أنه لا يوفر تغطية كاملة. وفي بعض الحالات، تقتصر التغطية على المعدات الموجودة في المقر الرئيسي وحدها، فقد أشارت سبع منظمات إلى أن مكاتبها الميدانية تتبع ممارسات منفصلة لإدارة الأجهزة، وفي حالات أخرى، لا تحصل على تغطية مركزية إلا أجهزة الحاسوب المتصلة بشكل دائم، بينما لا يوفر نحو ثلث المنظمات المشارِكة أية إدارة أو حماية مركزية على الإطلاق للأجهزة المحمولة، مع أن قلة من هذه المنظمات في طور نشر منصات لهذا الغرض أو تخطط للقيام بذلك في المستقبل القريب. ويذكر ردان فقط تشفير أجهزة الاستخدام النهائي، وهو إجراء مهم لمنع سرقة البيانات وتسريبها، لا سيما على مستوى أجهزة المستخدم النهائي المحمولة، والتي تعتبر عموماً أكثر عرضة للضياع والسرقة. وقدمت الردود أدلة تشير إلى أن المنظمات كانت تدرك أن هناك حاجة إلى إدارة مركزية للأجهزة، غير أنها أظهرت أن إدارة الأجهزة المحمولة كانت متخلفة عن الركب. وقد زادت حدة أوجه الضعف الموجودة في هذا الصدد من خلال استخدام الأجهزة المحمولة الشخصية غير المؤسسية مثل أجهزة الحاسوب المحمولة الخاصة – وهي ممارسة شهدت زيادة كبيرة خلال الجائحة.

41- **استحداث تدابير مهمة في مجال الأمن السيبراني أو تسريع الأخذ بها.** على الرغم من التحديات العديدة المواجَهة، أدى ظهور الجائحة أيضاً إلى بعض التطورات الإيجابية. فقد ضُغط على كيانات الأمم المتحدة لكي تُلقي نظرة فاحصة على أطرها لإدارة الأمن، وبدأت المشاريع المؤسسية المخطط لها في مجال تكنولوجيا المعلومات والاتصالات تتحقق بحكم الضرورة العاجلة. ويمكن القول إن التحول الهائل إلى العمل عن بعد في غضون مهلة قصيرة للغاية أدى بالعديد من المنظمات إلى تسريع جهودها نحو تحسين أمن الوصول عن بعد، وربما وفّر، وفقاً للردود على استبياني وحدة التفتيش المشتركة، الزخم الذي تشتد الحاجة إليه لتحفيز العمل في هذا المجال. والواقع، أن معظم الكيانات أنشأت نظاماً للتحقق متعدد العوامل لأغراض الوصول عن بُعد، وطرحت أدوات التعاون وتقاسم البيانات عبر الإنترنت بمستويات لم يسبق لها مثيل، وأضفت الطابع المؤسسي على استخدام التوقيعات الإلكترونية، ووسّعت نطاق فرص التدريب على أمن المعلومات. فالجائحة، بمعنى ما، أصبحت حافزاً للتحويلات الخاصة بتكنولوجيا المعلومات والاتصالات في عدد من كيانات الأمم المتحدة ودفعتها باتجاه الرقمنة وممارسات العمل الرقمية المتقدمة – وهو عامل له آثار لا في مجال الأمن السيبراني وحده، ولكن أيضاً، وعلى نطاق أوسع بكثير، فيما يتعلق بأسلوب عمل المنظمات، فضلاً عن سبل إدارة الأصول والمباني.

الأنظمة القديمة

42- **أوجه ضعف محددة أوجدتها الأنظمة القديمة.** أشارت عدة منظمات مشارِكة إلى أن تحديث الأنظمة القديمة المتقادمة التي قد لم تعد مدعومة بأحدث التطبيقات يطرح تحديات كبيرة في مجال الأمن السيبراني، شأنه في ذلك شأن إنهاء العمل بها. وقيل إن استمرار وجود هذه الأنظمة القديمة يمثل مصدراً رئيسياً للضعف، فكثير منها كان مصمماً للاستخدام المحلي وحده، على شبكات خاصة – محلية أو واسعة – كانت تعتبر بيئات آمنة. ويرجع أساساً إلى تطور الوصول عن بُعد وزيادة استخدام الحوسبة السحابية أن هذه التطبيقات أصبحت الآن أكثر تعرضاً للمخاطر الناشئة عن الترابط الأكبر بين الأنظمة والبيانات على الصعيد العالمي، في حين أنها غير مصممة لمقاومة الأشكال الأحدث من الهجمات.

ويمكن تسجيل بعض أوجه الضعف الأمنية الناشئة عن ذلك والتنبيه إليها باستخدام أنظمة إدارة مكامن الضعف، ولكن تبقى هناك إمكانية عدم اكتشاف بعض التطبيقات القديمة، المسجلة الملكية، تلقائياً. ويمكن، حتى عند اكتشافها، ألا تتوفر لها بالضرورة حلول فورية، وأن تؤدي إلى تعرض الكيانات المعنية للخطر لفترات طويلة دون داع. وإضافةً إلى مخاطر التطبيقات القديمة نفسها، فإن أوجه الضعف هذه تشكل أيضاً خطراً على التطبيقات والبيانات الأخرى التي قد تتقاسم نفس البنية التحتية، إذ يمكن، عند اختراقها، استخدامها في التحرك الجانبي عبر الأنظمة والتطبيقات.

43- **هناك ما يبرر إجراء استعراض متأنٍ للأنظمة القديمة.** لذلك، فإن من الأهمية بمكان أن تتابع مؤسسات منظومة الأمم المتحدة هذه الأنظمة وأن تعمل بنشاط على تحديثها أو استبدالها. ونظراً لأن بعضها كبير ومعقد (مثل أنظمة التخطيط المركزي للموارد)، ولأن العديد منها بُني داخلياً حسب الاحتياجات على مدار فترات زمنية طويلة، فقد تكون هذه المهمة معقدة بالنسبة للكثيرين وتتطلب مزيداً من الموارد المالية والجهود للحصول على دعم وحدات الأعمال التي استثمرت في تطوير حلول مهيأة خصيصاً باتت تعتبر الآن غير آمنة، ولضمان استمرار ذلك الدعم. **ويقترح المفتشون أن يطلق الرؤساء التنفيذيون، بالتعاون الوثيق مع خبراء تكنولوجيا المعلومات والاتصالات والأمن السيبراني، فضلاً عن وحدات الأعمال المتضررة، استعراضاً متأنياً لمشكلة الأنظمة القديمة في منظماتهم، ما لم يكن ذلك الاستعراض قد بدأ بالفعل.** وينبغي أن تحتل اعتبارات الأمن السيبراني مكانة بارزة فيما يقومون به من تحليل، على قدم المساواة مع النظر الاستراتيجي في الوقت المناسب في الآثار المترتبة على الموارد والأثر الفوري والطويل الأجل على العمليات في حال إيقاف العمل بتلك الأنظمة، وهو ما ينبغي معالجته من خلال التخطيط المناسب لوضع تدابير للتخفيف المؤقت حيثما أمكن ذلك.

الأمن السحابي

44- **تحسنت إلى حد كبير الحماية التي يوفرها مقدمو خدمات الحوسبة السحابية الخارجية، وفقاً لمجتمع خبراء الأمن السيبراني.** منذ عام 2019، عندما أصدرت وحدة التفتيش المشتركة تقريرها عن الحوسبة السحابية[12]، طرأ نمو كبير في استخدام المنظمات المشارِكة في الوحدة للخدمات القائمة على الحوسبة السحابية، وفي نطاق هذه الخدمات، ونضجها. فقد أدى اتساع انتشارها ومرونتها (قدرتها على المضاهاة المستمرة بين تخصيص موارد الحوسبة والطلب الفعلي على الموارد في الوقت الفعلي)، وفعاليتها من حيث التكلفة، بالإضافة إلى تطورها التكنولوجي المتزايد باستمرار، إلى مضاعفة ثقة المستخدِمين في متانتها وسلامتها، وزيادة جاذبيتها لدى منظومة الأمم المتحدة. وتستمر المنظمات في ترحيل تطبيقاتها الحالية إلى الخدمات القائمة على الحوسبة السحابية، على أن قرار القيام بذلك يبقى خاصاً بكل منظمة. وفي هذا الصدد، يقرّ المفتشون بتزايد الاعتراف عبر مجتمع خبراء الأمن السيبراني بأن قدرات الحوسبة السحابية والضمانات التي يقدمها قادة الصناعة التجارية اليوم تتجاوز مستوى أمان البيانات وسريتها والقدرة على الصمود في المجال السيبراني الذين كانوا قادرين على تقديمه قبل عام أو عامين فقط. ووفقاً للخبراء، من المرجح أيضاً أن تتجاوز الحماية التي يتيحها مقدمو الخدمات هؤلاء حالياً قدرة أي منظمة على تحقيق درجة مماثلة من الأمن باستخدام الحلول المطورة داخلياً. وأثناء الاستعراض الحالي لم يصادَف إلا مثالٌ واحد لمنظمة مشاركة اختارت الانفصال كلياً عن الحلول القائمة على الحوسبة السحابية فيما يتعلق بجزء منفصل وحساس من البيانات التي تديرها. على أن من الجدير بالذكر أن هذا الخيار اتُخذ بخصوص مجموعة محدودة من البيانات واستند إلى قدرة تلك المنظمة – بما في ذلك قدرتها المالية – على توفير بديل صالح، وهو أمر غير متوفر لدى معظم المنظمات.

(12) JIU/REP/2019/5.

45- **هناك ما يبرر استمرار اليقظة في استخدام خدمات الحوسبة السحابية الخارجية.** حتى على خلفية التقدم الكبير المحرز خلال السنوات الأخيرة فيما يتعلق بأمن الحوسبة السحابية، تظل التوصيات المقدمة إلى الرؤساء التنفيذيين في تقرير وحدة التفتيش المشتركة المشار إليه سارية المفعول فيما يتعلق بما يلي: الحاجة إلى مواءمة خدمات الحوسبة السحابية مع احتياجات الأعمال لتحقيق قيمة الاستثمار؛ وتقييمات شاملة للمخاطر وإدارة متأنية للباعة لإشراك مقدمي الخدمات السحابية الخارجيين؛ واستراتيجيات للتخفيف من مخاطر احتمال فشل الباعة في تقديم الخدمات المتعاقد عليها. وهناك مخاوف مستمرة تتعلق بمخاطر الاحتكار والإفراط في تركيز بيانات الأمم المتحدة في أيدي عدد قليل نسبياً من عمالقة التكنولوجيا. وبناءً على ذلك، لا يمكن للمنظمات أن تتخلى عن حذرها عند استخدام التطبيقات القائمة على الحوسبة أو عند وضع تطبيقاتها وبياناتها في الفضاء السحابي، لا سيما على ضوء مخاطر الوصول غير المأذون به إلى البيانات السرية أو الحساسة. ويتعين عليها أن تستمر في ممارسة العناية الواجبة والحفاظ على ممارسات الأمن السيبراني السليمة عند الاعتماد على خدمات الحوسبة السحابية، لا سيما من خلال طلب دليل على امتثال مقدمي الخدمات لمتطلبات المراجعة المستقلة وإبراز الشهادات ذات الصلة، من قبيل تقارير ضوابط الأنظمة والتنظيم، وعلى وجه الخصوص تلك المعروفة باسم "تقارير ضوابط تنظيم الخدمة" (SOC 2 reports) أو ما يماثلها من ضمانات يعترف بها خبراء الصناعة على نطاق واسع. ويكتسي طلب هذا الضمان الخارجي المستقل أهمية عند النظر في الواقع المتمثل في أن كفاءة المراجعة الداخلية والآليات الرقابية الأخرى في المنظمة يمكن أن تتوقف عند التعاقد مع مقدمي خدمات خارجيين. لذلك يوصى بالحصول على رأي إدارة المراجعة الداخلية عند إبرام عقدٍ لهذه الخدمات، ضماناً لإدراج الأحكام اللازمة التي تعطي ضماناً معقولاً للامتثال لمعايير الرقابة الداخلية المناسبة فيما يتعلق بتجميع المعلومات المقدمة وتخزينها واستخدامها. كما يُنصح بالتشاور مع المكتب القانوني. ولذا يتعين على المنظمات أن تجد بدائل مقبولة لفرض درجة من السيطرة تعتبر كافية، على سبيل المثال من خلال إدراج أحكام في الترتيبات التعاقدية مع مقدمي الخدمات السحابية الخارجيين تسمح للكيان بممارسة الإشراف والرقابة على الامتثال. علاوة على ذلك، يمكن أن تتغير ملكية مرافق الحوسبة السحابية التجارية، حتى عبر الحدود، مما قد يؤدي، في بعض السياقات، إلى زيادة تفاقم خطر تعرض البيانات التي تحتفظ بها تلك المرافق أو تديرها، في حال محاولة الدخول في إجراءات قانونية تخضع للولاية القضائية الوطنية ذات الصلة. وفي مثل هذه الحالات، يتم التذرع بالامتيازات والحصانات والتمسك بها فيما يتعلق بجميع البيانات المحفوظة لصالح مؤسسات منظومة الأمم المتحدة. على أن المنظمات لا بدّ أن تَبقى على يقظتها وأن تتخذ الاحتياطات اللازمة لإدارة هذه المخاطر قدر الإمكان.

46- **لا يمكن القضاء كلياً على المخاطر، والمطلوب إجراء تحليل مفصل.** بصرف النظر عن كفاءة التكلفة والفوائد الأمنية التي ستُكتسب، يُذكِّر المفتشون بأن كلاً من الحلول القائمة على الخدمات السحابية ونهُج مراكز البيانات التقليدية تتعرض لتهديدات الأمن السيبراني ولا يمكن أبداً الادعاء بأنها غير قابلة للاختراق. لذلك فإن من غير الواقعي السعي للقضاء التام على المخاطر في أي من البيئتين. وبغض النظر عما إذا كان الخطر قد نُقل، إلى حد ما، إلى كيانات خارجية تدير بيئة الحوسبة ذات الصلة، فإن المساءلة عن عواقب الهجمات السيبرانية تبقى داخلية. وعلى هذا فإن من الحصافة أن تجري المنظمات تحليلاً مفصلاً قبل أن تبتّ فيما إذا كانت مستعدة لتكليف جهات خارجية بحماية معلوماتها، وإذا كان الأمر كذلك، فإن عليها أن تحدد الجوانب التي ستخضع لذلك التكليف. وبهذه الروح، ينبغي أن تضمن تقييمات حماية البيانات توافُقَ ضمانات خدمات الحوسبة السحابية مع متطلبات المنظمات وتناسُبَها مع نوع وحساسية أصول البيانات ذات الصلة. وتنطبق اعتبارات مماثلة على أي قرار يُتخذ بشأن الاستعانة بمصادر خارجية، ولا تقتصر تلك الاعتبارات، بالتالي، على سياق استخدام الأمن السحابي.

إدارة أوجه الضعف

47- **التفاوت بين ممارسات المنظمات المشارِكة.** تعتبر إدارة أوجه الضعف أحد أكبر تحديات الأمن السيبراني في المنظمات الدولية اليوم. وتُكتشف بشكل شبه يومي أوجه ضعف جديدة في البرمجيات المستخدمة على نطاق واسع، ومنها البرمجيات التي تستخدمها مؤسسات منظومة الأمم المتحدة. وفي حين أن موردي الأجهزة والبرمجيات يطورون باستمرار التصحيحات على البرمجيات ويتيحونها، فإن هذه التصحيحات تُترجم إلى قدر كبير من المعلومات التي تتعين معالجتها وتنطوي على عبء عمل كبير في تنفيذ التصحيحات في البيئات التقنية المعقدة. وللتعامل مع هذا التحدي، أفاد أكثر من نصف المنظمات المشارِكة بأنها تلجأ إلى واحد من أشكال حلول إدارة أوجه الضعف. وعلى سبيل المثال، تستخدم بعض المنظمات الاشتراكات في نشرات استخباراتية متعددة للتعرف باستمرار على التهديدات الجديدة (ولِدرئها)، بما في ذلك أوجه الضعف الجديدة، في حين اختارت منظمات أخرى نشر حلول أمنية متكاملة تشمل إدارة أوجه الضعف، وهي حلول تشتريها من مقدمي خدمات تجاريين. وسلطت بعض المنظمات الضوء على أن اكتشاف أوجه الضعف وتصحيحها يشكلان نشاطاً مُجهداً من أنشطة الأمن السيبراني. ولاحظ بعضها أن المحاولات الخبيثة للعثور على نقاط الضعف في شبكاتها وأنظمتها تتزايد مع الوقت، في حين أن الطبيعة الموزعة لشبكة تكنولوجيا المعلومات والاتصالات لديها تُصعِّب إدارة عملية تصحيح أوجه الضعف في البرمجيات مركزياً، لا سيما عبر مواقع ميدانية متعددة. كما أفادت عدة منظمات بأن نفقات هذا التصحيح تُعتبر من أكبر التكاليف المرتبطة ببرامج الأمن السيبراني لديها.

48- **متابعة الإدارة المستمرة لأوجه الضعف.** ينبّه المفتشون إلى وجود اختلاف كبير في الفعالية بين التقييمات المخصصة (على سبيل المثال، السنوية) لأوجه الضعف والعملية المستمرة لإدارة أوجه الضعف وللتصحيح. وإذا لم تنفذ التصحيحات بانتظام، فإن أنظمة تكنولوجيا المعلومات والاتصالات تظل معرضة لمحاولات التدخل الخبيث لفترة طويلة جداً، في حين أن خطر الاختراق يزداد بشكل كبير. ولا تتيح المعلومات المجموعة من المنظمات المشارِكة في هذا الصدد مستوىً كافٍ من الثقة في أن هذا التحدي يعالج بطريقة مناسبة ومتسقة. وتشير ردود عدة منظمات على استبيان وحدة التفتيش المشتركة إلى أنها تأخذ بنهج مخصص لتقييم الضعف (يجري التقييم إما سنوياً أو حتى على فترات أطول)، في حين أن منظمات أخرى مثل وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين في الشرق الأدنى (الأونروا) وبرنامج الأغذية العالمي ومنظمة الطيران المدني الدولي ومنظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) تعتبر الإدارة الفعالة والمستمرة للضعف من بين الممارسات الجيدة لديها. **وهناك مجال للتحسين في هذا المجال، ويحث المفتشون الرؤساء التنفيذيين على إيلاء الاهتمام الكافي وتوفير الموارد المناسبة للتمكين من إجراء تقييمات منتظمة لأوجه الضعف، بهدف إرساء إدارة أوجه الضعف كممارسة منهجية في مؤسسات منظومة الأمم المتحدة.**

تكنولوجيا معلومات الظل (shadow IT)

49- **أسباب اللجوء إلى تكنولوجيا معلومات الظل.** يشير مصطلح تكنولوجيا معلومات الظل إلى تطبيقات أو حلول لتكنولوجيا المعلومات والاتصالات يتم تطويرها أو اعتمادها داخل منظمة ما ولكن خارج الإطار الرسمي لعمل تكنولوجيا المعلومات والاتصالات الذي يُدار مركزياً عادةً. وعلى الأغلب، تأتي تكنولوجيا معلومات الظل كنتيجة لمحاولة المستخدِمين حل مشكلة عملية باستخدام أدوات يمكن الوصول إليها بسهولة في السوق بتكلفة منخفضة أو بدون تكلفة، عندما يُنظر إلى الحلول المتاحة من خلال القنوات القائمة والقدرات الرسمية لتكنولوجيا المعلومات والاتصالات على أنها لا تلبي احتياجاتهم من حيث التوقيت أو التكلفة أو التكييف. كما يمكن أن تتأتى عن الرغبة في الابتكار بسرعة استجابة لاحتياجات ناشئة

أو لضمان المواءمة أو التوافق مع الأدوات المستخدمة من قبل الشركاء المنفذين والتي قد لا تتماشى مع خيار المنظمة المعتمد مؤسسياً. وتشمل الأمثلة فتح حسابات مجانية مع مقدمين للخدمات توفر الحلول لتخزين البيانات أو نقل الملفات أو التصميم الشبكي أو إدارة المحتوى، أو تطوير تطبيقات داخلية لاستخدام فرادى الإدارات أو المكاتب الميدانية أو لاستخدامها في بيئة مشروع ما. ولا يجري التدقيق في هذه الحلول عادة أو بالضرورة للتحقق من امتثالها لسياسات وإجراءات الأمن السيبراني التي وضعتها السلطة المركزية الرسمية على المستوى المؤسسي، وبالتالي يمكن اعتبارها تعمل في بيئة "ظل" غير مأذون بها.

50- **المخاطر المرتبطة باستخدام تكنولوجيا معلومات الظل.** ذُكر أن هذه الظاهرة انتشرت في بعض المنظمات، لا سيما في المكاتب الميدانية أو في إدارات تبتعد عن السيطرة المركزية بطرق أخرى. وغالباً ما تتضخم المخاطر في مثل هذه البيئات من خلال محدودية ما لدى الإدارات المركزية لتكنولوجيا المعلومات والاتصالات والأمن السيبراني من معلومات حول الأنشطة الفردية لتطوير تكنولوجيا المعلومات والاتصالات. وهنا أيضاً، أدت جائحة كوفيد-19، بما خلقته من حاجة مفاجئة لأداء العديد من الوظائف عن بُعد، إلى زيادة حدة هذا التحدي حيث بدأ العديد من المستخدِمين في استخدام أدوات للتعاون عبر الإنترنت، بما في ذلك لأغراض الاجتماعات الافتراضية، خارج الحلول التي تقدمها حزم البرمجيات المؤسسية. على أن كثيراً من الخدمات التي لجأ إليها المستخدِمون كبدائل محتملة لم تخضع لتقييم خبراء الأمن السيبراني في المنظمات أو موافقتهم عليها لأغراض استخدامها العام، الأمر الذي يمكن أن يعرض المنظمات للخطر (على سبيل المثال، من خلال التقيد بمعايير للتحقق أو السرية مختلفة عن تلك الموصى بها على مستوى الكيان). من ذلك مثلاً أن الفريق المختص بأمن المعلومات أجرى دراسة حول استخدام منصة معروفة للتداول الفيديوي عبر الإنترنت في الأيام الأولى للجائحة لتقييم مدى ملاءمتها للاستخدام من قبل مؤسسات منظومة الأمم المتحدة، غير أن خبراء الأمن السيبراني لم يتمكنوا من التوصل إلى توصية أكيدة قاطعة، سواء إيجاباً أو سلباً، يمكن اعتبارها صالحة للمنظومة ككل. وبدلاً من ذلك، صاغ الخبراء مجموعة من الخيارات، إلى جانب تحذيرات وتدابير احترازية، ينبغي أن تراعى عند استخدام المنصة عبر الإنترنت في بيئات محددة.

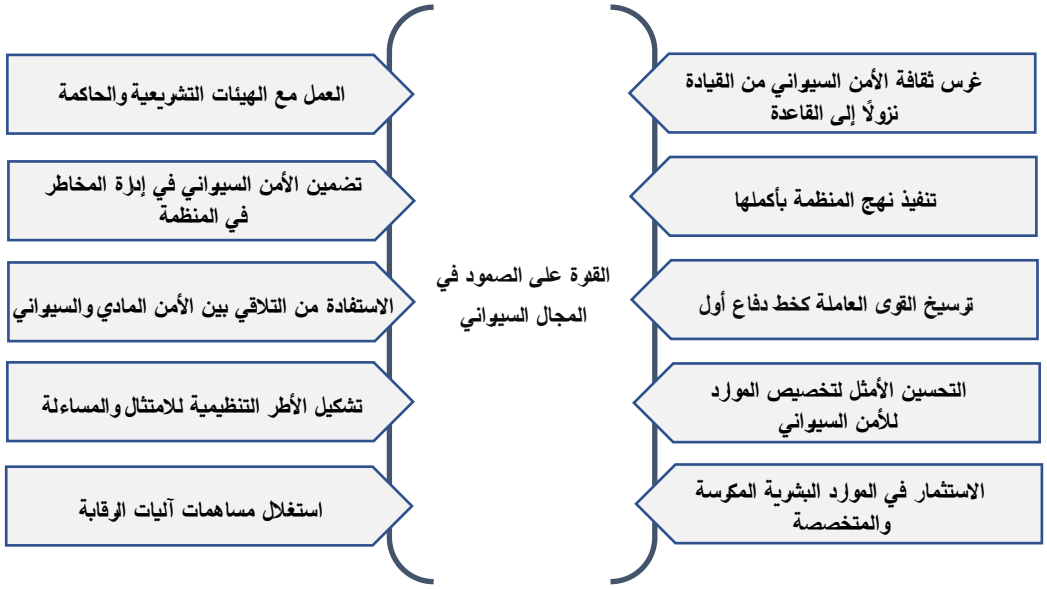
51- **بعض الاقتراحات من أجل المزيد من العناية في إدارة تكنولوجيا معلومات الظل. يرى المفتشون أن تحديات الأمن السيبراني المتعلقة بممارسات تكنولوجيا معلومات الظل تحتاج إلى مزيد من الاهتمام، وإلى تحقيق التوازن بين الحاجة إلى التحكم في بيئة معرضة للمخاطر السيبرانية وبين احتياجات المستخدِمين المشروعة ودوافعهم البناءة للابتكار وللاستفادة من الحلول البديلة عند توفرها.** في الواقع، قدمت المبررات لعدم القيام تلقائياً برفض دوافع بعض المستخدِمين للوصول إلى حلول تكنولوجيا معلومات الظل كسلوك غير مرغوب فيه، فقد اعتُبرت مؤشراً صحياً للاستعداد للابتكار، مما ينبغي أن يُعطى عموماً بعض المساحة والقدرات، بشكل مثالي في بيئة للحوسبة آمنة ومحمية. وتشمل الأفكار التي يمكن الاستفادة منها لتحقيق هذا الغرض إنشاء أو توسيع بيئات آمنة للابتكار الرقمي؛ وتحسين إبراز التطوير الموزع لتكنولوجيا المعلومات والاتصالات الذي تقوم به، في بيئات لامركزية، جهات التنسيق المحلية لتكنولوجيا المعلومات والاتصالات؛ وتعزيز تدريب المستخدِم النهائي وتدابير التوعية بتضمينها معلومات متينة وواضحة حول جوانب الأمن والمخاطر المتعلقة باستخدام خدمات جهات خارجية خارج نطاق الإجراءات والممارسات القياسية، إلى جانب معلومات حول البدائل المؤسسية المعتمدة، بالإضافة إلى توصيات للاستخدام الآمن لهذه الحلول.

ثالثاً- عناصر تساهم في تحسين القدرة على الصمود في المجال السيبراني

52- **القدرة على الصمود في المجال السيبراني كنتيجة لثقافة الأمن السيبراني.** بالإضافة إلى التأهب التكنولوجي الذي يتضمن تحديد الحلول الرقمية ومصادر البيانات لحماية الموارد المؤسسية، ينتج الموقف القوي للأمن السيبراني من نهج متعدد الأوجه يشمل جميع مستويات المنظمة، بما في ذلك الهيئات التشريعية والإدارية، وآليات الرقابة، والإدارة التنفيذية، والوحدات والبرامج الفنية أو وحدات وبرامج الأعمال، ومديرو البرامج، والقوى العاملة بشكل عام، وكذلك الشركاء المنفذين ومقدمي الخدمات الخارجيين. بعبارة أخرى، لا غنى عن نهج يشمل المنظمة بأكملها لتهيئة الظروف لتحسين القدرة على الصمود في المجال السيبراني. بالإضافة إلى ذلك، يشمل الأمن السيبراني عدداً من المجالات والكفاءات في المنظمة، بما في ذلك تكنولوجيا المعلومات والاتصالات، وإدارة المخاطر، والسلامة المادية والأمن، وإدارة المعلومات والمعرفة عموماً. ويمكن الإشارة إلى تعدد الاعتبارات وإدراك جميع أصحاب المصلحة لدورهم ومساهمتهم في رفع مستوى الأمن السيبراني بنجاح ضمن المنظمة على أنها مكونات لثقافة الأمن السيبراني التي تساعد، عند تأسيسها وممارستها، على تحقيق قدرة المنظمة على الصمود في المجال السيبراني. وفي هذا الفصل، يعرض المفتشون النتائج التي توصلوا إليها فيما يتعلق بمدى ما تعكسه أطر المنظمات المشارِكة وممارساتها من عناصر تسهم في تحسين القدرة على الصمود في المجال السيبراني (المنظور العمودي)، على النحو المعروض بشكل موجز في الشكل الرابع، كما يقترحون التحسينات الممكنة.

الشكل الرابع

العناصر التي تساهم في تحسين القدرة على الصمود في المجال السيبراني



المصدر: من إعداد وحدة التفتيش المشتركة.

ملاحظة: تُعرَّف القدرة على الصمود في المجال السيبراني في أحد المعايير الرائدة في الصناعة بأنها القدرة على توقع الظروف المعاكسة أو الضغوط أو الهجمات أو الخروقات في الأنظمة التي تستخدم الموارد السيبرانية أو يتم تمكينها بواسطة تلك الموارد، وعلى تحملها، والتعافي منها، والتكيف معها.

ألف- التعامل مع الهيئات التشريعية والإدارية

على الهيئات التشريعية والإدارية أن تقدم التوجيه الاستراتيجي وأن توفر الموارد

53- **يستحق الأمن السيبراني اهتمام الهيئات التشريعية والإدارية.** دأبت وحدة التفتيش المشتركة على القول إن للهيئات التشريعية والإدارية في المنظمات الحكومية الدولية دوراً حاسماً تؤديه في توفير التوجيه الاستراتيجي وتوفير الموارد الكافية لتمكين أية منظمة من تنفيذ الأنشطة المنوطة بها. وكما ورد في تقرير صدر مؤخراً عن وحدة التفتيش المشتركة حول الإدارة المركزية للمخاطر، يجب أن تُظهر الهيئات التشريعية والإدارية[13] مشاركتها وينبغي أن تكون على دراية، على الأقل، بالمخاطر الاستراتيجية الرئيسية التي تواجهها المنظمة المعنية وبالاستراتيجيات والأطر القائمة لإدارة تلك المخاطر. **ويرى المفتشون أن هذا ينبغي أن يشمل المشاركة والتوجيه في مجال الأمن السيبراني، بالنظر إلى طبيعته الحرجة كواحدة من مسائل إدارة المخاطر وكعامل تمكين رئيسي لتنفيذ ولايات المنظمات.** ويقترح الإطار 3 طرقاً ملموسة يمكن من خلالها زيادة مشاركة الهيئات المعنية ودعمها للجهود المؤسسية في هذا المجال. على أنه نظراً لأن الأمن السيبراني لا يزال يُنظر إليه كمسألة تقنية في الغالب، ما يجعله بالتالي مسألة تشغيلية وليست استراتيجية، فإن مدى دعوة الهيئات التشريعية والإدارية، لترسيخ مشاركتها في هذا الموضوع، أو مدى مطالبتها هي بذلك، كان حتى الآن محدوداً في معظم المنظمات.

الإطار 3

فرص مشاركة الهيئات التشريعية والإدارية في الأمن السيبراني

- صياغة بيان صريح حول درجة تحمل المخاطر وتقبلها في المنظمة فيما يتعلق بمسائل الأمن السيبراني يوضح مستوى المخاطر التي تعتبر مقبولة في سياق المنظمة المحدد. على أن الأدلة على وجود مثل هذه البيانات في المنظمات المشارِكة محدودة، فيما عدا برنامج الأمم المتحدة الإنمائي والمنظمة العالمية للملكية الفكرية، حيث نُفذت منهجية متطورة ومفصلة جيداً توضح درجة تقبل المخاطر.
- تقديم توجيهات إستراتيجية رفيعة المستوى بشأن مجالات الأمن السيبراني ذات الأولوية. ومن الأمثلة الجيدة على هذه التوجيهات القسم المتعلق "بأمن المعلومات" المدرج في استراتيجية تكنولوجيا المعلومات والاتصالات للأمانة العامة للأمم المتحدة، والتي أقرتها الجمعية العامة عام 2014 (A/69/517).
- تخصيص موارد مالية كافية استناداً إلى دراسة جدوى سليمة، تقدمها الإدارة التنفيذية، ومن شأن ذلك أن يمكّن من تنفيذ الأهداف المنصوص عليها في التوجيهات الاستراتيجية التي تقدمها الهيئات التشريعية والإدارية بما يتماشى مع درجة تقبل المخاطر.

54- **مشاركة العمل مع الهيئات التشريعية والإدارية في الممارسة العملية.** يختلف عمق ومستوى العمل مع الهيئات التشريعية والإدارية بشأن الأمن السيبراني، وهو اختلاف يستند إلى حد كبير على ولاية المنظمة ومتطلباتها التشغيلية. ولا يدرك إلا ما قلّ من المنظمات إمكانات العمل الفعال مع الهيئات التشريعية والإدارية في مسائل الأمن السيبراني، ناهيك عن استغلال تلك الامكانات. ومن بين هذه المنظمات القليلة، لم يفعل معظمها ذلك إلا بعد هجوم كبير استلزم مزيداً من الاهتمام والتفاعل على المستوى السياسي. وفي حين أن شكل هذا العمل يختلف بين المنظمات، وأنه لا يوجد مستوى أو قياس

(13) JIU/REP/2020/5.

وحيد "صحيح" لهذا التفاعل، هناك بالفعل بعض الاعتراف بأن تدفقاً معيناً للمعلومات بين المسؤولين عن الأمن السيبراني داخل المنظمة والأعضاء المكونين لها ليس مفيداً فحسب ولكنه قد يكون ضرورياً. ويميز المفتشون أدناه بين آليات الإبلاغ المنتظم بشأن الأمن السيبراني وبين الإجراءات التي يتعين اتباعها لتصعيد الحوادث إلى الهيئات التشريعية والإدارية.

آليات الإبلاغ والتصعيد

55- **آليات الإبلاغ القائمة.** وجد المفتشون أن أقلية من المنظمات أدرجت شكلاً من أشكال إبلاغ الهيئات التشريعية والإدارية الدوري عن مسائل الأمن السيبراني. ويتخذ هذا الإبلاغ، في حال وجوده، أشكالاً مختلفة: (أ) قد تقوم بعض المنظمات بإدراج المعلومات ذات الصلة في ميزانيتها البرنامجية وتقاريرها عن الأداء (عادةً كجزء من الفرع المتعلق بتكنولوجيا المعلومات والاتصالات، والذي قد يغطي، أو لا يغطي، الأمن السيبراني صراحةً)؛ و(ب) تشارك منظمات أخرى في إعداد تقارير مخصصة استناداً إلى طلب من الهيئة التشريعية ومجلس الإدارة، مثل تقديم التقارير لإبراز التقدم المحرز في تنفيذ الاستراتيجيات أو خرائط الطريق الموافق عليها أو المعتمدة؛ و(ج) على أن هناك منظمات أخرى تعتمد على التقارير السنوية لهيئاتها الرقابية الداخلية والخارجية، وتستخدمها كقناة أساسية للتدليل على وجوب زيادة الاهتمام بالموضوع.

56- **مقاييس الأمن السيبراني لا تُجمَع ولا تُعرَض بشكل منهجي.** هناك أيضاً تباين فيما يتعلق بمحتوى تلك التقارير المرفوعة إلى الهيئات التشريعية والإدارية، فقليل من المنظمات يقدم جوانب مختارة من المقاييس التي تجمعها وتحللها داخلياً فيما يتعلق بتعرضها وأدائها في مجال الأمن السيبراني. ويمكن من ناحية أن تكون هذه الممارسة غير المتكافئة في إعداد التقارير نتاجاً لترددٍ مشروع لدى العديد من المنظمات في إنشاء سجل عام أو حتى سري لمقاييس الأمن السيبراني قد يكشف أوجه الضعف وبالتالي يزيد من التعرض للمخاطر. ومن ناحية أخرى، قد تعكس هذه الممارسة الواقع المتمثل في أن المنظمات لا تزال تواجه صعوبات في تحديد المستوى الصحيح من تفاصيل المقاييس وفي انتقاء أهمها لأغراض الإبلاغ، فضلاً عن البتّ في مجموعة المقاييس الأجدى التي يتعين جمعها في المقام الأول. وتنتج غالبية المنظمات المشارِكة مقاييس تتعلق أساساً بتواتر حوادث الأمن السيبراني أو حدتها أو حجمها على مدار فترة زمنية معينة، وهي تجمعها للأغراض الداخلية، وهناك أيضاً بعض المنظمات التي لم تقم بعد بتأسيس مزيد من الأشكال المخصصة لجمع البيانات في هذا المجال أو إضفاء الطابع الرسمي عليها. على أن نوع البيانات التي تخضع للجمع والتحليل يختلف اختلافاً كبيراً من منظمة إلى أخرى، كما أن الطريقة التي تجري بها معالجة هذه البيانات بهدف توجيه عملية صنع القرار، سواء كانت داخلية أو على مستوى الهيئات التشريعية والإدارية، لم تُحدد بعد في كثير من المنظمات. ونظراً لأن هذه المقاييس توفر أحد المكونات الرئيسية التي يمكن للمنظمة على أساسها أن تحدد درجة تقبلها للمخاطر، **فإن المفتشين يعتبرون أن من الحصافة مواصلة دراسة مجموعات مختلفة من مقاييس الأمن السيبراني في المنتديات ذات الصلة ووضع منهجية أساسية يمكن تكييفها مع سياق كل منظمة حسب الحاجة.**

57- **التصعيد إلى الهيئات التشريعية والإدارية وفوائد الشفافية معها.** لا تبلِّغ الهيئات التشريعية والإدارية بشكل منهجي في حال وقوع حادث للأمن السيبراني، وهو ما يتضح من ردود المنظمات المشارِكة على استبيان وحدة التفتيش المشتركة. بالإضافة إلى ذلك، لاحظ المفتشون محدودية الأدلة على وجود عمليات تصعيد إلى الهيئات التشريعية والإدارية محددة مسبقاً بحيث يمكن الرجوع إليها عند تحقق ذلك الاحتمال. ويجري التعامل عادة مع قرار التصعيد على أساس كل حالة على حدة. وتشير تجربة تلك المنظمات التي أتيحت لها الفرصة، غالباً بسبب حدث سيبراني كبير، لاختبار قنواتها للتصعيد إلى الهيئات

الإدارية والتواصل معها إلى العوامل الرئيسية التالية التي يتعين النظر فيها للبتّ فيما إذا كان يتعين التصعيد: (أ) خطورة الحادث؛ و(ب) الأثر على العمليات؛ و(ج) الأثر على العمليات الحكومية الدولية؛ و(د) ما إذا كان من المرجح أن الحادث سيصبح معلوماً لدى الجميع. ومن الاعتبارات الحاسمة الأخرى توقيت التصعيد والتحوط لعدم الكشف عن أوجه ضعف أو تفاصيل معينة حول قدرة المنظمة على الاستجابة، مما قد يجتذب المزيد من الاهتمام إلى الهدف. وبشكل عام، اعتبر خبراء الأمن السيبراني الذين أجريت معهم المقابلات أن اللحظة المناسبة للتصعيد هي قبل التوصل إلى حل كامل للحادث، أو بالأحرى بمجرد التوصل إلى فهم كافٍ للمشكلة الجاري التعامل معها. وقد يكون التصعيد فور اكتشاف الاقتحام مبكراً جداً وينطوي على مخاطر تُعرّض جهود الحل الجارية للخطر، وبالتالي تزيد من التعرض عن غير قصد. وفي الوقت نفسه، فإن تأخير التصعيد إلى اللحظة التي يتم فيها حل الحادث بشكل كامل قد يلقي بظلال من الشك على مصداقية الإدارة التنفيذية أو استعدادها للتصرف بشفافية ولتحمل المسؤولية عن الثغرات المحتملة في الأمن السيبراني. أما الرسالة العامة التي ترسلها المنظمات المشارِكة التي "صارحت" هيئاتها التشريعية والإدارية فيما يتعلق بالحوادث وأوجه القصور في دفاعاتها السيبرانية فهي تتمثل في عدم الخوف من التواصل، نظراً لأن تضرر السمعة وكذلك فقدان ثقة الحكومات المانحة، يفوقان إلى حد كبير الإحراج المحتمل نتيجة للهجوم وأثره الضار – بما في ذلك أثره المالي غير المباشر.

58- **الحاجة إلى القيام مسبقاً بوضع بروتوكولات للتصعيد، سواء على المستوى الداخلي أو إلى الهيئات التشريعية والإدارية. ويرى المفتشون أن من الأهمية بمكان أن تُحدَّد مسبقاً الآلية التي سيتم من خلالها تصعيد الهجمات السيبرانية الكبيرة إلى اهتمام الهيئات التشريعية والإدارية.** نظراً لأن من الممكن استباق احتمال وقوع هذه الهجمات، فإنه يترتب على ذلك استباق استخدام بروتوكول للتصعيد أيضاً. وعلى وجه التحديد، فإن المعايير (ما الذي يؤدي إلى التصعيد) والآليات المتعلقة بتحديد الجهة التي يتعين عليها اتخاذ الخطوات اللازمة، وما هي هذه الخطوات، وترتيبها، ومن سيساهم بمدخلاته في ذلك، ينبغي ألا تخضع لعملية لاتخاذ القرار على أساس رد الفعل. فعملية اتخاذ القرار، إن تُركت للارتجال في وقت الأزمات الحادة، ستخضع لضغوط الاضطرار إلى العمل على احتواء الضرر على أساس مخصص بدلاً من الأخذ عموماً ببروتوكول ثابت مع التمتع بحرية التركيز على إدارة متغيرات حتمية خاصة بالحالة المواجَهة. وعلاوة على ذلك، فإن من شأن الاضطرار إلى ابتكار هذه الخطوات في ظل الأزمة أن يجعل العملية أكثر عرضة لتأثيرات غير مبررة في بيئة معقدة بالفعل ومن المحتمل أن تكون مُسيَّسة، وهي تأثيرات يمكن تجنبها إلى حد كبير من خلال النهج الاستباقي. وأخيراً، ودون المساس ببروتوكولات التصعيد التي وضعتها المنظمات داخلياً، قد يكون من الحصافة أن تنظر الهيئات التشريعية والإدارية في إجراء مناقشة حول قواعدها الخاصة بالتعامل مع أمور كهذه استباقاً لإحالة حالات خطيرة من الهجمات السيبرانية إليها من أجل التداول بشأنها والبتّ فيها. وقد يساعد هذا النهج التطلعي في وضع بعض الحدود المدروسة بعناية والمتفق عليها لإجراءات تتخذها الهيئات التشريعية والإدارية ويمكن أن تيسر إزالة التسييس واتخاذ القرارات السليمة في هذا المجال الذي يمكن أن يتصف بالحساسية.

باء- تضمين الأمن السيبراني في إدارة المنظمة للمخاطر

59- **فوائد نهج إدارة المخاطر إزاء الأمن السيبراني.** وصف تقرير أصدرته مؤخراً وحدة التفتيش المشتركة الإدارة المركزية للمخاطر بأنها عملية على مستوى المنظمة ككل لتحديد المخاطر وتحليلها وتقييمها ومعالجتها ورصدها، على أساس هيكلي ومتكامل ومنهجي، بهدف تحقيق أهداف المنظمة[14]. وتعكس الوظائف الأساسية المرتبطة بالأمن السيبراني (وهي عادة الأشكال المختلفة للتحديد والوقاية

(14) JIU/REP/2020/5.

والكشف والاستجابة والتعافي) المراحل والأهداف الرئيسية لإدارة المخاطر. كما أن التعامل مع الأمن السيبراني باعتباره مسألة خاصة بإدارة المخاطر على المستوى المؤسسي يحمل معه فوائد عملية ملموسة. على سبيل المثال، ونظراً للاعتراف بالأمن السيبراني كمصدر قلق استراتيجي على مستوى المنظمة ككل، فإنه يصبح مسألة تهم جميع وحدات الأعمال وجميع الموظفين، وهو يشجع ويدعم نهج المنظمة بأكملها والتقبل من خلال الملكية الموزعة للمخاطر. **علاوة على ذلك، يؤكد المفتشون أن تضمين الأمن السيبراني رسمياً في إطار الإدارة المركزية للمخاطر في المنظمة يساهم في الارتقاء بأولوية الموضوع بين الأولويات المختلفة في المنظمة ويوفر نقطة مرجعية رسمية تستند إليها الهيئات التشريعية والإدارية والإدارة العليا في رسم المسار بشكل مشترك لإدارة المخاطر الرئيسية بصورة أفضل.** ونظراً لأن هذه الأطر تصاغ عادة كوثائق حية، فإنها توفر أيضاً فرصة للقيام بشكل منهجي ومتكرر بإعادة النظر في تدابير التخفيف من المخاطر وتكييفها وتهيئتها في ضوء التطور السريع لاحتياجات المنظمة.

60- **يُعترف جزئياً بالفعل بنموذج إدارة المخاطر.** تعترف منتديات مختلفة بالفعل بفائدة النظر إلى الأمن السيبراني من خلال عدسة إدارة المخاطر، مع أن الآثار المترتبة على عرض الأمن السيبراني بهذه الطريقة لا تحظى، على صعيد الممارسة، بالفهم والاستيعاب بصورة كاملة في كثير من أنحاء المنظومة. وعلى سبيل المثال، تضمنت محاضر الندوات الأخيرة التي عقدها الفريق المختص بأمن المعلومات وحضرها خبراء الأمن السيبراني، عدة بنود على جدول الأعمال تتناول إدارة المخاطر، وشملت فيما شملته دعوة أعضاء الفريق للعمل مع ممثلين من منظماتهم عملوا في منتدى إدارة المخاطر التابع للجنة الإدارية الرفيعة المستوى، من أجل ضمان إدراج مخاطر الأمن السيبراني في المنظورات المساهمة في نموذج نضج المخاطر لدى المنتدى[15]. كما شددت لجان المراجعة والرقابة في عدة منظمات على الحاجة إلى إدراج اعتبارات الأمن السيبراني كجزء من أطر الإدارة المركزية للمخاطر والأطر الأعم الخاصة باستمرارية الأعمال. والواقع أن معظم المنظمات تناولت الأمن السيبراني كجزء من ولايتها في مجال الإدارة المركزية للمخاطر وشددت على الحاجة إلى مزيد من التكامل بين وظائف تكنولوجيا المعلومات والاتصالات وإدارة المخاطر. علاوة على ذلك، فإن المعايير الأحدث في مجال الأمن السيبراني، بما فيها معيار المنظمة الدولية لتوحيد المقاييس رقم 27001، وأهداف الرقابة للمعلومات وما يتصل بها من تكنولوجيا، وإطار عمل المعهد الوطني الأمريكي للمعايير والتكنولوجيا، تتعامل مع مخاطر الأمن السيبراني على أنها مخاطر على الأعمال تتجاوز بكثير نطاق البنية التحتية للحوسبة، وتؤكد على البعد الاستراتيجي لتحسين وضع الأمن السيبراني في المنظمات، مما يُعتبر أنه يتحقق على أفضل وجه عندما يرتبط بشكل كامل بإدارة المخاطر على المستوى المركزي.

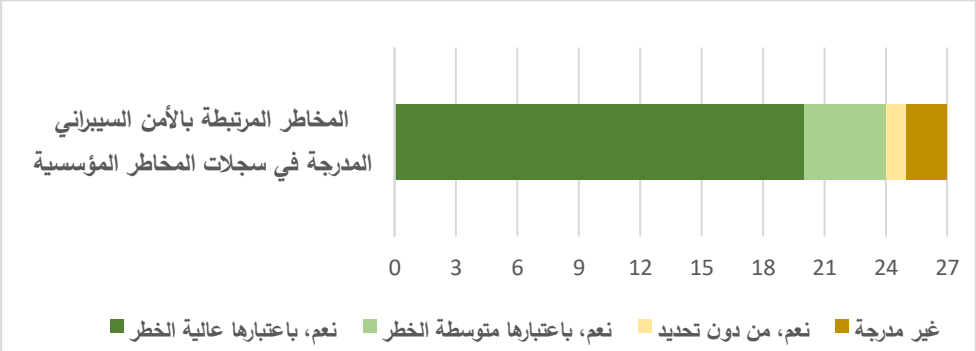
61- **الاهتمام بإدارة المخاطر في المنظمات المشارِكة.** تختلف درجة تبني الأمن السيبراني كمسألة تخص إدارة المخاطر بين المنظمات المشارِكة التي شملتها دراسة وحدة التفتيش المشتركة. فقد ذكرت الغالبية العظمى من المنظمات (24 من 27) في ردودها أن مخاطر الأمن السيبراني مدرجة رسمياً في سجل المخاطر المؤسسية. وأكد 20 من هذه المنظمات أن مستوى المخاطر المحدد للأمن السيبراني "مرتفع" (الشكل الخامس)، في حين أن 19 منظمة أدرجت تدابير محددة لتخفيف مخاطر الأمن السيبراني في سجل المخاطر المؤسسية. وزود 11 منظمة مشاركة فقط المفتشين بوثائق داخلية تتعلق بإدارة المخاطر، وقدمت لها، على اساس السرية، مقتطفات من سجلات المخاطر لديها. ونظراً لعدم اكتمال مجموعة البيانات، يجب اعتبار الاستنتاجات المستخلصة أولية. على أنه عند مقارنة بعض عينات سجل المخاطر المقدمة، يمكن ملاحظة بعض الاختلافات في تقييم مخاطر الأمن السيبراني وتصنيفها والتخطيط لها. فمن ناحية، ركزت بعض المنظمات على الجوانب الاستراتيجية، مثل التأثير المحتمل لحوادث الأمن

(15) CEB/2019/HLCM/DTN/02.

السيبراني على سمعة المنظمة وإنتاجيتها وتمويلها. وهناك، من الناحية المقابلة، أمثلة على تركيز سجلات المخاطر شبه الكامل على أمن تكنولوجيا المعلومات والاتصالات، مع التشديد أساساً على الحفاظ على توافر المعلومات بدلاً من سريتها وسلامتها. ويميل ذلك إلى تطلُّب تدابير أكثر تعقيداً من تلك الموجهة نحو تجنب الأعطال التقنية وتفادي "فترات التعطل" فقط، مما قد يفسر سبب معالجة هذه الجوانب بدرجة أقل في الوثائق المستعرضة. ويتمثل أحد عيوب سجلات المخاطر التي تضع بشكل أساسي الجوانب التقنية للأمن السيبراني في مركز الاهتمام، في أنها قد تفشل في الربط بين هذه العناصر والعواقب الأوسع بالنسبة للمنظمة.

الشكل الخامس

إدراج الأمن السيبراني في سجلات المخاطر المؤسسية، حسب عدد من المنظمات المشارِكة



المصدر: استبيان وحدة التفتيش المشتركة 2020.

62- **تدابير التخفيف تتطلب مزيداً من الاهتمام.** يتمثل أحد المجالات التي برزت، حتى مع محدودية البيانات المتاحة للمفتشين، في مستوى التفصيل في صياغة تدابير التخفيف من مخاطر الأمن السيبراني، إما ضمن إطار إدارة المخاطر أو خارجه. وكما أوضحت لجان المراجعة والرقابة، غالباً ما تكون تدابير التخفيف وصفية للوضع القائم (على سبيل المثال، العرض التفصيلي للتدابير المعمول بها بالفعل، بدلاً من تحديد إجراءات استباقية يؤخذ بها في حال التعرض لمخاطر محددة)، مما يؤدي إلى عملية خدمة الذات في تحديد أهداف تحققت بالفعل سعياً وراء تحسين التقارير، بدلاً من بذل جهد جاد لاستنباط إجراءات للتخفيف تستخدم كمعيار يقاس به التنفيذ التدريجي. وإدراكاً لأن بعض المنظمات ربما اختارت عمداً عرض تدابيرها الخاصة بالتخفيف بعبارات غير محددة بغية حماية دفاعاتها، **يرى المفتشون أن التركيز في المستقبل ينبغي أن ينصب على صياغة تدابير التخفيف بطريقة تطلعية بحيث تستمر في عكس القيود وأوجه الضعف القائمة، مع الاعتراف بأن ذلك يمكن أن ينطوي على جهد إضافي لبلوغ الأهداف المحددة حديثاً وكذلك على فترة انتقالية للإبلاغ قد تكشف عن الأهداف التي لم تتحقق بالكامل.**

63- **خرائط الطريق.** في بعض المنظمات، أدت تقييمات مخاطر الأمن السيبراني إلى اعتماد خارطة طريق مؤسسية لتحسين قدرة المنظمة على الصمود في المجال السيبراني، أعدتها الإدارة مستفيدة من تعقيبات من جميع أصحاب المصلحة الداخليين المعنيين، وعُرضت في كثير من الحالات على الهيئات التشريعية أو الرئاسية لإقرارها. ووجد المفتشون أن لخرائط الطريق هذه فائدة أكبر عندما تكون مصممة كخطة متعددة السنوات مرتبطة بمعايير للتنفيذ ومؤشرات للإنجاز، ومصحوبة بتحول في تخصيص الموارد لضمان التمكن من تنفيذ تدابير التخفيف في الممارسة العملية. وكانت عمليات وضع خرائط الطريق تلك، وقت صياغة هذا التقرير، قد اكتملت أو كانت جارية في عدة منظمات (منظمة الطيران المدني الدولي، ومنظمة الأغذية والزراعة للأمم المتحدة، وصندوق الأمم المتحدة للسكان، ومفوضية الأمم المتحدة لشؤون

اللاجئين، ومكتب الأمم المتحدة لخدمات المشاريع، والمنظمة العالمية للملكية الفكرية)، واعتُبرت ممارسة جيدة لتعميم جهود التحسين على المنظمة ككل.

64- **الانتقال من الوعي بالمخاطر إلى إدارتها الاستباقية.** في الختام، في حين أن العديد من المنظمات المشارِكة أدركت أهمية اعتبارات الأمن السيبراني وحاولت تضمينها، بدرجات متفاوتة من التفصيل، في أطرها لإدارة المخاطر الأوسع، فإن الصورة الشاملة على مستوى المنظومة لا تزال متفاوتة وتتطلب مزيداً من الاهتمام للانتقال من مجرد الوعي بمخاطر الأمن السيبراني لإدارتها حقاً وفقاً لمتطلبات كل كيان، مع الاعتراف بأنه لا يمكن في هذا المجال التخلص من جميع الأخطار. **ولذلك يتفق المفتشون مع ما يطالب به خبراء الأمن السيبراني من وجوب توخي الحذر، ويكررون القول به: فالمخاطر كبيرة، والمطلوب أن يؤخذ بالنهج القائم على المخاطر (المرفق الثاني).** ويتعين أن ينصب التركيز في المستقبل على وضع تدابير فعالة مفيدة للتخفيف من المخاطر بالاقتران مع التخطيط المتين لاستمرارية الأعمال. وتكتسي مساهمة خبراء الأمن السيبراني في العمليات الداخلية لإدارة المخاطر ومشاركتهم الكاملة فيها، من التصميم إلى التنفيذ والرصد، أهمية بالغة لتحقيق هذه الأهداف.

جيم- البناء على التقارب بين الأمن المادي والأمن السيبراني

65- **عدم وضوح الخطوط الفاصلة بين الأمن المادي والأمن السيبراني.** في وقت مبكر، وحتى أثناء مرحلة وضع المفاهيم الخاصة بهذا الاستعراض، ظهر السؤال الفلسفي إلى حد ما حول ما إذا كان الأمن السيبراني في الغالب يعتبر مسألة "سيبرانية" – أي مسألة تحركها التكنولوجيا – أو أنه مسألة أمنية (تتشابه مع السلامة المادية والأمن ولكنها نُقلت إلى العالم الرقمي)، وأثار هذا السؤال نقاشاً ثرياً بين أصحاب المصلحة الذين قابلهم المفتشون. ومع أن مؤسسات منظومة الأمم المتحدة تعاملت تقليدياً مع السلامة المادية والأمن والأمن السيبراني كمجالين منفصلين، فإن كلاهما معني بحماية العاملين في المنظمات وبالحفاظ على أصولها. وتحقيقاً لهذه الغاية، تُعنى كلتا الوظيفتين بإدارة عدم اليقين أو المخاطر من خلال توقع ما يجب القيام به في مواجهة الهجوم واتقائه ومعرفته، مما يجعل إدارة المخاطر قاسماً مشتركاً يربط بين المجالين. كما يشترك الأمن المادي والأمن السيبراني في فهم أنه حتى أفضل تدابير الحماية لن تمنع الهجمات تماماً من اختراق دفاعات المؤسسة، بغض النظر عن مدى تفصيلها أو قوتها. أخيراً، عند استحضار السيناريوهات التي قد توضح أين ينتهي الأمن السيبراني ويبدأ الأمن المادي، أو العكس بالعكس، سرعان ما أصبح واضحاً أن الفصل بين المجالين المادي والرقمي قد لا يكون سهلاً كما قد يبدو للوهلة الأولى.

66- **يتقاطع الأمن المادي والأمن السيبراني في الممارسة العملية.** في الوقت الحالي، تُعدّ الأنظمة التي تدعم وظيفة السلامة والأمن والتي تعمل دون الاعتماد، بشكل ما، على استخدام تكنولوجيا المعلومات والاتصالات، هي الاستثناء وليس القاعدة. ونتيجة لذلك، يُرجح أن تتحقق عواقب انتهاكات الأمن السيبراني التي تؤثر على هذه الأنظمة في العالم المادي، وأحياناً إلى درجة تعريض حياة الأشخاص أو سلامتهم الجسدية لخطر كبير. ولا يوجد نقص في الأمثلة على السبل التي يتقاطع بها الأمن السيبراني والأمن المادي في الممارسة العملية. فعلى سبيل المثال، قد يسيطر القراصنة الحاسوبيون على بوابة أمنية، ويستغلون أوجه الضعف في بروتوكولات الأمان لزرع برمجيات للتجسس على الأجهزة الإلكترونية أو لتنزيل معلومات سرية على أجهزة محمولة، ويتمكنون من الوصول عبر الإنترنت إلى مخططات طوابق المكاتب بهدف دراسة أفضل هدف لهجوم مسلح، أو يقومون بسرقة الهوية الافتراضية بقصد الدفع بالآخرين إلى مواقف تنتهي بهم إلى تعريض أنفسهم للخطر عن غير قصد من خلال الاعتماد على معلومات من مصادر موثوقة عادة ولكنها باتت منتحلة احتيالياً من قبل مجرمي الفضاء السيبراني.

بالإضـــافة إلى ذلك، قد يكون للتدابير الأمنية التي يســـهل اختراقها والتي تهدد حماية المباني أو مراكز البيانات أو غرف الخوادم أو نقاط الوصول الرقمية، من الدخول غير المصرح به أو من أشكال أخرى من التدخل غير المأذون به الناجم عن أخطار مادية (طبيعية أو من صـنع الإنسـان)، تأثير سـلبي مباشـر يمكن الشـعور به في المجال الرقمي. ويظهر التقارب بين العالمين بصـورة أشـد وضـوحاً في المواقع الميدانية، والتي تميل إلى الابتعاد عن الآليات المركزية لمراقبة الأمن السـيبراني وعن الرصـد المركزي، بينما هي في الوقت نفسـه هدف محتمل أكثر جاذبية نظراً لأن المعلومات المحفوظة مهمة بشكل مباشـر لســلامة الأرواح وللســلامة الجســدية. ومن الأمثلة على ذلك البيانات المتعلقة بمكان تواجد العاملين أو حركتهم في مناطق أقل حماية.

67- **لا تزال الروابط المؤسـسـية بين الأمن المادي والأمن السـيبراني متفرقة.** كشـفت الردود على استبياني وحدة التفتيش المشتركة والمقابلات اللاحقة مع المسؤولين عن التفاوت بين المنظمات المشارِكة في إدراك الروابط بين المجال المادي والعالم السـيبراني. ويعكس الهيكل المؤسـسـي لمنظمتين فقط تكاملاً فعلياً بين إطاري السـلامة المادية والأمن وإدارة الأمن السـيبراني، إما من خلال وضـع الوظيفتين في إدارة واحدة بمســؤولية مشــتركة أمام نائب للمدير التنفيذي يتولى الولاية الأمنية العامة في المنظمة (المنظمة العالمية للملكية الفكرية)، أو من خلال الصـياغة الاسـتراتيجية لكلتا الوظيفتين كمسـاهمتين بين كثير من المسـاهمين في "إطار أوسـع لإدارة قدرة المنظمة على الصـمود" يجمع بين الدفاعات الموجهة ضـد جميع أنواع التهديدات، سواء كانت مادية أو رقمية أو سياسية أو طبيعية أو غيرها (الاتحاد الدولي للاتصالات). وتقرّ منظمات أخرى بأن هناك أوجه تقارب وتآزر يمكن اكتسابها، وقد أضفت الطابع الرسمي على تنسيق المعلومات وتبادلها بين الوظيفتين إلى حد ما، على سـبيل المثال من خلال التسـلسـل الإداري المزدوج، أو الإحاطات المشــتركة المقدمة للإدارة العليا، أو المشــاركة في الاجتماعات، أو من خلال جعل كلتا الوظيفتين تسـاهمان على قدم المسـاواة في العمليات المؤسـسـية من قبيل إدارة المخاطر أو التخطيط لاستمرارية الأعمال، أو على أساس مخصـص في حالات الاسـتجابة للطوارئ التي تتطلب مدخلات من كليهما. كما ينفذ بالفعل التعاون بشــأن تدابير محددة على المســتوى التشــغيلي (مثل توحيد المعلومات المتعلقة بالتهديدات السـيبرانية والمادية لأغراض التحذيرات الخاصـة بالسـفر الرسـمي، أو الاشـتراك في ابتكار حلول تكنولوجية متطورة لتحديد هوية الموظفين وبطاقات الدخول إلى أماكن العمل)، مما يحقق بعض الفوائد الملموسة للوضـع الأمني للمنظمات المعنية. وحتى في أجزاء من المنظومة يُعتبر فيها مجال السـلامة المادية والأمن متميزاً وغير معني عموماً بالفضـاء السـيبراني، قدمت المنظمات أدلة على وجود اتصـالات عرضـية وغير رسـمية بين المجالين. على أنه، بالنسـبة لغالبية المنظمات التي شـملتها الدراسـة يتمثل الواقع في أن الصـلة بين الأمن المادي والأمن السيبراني تبقى أقل من قيمتها الحقيقية أو لا يعترف بها إلا بشكل هامشي، وهذا هو الحال أيضاً على مستوى المنظومة بأكملها (الفقرات 159-164).

68- **الارتقاء بمهارات قدرات الأمن السـيبراني ضـمن وظيفة السـلامة المادية والأمن.** في رأي المفتشـين، هناك إمكانية للبناء على التقارب بين الأمن المادي والأمن السـيبراني لصـالح كلا المجالين ولفائدة قدرة المنظمة على الصـمود على نطاق أوسـع. ويتمثل أحد الخيارات في اسـتكشـاف إمكانية بناء القدرات الداخلية من خلال الارتقاء بمهارات مؤهلات عدد كبير من مختصـي السـلامة والأمن وتوسـيعها وإدراج جوانب الأمن السـيبراني في مجموعة مهارات المختصـين في المسـتقبل، ولا سـيما من خلال إعادة التفكير في طريقة وضـع التوصـيفات الوظيفية الحالية (على سـبيل المثال، زيادتها بعناصـر معالجة المعلومات الاسـتخبارية الخاصـة بالتهديدات السـيبرانية، ووضـع نماذج التهديدات، وما شـابه ذلك من القدرات التحليلية). وقد يكون للتصـور القائل إن الأمن السـيبراني بطبيعته غير مرتبط بواجبات هؤلاء المهنيين ومنفصـل عنها ما يبرره جزئياً في الممارسـة الطويلة الأجل المتمثلة في تجنيدهم في المقام الأول من بين قوات الشرطة والقوات العسكرية – على أن هذه الفكرة لا تدرك أن تلك القوات نفسها طورت بالفعل

قدرات حديثة في المجالات المطلوبة. فالخبراء موجودون وهم متاحون بسهولة أمام مؤسسات منظومة الأمم المتحدة لتعيينهم. وهذه القدرة الإضافية، عند بنائها، لن تحل محل الآلية المتقدمة والمجهزة جيداً والمتمثلة في القوى العاملة التقليدية الحالية المهتمة بالأمن، بل ستكملها وستمكنها من التفاعل بشكل أكثر فعالية مع قدرات الأمن السيبراني المكرسة داخل مؤسسات منظومة الأمم المتحدة المعنية. ويدرك المفتشون أن المجالين يتمتعان بقدرات متمايزة وعالية التخصص ومبنية جيداً لخدمة أهداف الحماية الخاصة بكل منهما، وبالتالي، فإن محاولات دمجهما في هيكل واحد أو دمج أحدهما في الآخر لا تبدو حصيفة دون مزيد من الدراسة. على أن جهود توسيع القدرات الحالية لتحسين الروابط بين المجالين يمكن أن تكون أحد العناصر التي ينبغي استكشافها، بهدف تحقيق نهج أكثر شمولية لحماية عاملي المنظمة وأصولها، على النحو المتوخى في التوصية 5.

دال- تشكيل الأطر التنظيمية للامتثال والمساءلة

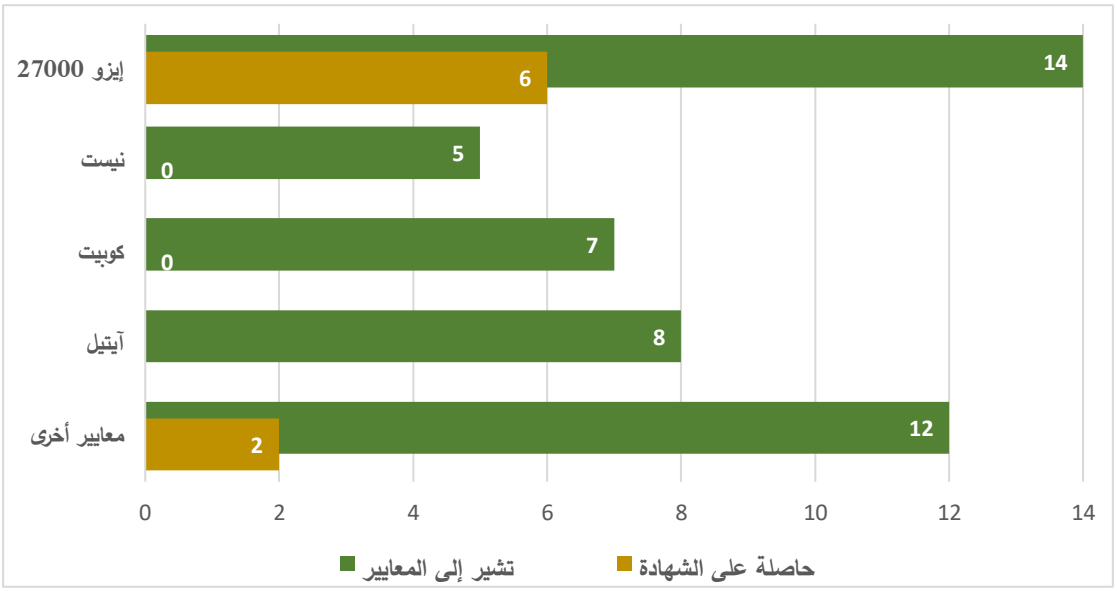
معايير الصناعة فيما يتعلق بأمن المعلومات

69- **المعايير التي تستخدمها المنظمات المشارِكة.** الأمن السيبراني مجال طُوِّر له عدد من المعايير الوطنية والدولية للصناعة، وتوفر هذه المعايير التوجيه ومقاييس الأداء بهدف بناء أنظمة لإدارة أمن المعلومات قادرة على الصمود. ويشير المصطلح، الذي وضعته المنظمة الدولية لتوحيد المقاييس، إلى مجموع التدابير – الإدارية والتنظيمية والتكنولوجية – التي تعكس نهج الكيان المعني إزاء الأمن السيبراني. وهو يتألف من مجموعة معقدة من الضوابط، تتراوح من القواعد ووثائق السياسة إلى أدوات الإدارة وعملياتها، ومفاهيم الأمن، واستراتيجيات إدارة المخاطر، من بين أمور أخرى. وأشارت المنظمات المشارِكة إلى مجموعة واسعة من هذه المعايير، وأحياناً إلى أكثر من مجموعة واحدة، وأوضحت أنها اختارتها على أساس ملاءمتها للبيئة والمتطلبات المحددة لكل منظمة، وقد استمر تنقيحها من خلال تسجيل الضوابط الخاصة بمعيار معين الأكثر صلة في "بيان انطباق" مهيأ خصيصاً. ويذكِّر المفتشون أنه منذ عقد مضى، في عام 2011، أيدت شبكة تكنولوجيا المعلومات والاتصالات قيام وكالات منظومة الأمم المتحدة باتباع معيار المنظمة الدولية لتوحيد المقاييس رقم 27001[(16)]، وفي عام 2017، أعاد الفريق المختص بأمن المعلومات التأكيد على هذا الموقف. ويؤكد الاستعراض الحالي أن معظم مؤسسات منظومة الأمم المتحدة إما حصلت بالفعل، أو تخطط للحصول، على شهادة بموجب المعيار رقم 27001، أو اختارت مواءمة إطارها معه على أساس طوعي دون أن تسعى للحصول على شهادة رسمية. وإلى جانب ذلك المعيار، توجد عدة معايير أخرى تستخدمها مؤسسات منظومة الأمم المتحدة، وهي مدرجة في الشكل السادس أدناه ويرد وصفها بمزيد من التفصيل في المرفق الثالث. وهناك ثلاث منظمات فقط لم تشر إلى أية معايير أو لم ترسل معلومات في هذا الصدد.

(16) CEB/2011/HLCM/ICT/16.

الشكل السادس

معايير الصناعة الرئيسية التي تستخدمها المنظمات المشارِكة في وحدة التفتيش المشتركة



المصدر: استبيان وحدة التفتيش المشتركة (2020) والمقابلات.

المختصرات: نيست (NIST)، المعهد الوطني الأمريكي للمعايير والتكنولوجيا؛ كوبيت (COBIT)، أهداف الرقابة المتعلقة بتكنولوجيا المعلومات والتكنولوجيات المتصلة؛ آيتيل (ITIL)، مكتبة الهياكل الأساسية لتكنولوجيا المعلومات.

70- **الحصول على شهادة رسمية في مقابل الإشارة إلى المعايير**. فيما يتعلق بفائدة الشهادات الرسمية بالمقارنة بأشكال الامتثال الطوعي الأكثر مرونة، وجد المفتشون تبايناً بين آراء الخبراء. والواقع أن التماس الشهادة قرارٌ إداري يوفر وسيلة لطمأنة الهيئات التشريعية والإدارية فضلاً عن الشركاء الخارجيين بصورة موثوقة، استناداً إلى شكليات عملية الاعتماد وبيان الشهادة، فضلاً عن الصرامة التي يحققها اشتراط إجراء مراجعات مستقلة سنوياً للحفاظ على الشهادة. كما قد تكون الشهادة أداة لتحريك الابتكار على أساس متكرر، نظراً لمتطلبات التدليل على التحسين المستمر. وفي الوقت نفسه، تحتج بعض المنظمات بأن الشهادة قد تكون على درجة من التكلفة والتفصيل عالية بحيث أنها لا تبرر الاستثمار. كما تنتقد هذه المنظمات شدة اعتماد الشهادات على الامتثال الرسمي، مما قد يدفع إلى تقديم تقارير إيجابية بدلاً من التقارير الواقعية. ويقر المفتشون بأن الحصول على الشهادة والمواءمة مع المعايير يمكن أن يكونا خيارين مفيدين، لا سيما في مراحل مختلفة من النمو التدريجي للدفاع السيبراني. وهذا صحيح بشكل خاص لأنه يمكن استخدام المعايير بطرق مختلفة، بما في ذلك كمقياس أو إطار عمل لأغراض المراجعة، أو كخارطة طريق داخلية للتحسين الذاتي، أو كحافز إضافي للامتثال للضوابط، أو كمصدر إلهام أو أداة مرجعية لنُهج مهيأة خصيصاً وفقاً للاحتياجات.

71- **فوائد الإشارة إلى المعايير**. يمتنع المفتشون عن الدفاع عن الأخذ بمعيار صناعي معين أو اتباع نهج منسق على نطاق المنظومة ككل في هذا الشأن، لأن المعايير المختلفة قد تخدم بشكل صحيح أغراضاً مختلفة وتوفر خيارات مناسبة لمستويات متباينة من النضج. وعلى هذا فإنه لا يوجد معيار واحد صحيح ولا نهج واحد صحيح للأمن السيبراني، ولكن هناك ما يدلل بقوة على وجوب استلهام معايير الصناعة ذات الصلة – سواء بشكل رسمي أو غير رسمي – عند إعداد الإطار التنظيمي وإدارته. لذلك يجب على المنظمات المشارِكة تحديد المعيار المناسب، ومن ثم، في إطاره، الضوابط الأكثر صلة استناداً إلى مستوى الحماية الذي يقتضيه وضعها، وفقاً للمتطلبات والمخاطر المحددة على أساس تقييمات مخاطر الأمن السيبراني الخاصة بكل منظمة. ويلاحظ المفتشون، دون إصدار حكم على ذلك، أن القرار المؤسسي

في هذا المجال قد يأتي بآثار على مستوى المنظومة أيضاً، إذ أن استخدام نفس الإطار أو المعيار يمكن أن يؤدي إلى تيسير المقارنة وتوفير لغة مشتركة بين الجميع. وفي المقابل فإن تنوع النُهج يمكن أن يوفر، في سياق الآليات المشتركة بين الوكالات، فرصاً إضافية للنقاش عبر المنظمات، ولاختبار الافتراضات، ولإجراء فحص أكثر انتقاداً لخيارات المنظمة مقابل خيارات المنظمات الأخرى، وللتعلم المتبادل بشكل عام، مما يفيد المنظمات بشكل فردي في نهاية المطاف.

أطر السياسات والإجراءات

72- **يقع الحق في إنشاء الإطار التنظيمي المناسب ضمن اختصاص كل كيان.** فالتوجيهات الموثوقة القابلة للتطبيق عالمياً حول سبل تنظيم مسائل الأمن السيبراني ليست متاحة بسهولة بخلاف مجموعة معايير الصناعة المتنوعة المذكورة أعلاه. ويمكن أن يُعزى عدم وجود صك قانوني أو إطار عمل دولي في هذا المجال إلى حقيقة أن المجال نفسه متعدد الأوجه ويصعب رسم حدوده، وهو بالتالي يطرح تعقيدات على التنظيم، حتى في سياق القانون المحلي لأي دولة لوحدها. ومع الارتقاء بهذه التعقيدات إلى مستوى الساحة الدولية، تتزايد صعوبة تحديد إطار مشترك يحكم العلاقات بين الدول وكذلك بين أصحاب المصلحة الآخرين العاملين في الفضاء السيبراني في القطاعين العام والخاص. وفي الوقت هذا، لا يوجد صك ملزم قانوناً في القانون الدولي ولا إطار معياري واحد لمؤسسات منظومة الأمم المتحدة لتنظيم الأمن السيبراني تحديداً. ونتيجة لذلك، يتمثل الوصف الأفضل لإطار الحوكمة الدولي للفضاء السيبراني في أنه خليط من المؤسسات والقواعد الرسمية وغير الرسمية المكونة من معايير تقنية وعقود وقوانين وقرارات حكومية دولية متقاطعة ومتداخلة. ونظراً لعدم وجود إطار عمل متسق يمكنه أن يقوم بدور النموذج، فإن كل كيان يحتفظ بالحق – ضمن حدود المعايير التي تمليها وثيقته التأسيسية وما يتصل بذلك من قرارات الهيئات التشريعية والإدارية – في صياغة قواعده الخاصة ضمن استقلاله النسبي وفي اختيار ما سيكون عليه مخططه الرئيسي للأمن السيبراني.

73- **تشير استراتيجيات تكنولوجيا المعلومات والاتصالات بشكل روتيني إلى الأمن السيبراني.** هناك تنوع في أساليب تغطية الأمن السيبراني في الأطر التنظيمية الحالية، وبمعنى آخر البيئة المعيارية التي تعمل من خلالها وظائف المنظمة، فهي تميل إلى عرض التطور التاريخي للأمن السيبراني كمجال نشأ في ميدان تكنولوجيا المعلومات والاتصالات ونما ليصبح تخصصاً متميزاً. وليس هناك إلا قلة من المنظمات التي تعبر عن الأمن السيبراني بشكل مستقل تماماً عن تكنولوجيا المعلومات والاتصالات، وتعامله على أنه مسألة منفصلة في حد ذاتها وعلى قدم المساواة مع الأمن المادي (المنظمة العالمية للملكية الفكرية) أو كجزء من رؤية أوسع لإدارة قدرة المنظمة على الصمود (الاتحاد الدولي للاتصالات)، فهذه الأساليب تبقى هي الاستثناء. وقد وضع معظم المنظمات المشارِكة وثيقة استراتيجية مؤسسية متعددة السنوات تعرض رؤيتها في مجال تكنولوجيا المعلومات والاتصالات، وتتضمن في غالبيتها العظمى، اعتبارات خاصة بالأمن السيبراني. ومع ذلك، فإن بعض هذه الاستراتيجيات لا يحتوي إلا على إشارة مرجعية أساسية تُستكمل أحياناً بتوجيهات أكثر تفصيلاً على المستوى الأدنى، في حين أن بعضها الآخر يتضمن فصولاً كاملة مكرسة لهذا الموضوع. **وبغض النظر عن درجة التفصيل في توجيهات الأمن السيبراني ضمن استراتيجيات تكنولوجيا المعلومات والاتصالات الأوسع لدى المنظمات، فإن المفتشين يعتبرون أن وجود إشارات مرجعية إلى الموضوع في استراتيجيات تكنولوجيا المعلومات والاتصالات هذه يشكل خطوة إيجابية أولى.**

74- **تتوفر سياسات محددة في مجال الأمن السيبراني، أو يجري العمل على وضعها، في كثير من المنظمات المشارِكة.** تجدر الإشارة إلى أن الوثائق الأساسية لعدد من المعايير الرائدة في الصناعة تتطلب

وجود سياسات محددة وإجراءات موثقة للأمن السيبراني كركيزة أساسية للضوابط التي يقوم عليها نظام إدارة أمن المعلومات في الكيان المعني[17]. وقد وجد الاستعراض الحالي أن كثيراً من المنظمات أصدرت توجيهات مكرسة كهذه، وأن المنظمات التي لم تفعل ذلك، مع استثناءات قليلة، تعمل حالياً على وضعها. وبشكل أكثر تحديداً، هناك ما يدلّ على أن 17 منظمة قد وضعت صكوكاً تنظيمية خصيصاً للأمن السيبراني (ثلاثة منها قيد التنقيح حالياً)، بينما أكدت 4 منظمات أنها في طور وضع سياسات جديدة. وهناك ثلاث منظمات فقط أفادت بأنها لم تُصِغ ولم تبدأ في صياغة سياسات أو تنظيمات محددة للأمن السيبراني وذكرت أنها تعتمد على سياسات وإجراءات تكنولوجيا المعلومات والاتصالات لديها لتناول هذه المسألة. ومع استثناءات قليلة، يمكن القول إن المنظمات أدركت أهمية وجود إطار مرجعي مفصل لتوجيه نهجها إزاء الأمن السيبراني. ويدرج المرفق الرابع الصكوك الرئيسية التي تحكم الأمن السيبراني ضمن الإطار التنظيمي للمنظمات المشارِكة.

75- **الأطر معقدة بشكل عام وغير متجانسة ومتعددة الطبقات.** بغض النظر عما إذا كانت المنظمات المعنية قد وضعت أطراً تنظيمية أكثر تفصيلاً للأمن السيبراني أو ما إذا كانت تشير إلى تلك المطبقة على تكنولوجيا المعلومات والاتصالات بشكل عام، فإن الأطر التي واجهها المفتشون تميل إلى أن تكون مبعثرة عبر مجموعة من الوثائق التوجيهية الاستراتيجية والسياساتية والإجرائية والتقنية. وتختلف بين المنظمات المشارِكة المصطلحاتُ المرتبطة بهذه الوثائق، بدءاً من الاستراتيجيات إلى بيانات المهمة، ومن السياسات إلى التعليمات الإدارية، ومن الإجراءات التشغيلية الموحدة إلى المبادئ التوجيهية، ومن "الكتيبات الدليلية" إلى البروتوكولات، وكثيراً ما تكون هذه المصطلحات متداخلة من الناحية المفاهيمية أو حتى مستخدمة كمترادفات. وقد وضع مركز الأمم المتحدة الدولي للحوسبة نموذجاً يمثل المكونات المعيارية المختلفة لنظام إدارة أمن المعلومات على شكل طبقات، ويعكس أعلى مستوى من التجريد في الجزء الأعلى منه وأوسع مستوى من التفصيل في الجزء السفلي منه، وهو نموذج دعم عدداً من مؤسسات منظومة الأمم المتحدة في تقييم أطر التنظيمات والحوكمة القائمة وتحسينها. واستناداً إلى هذا النموذج، يقدم المرفق الرابع لمحة عامة عما يصادف من أهداف وقوالب ومحتوى نموذجي في وثائق المنظمات المتعلقة بالأمن السيبراني وتكنولوجيا المعلومات والاتصالات والتي استعرضها المفتشون، مع التسليم بأن التحليل النوعي المفصل للمحتوى عبر جميع المنظمات المشارِكة يتجاوز نطاق هذا الاستعراض.

76- **التكييف حسب السياق، والاستعراض الدوري.** يمكن لضمان أن تعكس السياسات خصوصيات المنظمة أن يشمل تكييفها بحيث تتفق مع الضوابط الدقيقة التي تتطلبها معايير الصناعة التي اختارت المنظمة اتباعها، في حال انطباق ذلك. وقد وجد المفتشون مثالاً على ذلك في برنامج الأغذية العالمي وبرنامج الأمم المتحدة الإنمائي، حيث يوجد، لكل ضابط تقني اختارته المنظمة من ضوابط المعيار رقم 27001 لتضمينه في "بيان قابلية التطبيق" لديها، بيانُ سياسة مقابل في إطار التنظيمات لديها. كما يمكن أن يشمل ذلك تنظيم مجالات الاهتمام الخاص التي قد تكون أكثر صلة ببعض المنظمات من غيرها، مثل التوجيهات الخاصة بالممارسات الآمنة لإنشاء موقع شبكي داخلي أو قاعدة بيانات أو تطبيقات. وعلى هذا فإنه يمكن التوصل إلى تفسير صحيح، على الأقل جزئياً، لما لوحظ من تنوع في السياسات ومن فوارق في وضع الأطر التنظيمية، من خلال تكييفها حسب سياق واقع المنظمة، بدلاً من الإشارة إلى عدم وجود نهج منهجي للتنظيمات. علاوة على ذلك، فإن من الأهمية بمكان في مجال الأمن السيبراني

(17) يبدأ معيار المنظمة الدولية لتوحيد المقاييس 27001، في قائمته المعيارية لأهداف الرقابة، بالضابط ألف-5 المعنون "سياسات أمن المعلومات"، مشيراً إلى أنه ينبغي وضع مجموعة من السياسات وإبلاغ الموظفين والأطراف الخارجية ذات الصلة بها. ويحدد المعهد الوطني الأمريكي للمعايير والتكنولوجيا، في وثيقته الأساسية "إطار تحسين الأمن السيبراني للبنية التحتية الحرجة"، كجزء من فئة الحوكمة، أن "السياسات والإجراءات والعمليات" تهدف إلى إرشاد "إدارة مخاطر الأمن السيبراني".

السريع التطور أن تظل التوجيهات المعيارية قابلة للتكييف وذات صلة، وهو ما سعت بعض المنظمات إلى تحقيقه من خلال إخضاع التوجيهات لاستعراض دوري. وفي هذا الصدد، يمكن القول بأن من حسن الممارسة أن تُدرَج في وثائق التوجيهات وفي السياسات أطرٌ زمنية صريحةٌ لإجراء الاستعراض والتنقيح رسمياً حسب الضرورة، مع إرفاق ذلك بمؤشرات تبين الجهة المسؤولة عن بدء هذه العملية.

77- **لوجود التوجيهات أهميته بغض النظر عن نطاقها أو درجة التفصيل فيها أو بيئة المنظمة ذات الصلة.** نظراً للتنوع الكبير في المسائل المتعلقة بالأمن السيبراني والتي يمكن إخضاعها للتنظيمات، فإن من الصعب تحديد الأنواع الدقيقة للسياسات أو الإجراءات التي من شأنها أن تدعم على النحو الأمثل إطار عمل قوي للأمن السيبراني، ناهيك عن عرض تلك السياسات والإجراءات. ويكفي أن نقول إن وجودَ توجيهات أساسية في هذا المجال، وهو مجال غالباً ما يكون تقني للغاية ومتعدد الأوجه، مهمٌ لضمان التماسك والاتساق في تطبيق التدابير الأمنية، بغض النظر عن حجم المنظمة أو الموارد المتاحة لها.

تعميم الأمن السيبراني

78- **التعميم.** سيكون من قصر النظر التوقف فقط عند السياسات الخاصة بتكنولوجيا المعلومات والاتصالات والأمن السيبراني عند وضع إطار تنظيمي يحقق للمنظمة قدرة أكبر على الصمود في المجال السيبراني. فالحفاظ على الدفاعات السيبرانية لمنظمة ما هو مسؤولية مشتركة بين كثير من الإدارات، ويمكن لتعميم الأمن السيبراني أن يفعل الكثير نحو تحقيق الاعتماد العضوي لنهج يشمل المنظمة بأكملها وليس اعتماد ذلك النهج كأمر مفروض (الفقرات 92-95). ويُظهر عدد من المنظمات ما يُشير إلى أنها بدأت بالفعل في تعميم اعتبارات الأمن السيبراني عبر سياساتها المختلفة. غير أن تقييم مدى تعميم الأمن السيبراني في الأطر التنظيمية العامة للمنظمات المشاركة سيتطلب نطاقاً من التحليل أوسع بكثير، ودراسة أشد تعمقاً، مما يسمح به الاستعراض الحالي. ويقترح المفتشون في الإطار 4 بعض المؤشرات للنظر فيها.

الإطار 4

مؤشرات لتعميم الأمن السيبراني عبر الأطر التنظيمية المؤسسية

- يمكن دمج العناصر ذات الصلة بالأمن السيبراني مباشرة في السياسات والعمليات والممارسات التي توجه عمل إدارات من قبيل الموارد البشرية أو المشتريات أو الاتصالات أو الدائرة القانونية. وهناك مثالان على ذلك، أحدهما إدراجُ متطلبات التدقيق المحددة للتعاقد مع مقدمي الخدمات الخارجيين في دليل المشتريات، والثاني إدخالُ الخطوات التي يتعين اتباعها في إدارة المخاطر السيبرانية طوال دورة حياة المشروع في نموذج وثائق المشاريع أو في وثائق التوجيه البرنامجي التي تستخدمها وحدات الأعمال في عملها اليومي.
- يمكن تحديد الجهات المعنية بأدوار ومسؤوليات الإدارات أو الوظائف بخلاف تلك التي تتعامل بشكل مباشر مع تكنولوجيا المعلومات والاتصالات أو الأمن السيبراني، وإبرازها صراحةً، ضمن الأدوات التنظيمية الرئيسية المعمول بها. وعلى سبيل المثال، توضح السياسة المؤسسية لأمن تكنولوجيا المعلومات لدى برنامج الأغذية العالمي بالتفصيل أدوارَ ومسؤوليات مختلف فئات الأفراد مثل مالكي المعلومات وأمناء المعلومات ومستخدِمي المعلومات والمشرفين والعاملين. وتعتبر المنظمة العالمية للملكية الفكرية مثالاً آخر على ذلك.

- يمكن تحديد سبل يُطلب من خلالها من جميع أصحاب المصلحة ذوي الصلة بخلاف موظفي تكنولوجيا المعلومات والاتصالات والأمن السيبراني المساهمة بشكل روتيني ليس فقط في صياغة تلك الصكوك ولكن أيضاً في تنفيذها (على سبيل المثال من خلال تضمين ممثلين عن أصحاب المصلحة كأعضاء في هيئات الحوكمة الداخلية ذات الصلة أو الأخذ بعملية للموافقة على السياسات تتطلب استشارة بعض أصحاب المصلحة قبل الموافقة على النص النهائي).

المصدر: من إعداد وحدة التفتيش المشتركة.

الامتثال والمساءلة

79- **إمكانية الوصول كشرط مسبق للامتثال.** لا يمكن أن يكون الإطار التنظيمي الأكثر تفصيلاً فعالاً إلا بدرجة فعالية مستوى امتثال الأطراف ذات الصلة له. ويمكن أن يتأثر الامتثال بعدة عوامل منها إمكانية الوصول إلى المواد التي تحدد بعبارات واضحة ما هو مطلوب من كل صاحب مصلحة وعضو في القوى العاملة ولماذا يُطلب منه ذلك. وقد شدد على هذه النقطة الأخيرة أحد رؤساء موظفي أمن المعلومات الذين قابلهم المفتشون، مشيراً إلى أن المشكلة لا تكمن في الافتقار إلى التوجيهات المكتوبة بل تتعلق بالأحرى بسوء فهم المستخدِمين لسبب وجود هذا التوجيه، وما الذي يحميه، وما يمكن للفشل في معرفته وتطبيقه أن يتركه من أثر، سواء على الشخص المعني أو على المنظمة. ويرد عرض أكثر تفصيلاً لأهمية هذه المعرفة في أجزاء أخرى من هذا التقرير (الفقرات 97-103) وهي تشمل الحاجة إلى لغة ورسائل بسيطة وغير تقنية وجذابة تركز على توضيح عواقب السلوك السيبراني المحفوف بالمخاطر بالنسبة للفرد. وتقدم الأمانة العامة للأمم المتحدة مثالاً على مستودع جيد التنظيم وشامل للمواد التوجيهية الخاصة بالأمن السيبراني، يتضمن فيما يتضمنه مقاطع فيديو بلغة واضحة، وملصقات، ومقالات موجزة عن "كيفية التنفيذ"، وأسئلة متداولة، ومجموعة كاملة من التنظيمات والسياسات المعمول بها مصنفة حسب الموضوع ومُستكمَلة بالحواشي التوضيحية، يمكن الوصول إليه بصورة مباشرة من خلال نقرة واحدة من صفحة الشبكة الداخلية الرئيسية لمكتب تكنولوجيا المعلومات والاتصالات.

80- **قد يكون التعامل الحالي مع عدم الامتثال للأمن السيبراني غير كافٍ.** هناك عامل مهم من المرجح تماماً أن يؤثر على الامتثال وهو وجود تدابير إنفاذ فعالة يمكن تطبيقها في حال عدم الامتثال، وتُدعَّم في الوضع المثالي بمعرفة أن السلوك غير الممتثل يخضع للمعاقبة وأن هذه المعاقبة متوقعة فعلاً. ولا توجد لغة محددة بشأن عقوبات خرق الأمن السيبراني إلا في قلة من السياسات التي استعرضها المفتشون. وحتى في الحالات التي تتضمن فيها السياسات ذات الصلة عقوبات محددة، فإن المعلومات التي جُمعت بشأن تنفيذها في الممارسة العملية تشير إلى أنه نادراً ما يتم إنفاذها، ونتيجة لذلك، فإن الموظفين المنخرطين في ممارسات محفوفة بالمخاطر لا يخضعون للمساءلة عموماً. وفي معظم المنظمات المشارِكة، يمكن أن تحتوي سياسة الاستخدام المقبول لموارد تكنولوجيا المعلومات والاتصالات بعض التفاصيل الخاصة بمعاقبة سوء السلوك المتعلق بتكنولوجيا المعلومات والاتصالات، مما يتضمن عموماً خروقات الأمن السيبراني. وبشكل عام، تخضع هذه الخروقات لنفس الإجراءات التأديبية التي ترتبط بانتهاكات أي قاعدة أو نظام آخر يُعنى بشؤون الموظفين. غير أنه من المعروف أن العمليات المعتادة المتعلقة بتلك الإجراءات، حتى عند استحضارها وإكمالها بنجاح، تتصف بالبطء وهي مرهقة وكثيفة الاستخدام للموارد ولا يُلجأ إليها إلا في حالات سوء السلوك الجسيم فيما يتعلق بتكنولوجيا المعلومات والاتصالات.

81- **الحاجة إلى النظر في نظام عقوبات يراعي التفاصيل الأكثر دقة.** في حالة خروقات الأمن السيبراني، والتي كثيراً ما تكون بسبب الجهل أو الإهمال البسيط، **يرى المفتشون أن العقوبات التي يمكن فرضها بسهولة أكبر والتي تتصف بأنها أقل رسمية وتدخلاً يمكن أن تمثل نهجاً أكثر وعداً.** فهذه العقوبات

تعالج المشكلة بطريقة أكثر مباشرة وفورية تتناسب مع خطورة المخالفة. على أنه يتعين تحقيق توازن لضمان أن عواقب السلوك غير الممتثل تبقى محسوسة بشكل كافٍ لدى الأطراف الملتزمة من أجل تشجيع الصحة السيبرانية الأفضل والسلوك الأكثر مسؤولية. ويمكن ملاحظة وجود اعتراف ضمني بهذه الحقيقة في ممارسات بعض المنظمات التي تميز بين الانتهاكات الطفيفة والأكثر خطورة في سياساتها الخاصة بالأمن السيبراني. على أنه لم يكن من الواضح ما إذا كانت هذه المنظمات قد نجحت في ترجمة هذا التمييز إلى عقوبات أكثر تكيفاً مع المخالفات الطفيفة دون فقدان فعاليتها. وعلى سبيل المثال، تتوقع بعض السياسات إبلاغ المديرين التنفيذيين أو رئيس إدارة تكنولوجيا المعلومات والاتصالات، الأمر الذي قد يمثل الضغط "الناعم" الوحيد المتاح للامتثال ولكنه لا يشير إلى أية عواقب بخلاف الإحراج المحتمل. وهناك مثال مضاد جدير بالملاحظة، نظراً لخصوصيته وأثره السلبي المباشر على المستخدم دون الإفراط في العقاب، تقدمه الوكالة الدولية للطاقة الذرية، والتي تنص سياستها على عقوبة صريحة غير تأديبية في شكل إلغاء حق الأشخاص غير الممتثلين في الوصول إلى أنظمة المعلومات. ومن الجدير بالذكر أيضاً أن هذه السياسة تعترف بالحاجة إلى التناسب في تطلب المعرفة قبل معاقبة الشخص على ارتكاب المخالفة وتُوازن بين هدف الحماية الفعالة لأصول المنظمة وضمان ألا تعني إجراءات الإنفاذ إخضاع القوى العاملة لإجراءات رقابية مفرطة. وعلى الصعيد العملي، يُنفَّذ إلغاء حق الوصول على أساس مؤقت وبعد تحذيرات متكررة. ويود المفتشون أن يشددوا على أن أية آلية مفيدة للجزاءات لا يمكن أن تُنفّذ دون دعم صريح من الرئيس التنفيذي، مما يشكل عاملاً مساهماً في سياق المثال المذكور. **ويرى المفتشون أنه ينبغي للرؤساء التنفيذيين أيضاً أن يستكشفوا إمكانية تقديم حوافز للإبلاغ عن الحوادث وأن يشجعوا الأفراد على تحمل المسؤولية عن ممارساتهم غير الآمنة أو المحفوفة بالمخاطر.** ومن الأهمية بمكان في سياق ذلك إيجاد طرق للتوفيق بين هدف الردع من خلال عقوبات أكثر تمايزاً وبين هدف تقديم حوافز للإبلاغ دون خوف من التداعيات.

هاء- تسخير مساهمات آليات الرقابة

82- **تنبُّه هيئات المراجعة والرقابة على جميع المستويات للأمن السيبراني.** درس المفتشون سبل تعامل هيئات الرقابة مع اعتبارات الأمن السيبراني في سياق مجالات تركيز كل منها، سواء على مستوى وظيفة المراجعة الداخلية (التي تهدف في المقام الأول إلى تقييم الامتثال للسياسات والإجراءات)، أو على مستوى عمليات المراجعة الخارجية (المعنية بشكل رئيسي بالمراجعة المالية والمراجعة الخاصة بالامتثال، وفي بعض الأحيان بالمراجعة الخاصة بالأداء في مجالي الإدارة والتسيير) أو على مستوى لجان المراجعة والرقابة (بشكل رئيسي إسداء المشورة بشأن المسائل الأعم في المنظمة والتي تتطلب الاهتمام والإجراءات من جانب الإدارة العليا، وكذلك الهيئات التشريعية والإدارية، على سبيل الأولوية). ويرحب المفتشون بأن الأمن السيبراني، على كل من هذه المستويات، برز كموضوع للاهتمام على مدى السنوات الخمس الماضية، بل ولفترة أطول من ذلك في بعض المنظمات.

هيئات الرقابة التي تعالج مسائل الأمن السيبراني

83- **المراجعة الداخلية والخارجية التي تركز بشكل رئيسي على تكنولوجيا المعلومات والاتصالات، بما في ذلك الأمن السيبراني إلى حد ما.** يتم بشكل عام دمج المسائل المتعلقة بتكنولوجيا المعلومات والاتصالات بشكل جيد في تخطيط المراجعات الداخلية القائمة على المخاطر. على أن وحدة التفتيش المشتركة لم تجد، في سياق ما قامت به من بحوث، إلا عدداً محدوداً من مهام المراجعة التي ركزت على الأمن السيبراني تحديداً خلال السنوات الخمس الماضية. وفيما يتعلق بالقدرة على إجراء هذه المهام، فإن الخبرة الداخلية لإجراء مراجعات خاصة بتكنولوجيا المعلومات والاتصالات لا تتوفر إلا لدى عدد قليل من المنظمات، في حين أن غالبية المنظمات تعتمد على استخدام خبراء خارجيين. ويبدو أن هذا النهج مُرضٍ

في معظم الحالات. كما كانت تكنولوجيا المعلومات والاتصـــالات أحد مجالات التركيز لدى المراجعين الخارجيين في العديد من المنظمات المشارِكة على مر السنين، وقد تناولوا موضوعات من قبيل استمرارية الأعمال، وتقييم المخاطر وإدارتها، وسياسات تكنولوجيا المعلومات والاتصالات، وإدارة أصول تكنولوجيا المعلومات والاتصالات. وعموماً، أظهرت ردود الإدارة التي رجع إليها المفتشون تقبلاً للتوصيات وأشارت إلى التدابير المتخذة من أجل التنفيذ.

84- **تولي لجان المراجعة والرقابة اهتماماً مستمراً للأمن السيبراني.** في عام 2016، حدد ممثلو لجان الرقابة في 19 كياناً من كيانات منظومة الأمم المتحدة، "من بين أمور أخرى، المخاطر المرتبطة بالأمن السيبراني في بيئة رقمية كمجالٍ للتركيز واتفقوا على تحدي الإدارة بشأن ما لديها من فهم واستعداد"[(18)]. والواقع أن، تحليل محتوى تقارير هذه اللجان يُظهر أنه كان هناك اهتمام مستمر يركز على تعزيز جوانب الحوكمة وإدارة المخاطر في الأمن السيبراني، مع أن أياً من اختصاصات هذه اللجان لم يتضمن إشارة محددة إلى الأمن السيبراني، في حين أن اختصاصات أربع لجان فقط أشارت إلى تكنولوجيا المعلومات والاتصالات. وفي الغالب، تناولت اللجان هذه المسائل كجزء من ولايتها بشأن الإدارة المركزية للمخاطر في المنظمة المعنية أو، عند الاقتضاء، عند متابعة حالة تنفيذ توصيات المراجعة الداخلية أو الخارجية المتعلقة بتكنولوجيا المعلومات والاتصالات. ويُظهر الاستعراض الحالي أن الخبرة المتخصصة لم تكن متوفرة بشكل منهجي لدى أعضاء لجان المراجعة والرقابة، إذ أن أربع لجان فقط على ما يبدو استفادت من هذه الخبرة، في حين أن معظمها اعتمد على المشورة الخارجية على أساس مخصص، على غرار الترتيب السائد في وظيفة المراجعة الداخلية. ومن الجدير بالثناء أن هذه اللجان تتبنى الموضوع، ليس فقط لأن ذلك قد يدعم الإدارة في اتباع نهج قائم على المخاطر إزاء الأمن السيبراني ولكن أيضاً كطريقة لتثقيف الهيئات التشريعية والإدارية حول مخاطر الأمن السيبراني ذات الصلة، وبالتالي تمكينها من المساهمة في تخفيف المخاطر على مستوى المنظمة.

قيمة توصيات الرقابة لتعزيز وضع الأمن السيبراني لدى المنظمات

85- **توصيات الرقابة تدفع إلى إجراء تغييرات هيكلية إيجابية.** أفادت المنظمات المشارِكة أن تغييرات هيكلية كبيرة في نهجها إزاء الأمن السيبراني نشأت عن ملاحظات قدمتها هيئات الرقابة، مما يسلط الضوء على القيمة المضافة لهذه الآليات. وأثناء المقابلات، أعرب المسؤولون عن تكنولوجيا المعلومات والاتصالات والأمن السيبراني عموماً عن تقديرهم لتقارير الرقابة باعتبارها محركات للتغيير، فهي ترفع الوعي على مستوى الإدارة العليا بالحاجة إلى مضاعفة الاهتمام بتقوية وضع الأمن السيبراني. ووجد المفتشون بالفعل أمثلة على أن توصيات المراجعة الداخلية ساهمت بشكل مباشر في تعزيز الأمن السيبراني في المنظمة المعنية، مثل المنظمة العالمية للملكية الفكرية. كما وجدوا أمثلة أخرى في منظمة الطيران المدني الدولي أو صندوق الأمم المتحدة للسكان، حيث أدت توصية مراجعة الحسابات إلى وضع خارطة طريق متعددة السنوات؛ أو في اليونسكو، حيث تم إنشاء منصب رئيس موظفي أمن المعلومات؛ أو في الأمانة العامة للأمم المتحدة، حيث شهد الامتثال للتدريب على أمن المعلومات تعزيزاً كبيراً. كما قام المراجعون الخارجيون بصياغة توصيات بشأن مسائل الأمن السيبراني لـ 16 منظمة مشاركة خلال السنوات الخمس الماضية، لا سيما فيما يتعلق بالامتثال للتدريب على أمن المعلومات، واستعادة البيانات، والتحكم في وصول المستخدِمين، والموارد التي ستُكرس للأمن السيبراني. ويبدو أن هناك تحسن في الاعتراف بفائدة توصيات المراجعة عندما تتجاوز هذه التوصيات نهج الامتثال للجوانب التشغيلية والتقنية لتقترح تحسينات استراتيجية، تسليماً بأن الامتثال وحده للأطر التنظيمية لا يعني توفر الحماية. وفي الوقت

(18) انظر A/72/295، الفقرات 40-43.

نفسه، أعرب كثير من المنظمات عن قلقها لأن هذه التوصيات لم تكن في بعض الأحيان على دراية كافية بالقيود المفروضة على الموارد وبواقع ظروف العمليات، مما أضعف احتمال تنفيذ بعضها.

86- **استرشاد وظيفة الرقابة بالخبرة في مجال الأمن السيبراني بصورة منهجية.** للتأكد من أن هيئات الرقابة تقدم أقصى قيمة من وجهة نظر الأمن السيبراني، من المهم بمكان أن تتوفر لها إمكانية الوصول إلى جميع المعلومات ذات الصلة بالمخاطر والقدرات والقيود داخل المنظمة وفهمها جيداً. وتتمثل الطريقة الأكثر فعالية لذلك في التأكد من أن معرفة وخبرة خبراء الأمن السيبراني داخل منظمة ما يمكن أن ترشد عمل وظيفة الرقابة وأن تصب فيه. وهناك مجموعة متنوعة من الخيارات في هذا الصدد، بعضها قد ترسخ بالفعل في الممارسة أو حتى في الأطر التنظيمية لدى المنظمات المشارِكة، سواء بشكل فردي أو مجتمعة، ويمكن اعتبارها ممارسة جيدة. وتشمل هذه الخيارات ما يلي: (أ) استشارة رئيس موظفي أمن المعلومات، أو وحدة أمن المعلومات، على أساس إلزامي فيما يتعلق بالتخطيط للمراجعة القائمة على المخاطر، ومشاركته الكاملة في تحديد الضوابط والمؤشرات ذات الصلة؛ و(ب) إرسال معلومات الأمن السيبراني إلى هيئات الرقابة وفقاً لاحتياجات ولاية كل منها، سواء كان ذلك من خلال الإبلاغ عن مقاييس الحوادث، أو الإحاطات المخصصة أو العادية، أو من خلال وسائل أخرى؛ و(ج) عرض أية تقارير أو توصيات منبثقة عن المراجعة فيما يتعلق بالأمن السيبراني على رئيس موظفي أمن المعلومات، أو وحدة أمن المعلومات، للتعليق عليها قبل وضعها في صيغتها النهائية وذلك للحد من التخوف من أن التوصيات لا تستند إلى أسس كافية في واقع المنظمة مما يجعلها غير قابلة للتنفيذ.

واو- غرس ثقافة الأمن السيبراني من القيادة نزولاً إلى القاعدة

87- **يتعين على القيادة أن تشجع الاعتراف بالأخطاء وبأوجه الضعف.** على النحو المناقَش أعلاه، يُعتبر وضع الأمن السيبراني في المنظمة أيضاً مسألة ثقافة داخلية قوية، تبدأ بأن تولي الإدارة التنفيذية الاهتمام للمسألة وأن تمنحها الأولوية – فالقيادة هي التي تحدد التوجه. على أن الأمر لا يتوقف عند ذلك ويحتاج إلى التدرج من القيادة نزولاً إلى كل فرد من أفراد القوى العاملة. وتحقيقاً لهذه الغاية، هناك حاجة إلى استمرار الالتزام والعمل في المستويات العليا من المنظمة، ويجب أن يتجاوز ذلك الاكتفاء بالتصريحات التي تصف الأمن السيبراني كأولوية مؤسسية. ويتمثل أحد العناصر الأساسية في تشجيع ثقافة داخلية لا يُنظر فيها إلى الاعتراف بوقوع الحوادث على أنه فشل ولكن كنقطة انطلاق لمعالجة مشكلة مشتركة ولحماية المنظمة وأصولها بشكل أفضل، من خلال إظهار الملكية المشتركة والفردية للأخطاء وأوجه الضعف والمساءلة عنها. وفي هذا الصدد، يمكن الاستفادة من ثقافة إنفاذ القانون في مجال السلامة المادية والأمن، حيث يُعتبر وقوع الحوادث أمراً مفروغاً منه، وحيث يُتوقع أن يتم الإبلاغ عنها والتعامل معها بشكل طبيعي، دون إصدار أحكام. **ويعتبر المفتشون أن من مسؤولية الرئيس التنفيذي غرس هذه الثقافة في جميع الوظائف وجميع المواقع التي تتواجد فيها المنظمة، حيث إن أنظمة المعلومات متصلة ومترابطة فيما بينها، ويمكن أن يؤدي الهجوم أو الاقتحام في أي مكان إلى اختراق في كل مكان.**

88- **وعي الإدارة التنفيذية والمساءلة كنقطة انطلاق.** تتمثل الخطوة الأولى نحو غرس عقلية وثقافة جديدة في أن تكون القيادة العليا نفسها على دراية بالمخاطر المرتبطة بالأمن السيبراني وأن تطور فهماً لتداعيات التقاعس عن العمل وضعف الصحة السيبرانية من خلال زيادة الاهتمام بالمسألة. ويمكن تحقيق ذلك بطلب إحاطات منتظمة من المسؤولين المعنيين داخل المنظمات، مثل خبراء الأمن السيبراني، وموظفي إدارة المخاطر، وممثلي هيئات الرقابة، وكذلك من خلال مبادرات التدريب والتوعية التي تستهدف كبار المديرين تحديداً. ومنذ عام 2020، في الأمانة العامة للأمم المتحدة، تحتوي الاتفاقات المبرمة بين

الأمين العام وكبار المسؤولين على أحكام مصممة لتعزيز الوعي والمساءلة في هذا المجال. ويتجاوز نطاق الاستعراض الحالي اتساق الاتفاقات ومؤشرات الأداء الواردة فيها وفعاليتها، لكن ترسيخ أهداف الأمن السيبراني في تقييمات أداء كبار المديرين يعتبر خطوة مرحباً بها نحو تحسين المساءلة وتحديد التوجه الصحيح انطلاقاً من قمة المنظمة. علاوة على ذلك، هناك مبادرات ينبغي تشجيعها، من قبيل العرض المقدم في سياق اللجنة الإدارية الرفيعة المستوى لتنبيه الإدارات العليا إلى التأثير المستمر لمخاطر الأمن السيبراني على العمليات، ليس فقط من حيث تعطيل الأنظمة الإدارية والشبكات والبنية التحتية، ولكن أيضاً تعريض تنفيذ الولاية الفنية للخطر، بما في ذلك ضمن كل منظمة مشاركة[19].

89- **المال وحده لا يُشتري ثقافة الأمن السيبراني.** هناك طرق كثيرة يمكن للإدارة التنفيذية من خلالها إلهام العمل والتأثير على العقليات بشكل ملموس نزولاً عبر سلسلة القيادة. أولاً، يمكن التعبير عن الأهمية الممنوحة للأمن السيبراني من خلال تخصيص الموارد الكافية. وفي الوقت نفسه، لا يمكن للمال وحده حل مشكلة استعداد الأمن السيبراني، كما أنه لا يشتري ثقافة الأمن السيبراني. وعلى وجه التحديد، لا يعفي الدعم المالي الإدارة التنفيذية من مسؤوليتها في توفير قيادة نشطة في مسائل الأمن السيبراني، الأمر الذي أكده تقرير صدر مؤخراً عن مجمع الفكر غارتنر المعروف والمعني بالأمن السيبراني[20]. فالتعبير عن الدعم مالياً فقط يمكن أن يؤدي في الواقع إلى نقل مسؤولية الإدارة التنفيذية إلى المستوى الأدنى التالي، حيث يمكن الإنفاق دون رؤية إستراتيجية شاملة. فتخصيص الموارد والاستثمارات ذات الصلة يجب أن يتقرر في سياق الأعمال وليس من منظور تكنولوجي بحت أو من منظور إدارة المخاطر وحدها، والإدارة التنفيذية هي الجهة الأفضل لاتخاذ قرار مستنير يوازن بين جميع الاعتبارات بشكل مناسب (الفقرتان 108-109).

90- **الطرق غير النقدية لإظهار الدعم على المستوى التنفيذي.** تشمل بعض الممارسات الجيدة المستقاة من المنظمات المشارِكة في مجال الدعم الهادف غير النقدي من جانب الإدارة العليا الإجراءات التالية التي اتخذها الرؤساء التنفيذيون: المشاركة بشكل واضح في برامج التوعية مثل تسجيل بيانات الدعم بالفيديو؛ ومخاطبة الموظفين حول مسائل الأمن السيبراني في لقاءات مفتوحة؛ وإطلاع الموظفين على التجارب الشخصية المتصلة بهجمات الأمن السيبراني؛ ووضع نماذج القدوة العامة للسلوكيات الموصى بها؛ ودعم الحملات المتكررة والمنتظمة لمحاكاة التصيد الاحتيالي والموجهة لجميع مستويات الموظفين، بما في ذلك كبار المديرين؛ وضمان تدرج المسؤولية نزولاً من خلال ممارسة الضغط على كبار المديرين للمشاركة بأنفسهم في التدريب ولإخضاع أفرقتهم للمساءلة عن الامتثال للسياسات وإظهار السلوكيات المناسبة؛ ودعم إنفاذ العقوبات المتناسبة، خاصة بالنسبة "للمخالفين المتكررين" الذين يستمرون في انتهاك قواعد الأمن السيبراني وإجراءاته. وكما ورد أعلاه، تتمثل نقطة البداية في الاعتراف بأن الأخطاء يمكن أن تحدث، وفي التعلم منها بالإضافة إلى معالجة عواقبها بشكل مشترك كمنظمة.

91- **التحول في العقليات يتطلب وقتاً ورسائل متسقة ودعماً رفيع المستوى.** لترسيخ مواقف الموظفين على جميع المستويات وبالتالي تكوين ثقافة الأمن السيبراني المؤسسية، يتعين أن تكون هذه الإجراءات متكررة، وهي تتطلب الوقت لإظهار نتائجها. وتبين التجربة أن فرص النجاح تزداد وتتسارع عندما تأتي من قمة المنظمة رسالة متسقة مفادها أن للأمن السيبراني أهميته وهو ليس مسعى يطرأ مرة واحدة. وكما ورد في الندوة الثامنة للفريق المختص بأمن المعلومات في عام 2019، فإن "من الصعب تغيير السلوك البشري فذلك يتطلب تعرضاً متكرراً ومتسقاً لرسائل تتضمن معلومات جديدة، كما يتطلب إعادة التعلم دورياً، فضلاً عن فهم المخاطر الكامنة التي تطرحها التكنولوجيا وعواقب سوء السلوك في الحوسبة"[21].

(19) أنظر CEB/2017/HLCM/ICT/9.

(20) غارتنر، *الحاجة الملحة لمعاملة الأمن السيبراني كقرار خاص بالأعمال*، شباط/فبراير 2020.

(21) CEB/2019/HLCM/DTN/02.

زاي- تنفيذ نهج المنظمة بأكملها

92- **دور إدارات الشؤون الإدارية.** تماشياً مع الفهم المتزايد بأن المسؤولية عن الأمن السيبراني لا يمكن أن تقع على عاتق إدارات تكنولوجيا المعلومات والاتصالات وحدها، أقرت غالبية المنظمات المشارِكة، بطريقة أو بأخرى، بأن لإدارات الشؤون الإدارية، فضلاً عن الإدارات الفنية، دوراً تؤديه. وفي معظم المنظمات، بدا هذا الفهم أكثر وضوحاً في الردود على استبياني وحدة التفتيش المشتركة فيما يتعلق بإدارات الشؤون الإدارية. وسواء انعكس ذلك رسمياً في الأطر التنظيمية لدى المنظمات أم لا، فإن سلسلة من إدارات الشؤون الإدارية تساهم في الواقع بشكل روتيني في الحفاظ على الحماية العامة للأمن السيبراني في المنظمات. ويشمل ذلك قيام إدارات الموارد البشرية بتيسير برامج التدريب على الأمن السيبراني؛ وتعامُل خدمات المشتريات مع مقدمي الخدمات الخارجيين، بما في ذلك التدقيق فيهم من وجهة نظر الأمن السيبراني؛ وما تقدمه الدوائر القانونية من مشورة بشأن المسائل التنظيمية والتعاقدية والامتثال؛ وما تقوم به إدارات الاتصال من إدارة لجوانب العلاقات العامة مع أصحاب المصلحة الخارجيين. بالإضافة إلى مساهماتها بحكم وظيفتها، من المتوقع بطبيعة الحال أن تكون معظم هذه الإدارات مهيأة مسبقاً لدمج اعتبارات الأمن السيبراني في أنشطتها اليومية نظراً لأن أعمالها الأساسية تنطوي على التعامل مع معلومات حساسة، بما في ذلك البيانات الشخصية والمالية. ولا توضح المواد التي درستها وحدة التفتيش المشتركة ما إذا كان ذلك يجري بقدر كافٍ على صعيد الممارسة وإلى أي مدى يمكن أن نعتبر أنه يعكس فهماً فعلياً لدى هذه الإدارات لدورها المتميز كقَيِّمَة على المعلومات الحساسة. ويمكن أن يكون هذا مجالاً يستحق اهتماماً متزايداً من جانب رؤساء تلك الإدارات والمراجعين الداخليين، ويمكن دمجه، عند الاقتضاء، في تقييمات الأمن السيبراني التي يجريها مقدمو الخدمات الخارجيون.

93- **دور الإدارات الفنية.** على خلاف إدارات الشؤون الإدارية، فإن المعلومات التي جُمعت في سياق التحضير لهذا الاستعراض تشير إلى أنه، باستثناء تلك المنظمات المشارِكة التي تفرض ولاياتها شرطاً صارماً يتعلق بسرية البيانات باعتبارها جانباً أساسياً من عملها، غالباً ما ينظر المديرون الفنيون إلى الأمن السيبراني على أنه عبءٌ إداري وقيدٌ تشغيلي. وبحسب ما ورد، لم تكن مكاتب البرامج متقبلة بصورة كافية لضرورة تضمين الأمن السيبراني ومتطلبات القدرة على الصمود في تصميم وتنفيذ مشاريعها وأنشطتها. وعلى حد تعبير موظف لأمن المعلومات أجريت معه مقابلة، "غالباً ما يُنظر إلى سياسات وإجراءات الأمن السيبراني على أنها عائق أمام سرعة التنفيذ وليس باعتبارها دروعاً واقية لسمعة المنظمات وأصولها، فضلاً عن كفاءة عملياتها". وعلى ضوء هذه الخلفية، يكتسي أهمية خاصة قيامُ الرؤساء التنفيذيين بالتصدي بقوة للتصورات التي تفيد بأن تدابير الأمن السيبراني المعززة تعرقل سرعة العمليات أو تعيق تحقيق الأهداف المقررة.

94- **تعميم الأدوار والمسؤوليات وملكيتها كمفتاح لنهج يشمل المنظمة بأكملها.** كما ذُكر أعلاه (الفقرة 78)، فإن تعميم اعتبارات الأمن السيبراني في السياسات التي تحكم عمل الإدارات المختصة وممارساتها سيكون بحد ذاته إقراراً بأن لكل وظيفة في المنظمة مساهمة تقدمها نحو بلوغ نهج المنظمة بأكملها. وعلى ضوء الاتجاه الأخير الملاحظ في العديد من المنظمات نحو اللامركزية وتفويض السلطة إلى الرتب الأدنى وصولاً إلى المديرين من المستوى المتوسط، فإن ذلك التعميم سيساهم أيضاً في ضمان المزيد من الملكية والمساءلة المباشرة على مستوى المنظمة من خلال توضيح المسؤوليات ذات الصلة بحيث يسهل لكل من أصحاب المصلحة الرجوع إليها فيما يتعلق بدوره. ويمكن لجعل أبعاد الأمن السيبراني في الوظائف البرنامجية والإدارية أكثر وضوحاً من خلال تعميمها أن يقلل من سوء الفهم والافتقار إلى الملكية. وعلى سبيل المثال، لاحظ المفتشون بعض التوتر بين خبراء الأمن السيبراني وممثلي الوحدات الأخرى في المنظمة نتيجة لتصورات كل منهم لأدوارهم في ضمان وضع قوي في مجال

الأمن السيبراني. **وفي هذا السياق، يشدد المفتشون على أن الإدارات الفنية تحتاج، على وجه التحديد، إلى تولي ملكية البُعد الخاص بالأمن السيبراني بقوة أكبر في عملها.** ومع ذلك، فإن مشاركة وحدات الأعمال ينبغي ألا تعني نقل المسؤولية حصرياً إليها كمالكة للمخاطر. كما لا يمكن تحميل خبراء الأمن السيبراني وحدهم المسؤولية عن حماية أصول المنظمة دون تقاسم جانب كبير من العبء مع وحدات الأعمال. ولتحقيق التوازن الصحيح أهميته في هذا المجال، ويمكن لتعميم اعتبارات الأمن السيبراني عبر مجالات المنظمة أن يرسي الأساس لخلق توقعات متبادلة صحيحة بين الإدارات المختلفة ولتحديد أدوار كل منها بصورة سليمة في هذا الصدد.

95- **ينبغي المضي في توسيع نطاق التدريب القائم على الأدوار.** تمثلت إحدى الممارسات المشجعة المواجَهة في عدد من المنظمات المشارِكة في توافر فرص التدريب وتدابير التوعية استناداً إلى الأدوار في مجال الأمن السيبراني، مما ينبغي المضي في توسيعه لتزويد جميع أصحاب المصلحة على النحو الأمثل بما يمكّن كلاً منهم من تقديم ما يُتوقّع منه على سبيل المساهمة في قدرة المنظمة على الصمود في المجال السيبراني. وعلى مستوى المنظومة ككل، شجعت شبكة تكنولوجيا المعلومات والاتصالات بالفعل على استهداف مجموعات محددة من المستخدِمين استناداً إلى مسؤولياتهم الوظيفية، مثل موظفي التخطيط المركزي للموارد، والمتخصصين في المالية والمحاسبة، وموظفي المشتريات، والمديرين التنفيذيين. كما أعدت بعض المنظمات دورات مهيأة خصيصاً للموظفين الذين يقومون بمهام حساسة أو للموظفين الميدانيين الذين يواجهون مخاطر تتعلق خصيصاً بالمواقع أو البنية التحتية. من بين هذه المجموعات الخاصة، قد يستحق المديرون التنفيذيون وكبار المديرين من ناحية ومديرو البرامج من ناحية أخرى إعطاءهم الأولوية، إذ أن فهمهم هم للأمن السيبراني وموقفهم تجاهه يمكن أن ينتقلا نزولاً إلى المستويات الأدنى داخل المنظمة أو الوحدة التي ينتمون إليها وأن يؤثرا بطرق مهمة على قيام ثقافة للأمن السيبراني – أو عدم قيام هذه الثقافة.

حاء- ترسيخ القوى العاملة كخط أول للدفاع

96- **"العامل البشري" – كتهديد لثقافة الأمن السيبراني والقدرة على الصمود، وكدفاع عنهما وركيزة لهما.** اتخذت غالبية مؤسسات منظومة الأمم المتحدة تدابير تكنولوجية وتشغيلية هامة للمساعدة في الوقاية والتخفيف من مخاطر الهجمات السيبرانية (الفقرة 38). على أن هناك إجماعاً في أوساط خبراء الأمن السيبراني على استمرار التحدي المتمثل في تثقيف كل فرد من القوى العاملة بشأن دوره في حماية معلومات المنظمة وأصولها الرقمية، وكذلك بشأن أهمية الالتزام بسياسات الأمن السيبراني وإجراءاته وأفضل ممارساته. ومن نواح كثيرة، يكتسب "العامل البشري" أهمية في المشهد العالمي لتهديدات الأمن السيبراني، كما ينعكس في القلق المتزايد بين المنظمات المشارِكة بشأن المستخدِمين النهائيين الأفراد الذين يتعرضون لاستهدافهم بشكل متزايد من خلال تقنيات الهندسة الاجتماعية (الفقرات 26-27). وثبت أيضاً أنه من الصعب بشكل خاص إدارة هذا العامل كمصدر للمخاطر. وبصرف النظر عن كونه الخط الأول للدفاع وفي نفس الوقت الحلقة الأضعف في شبكة الأمان الرقمية في المنظمة، فإن كل فرد من القوى العاملة يمثل أيضاً ركيزة مهمة لثقافة الأمن السيبراني ولقدرة المنظمة على الصمود. وتتعدد أوجه العواقب السلبية للممارسات السيبرانية السيئة وتتجلى غالباً على شكل تهديدات داخلية كبيرة. وقد تنشأ هذه التهديدات عن أخطاء يرتكبها مستخدِمون غير مهتمين أو معنيين؛ وعن نقص الوعي أو اليقظة (مما يُستغَل غالباً في هجمات التصيد الاحتيالي)؛ وسوء ممارسات حماية البيانات، من قبيل اختيار كلمات مرور ضعيفة أو تقاسم بيانات اعتماد الوصول بين عدة مستخدِمين؛ واستخدام برمجيات غير مأذون بها أو قديمة؛ وتطوير تطبيقات خارج بيئات تكنولوجيا المعلومات والاتصالات التي تديرها المنظمة؛ والأنظمة التي لا تحصل على تحديثات تصحيحية أو تتعرض صيانتها للإهمال. ومن المرجح أن هذه السلوكيات هي الأكثر انتشاراً بين أشكال التهديدات التي

تواجهها المنظمات على أساس يومي. ولذا فإن من الواضح أن تمكين المستخدِمين من أداء دور نشط في تحسين قدرة المنظمة على الصمود في المجال السيبراني أمرٌ محتّم.

97- **المعرفة الرقمية هي نقطة بداية غير قابلة للتفاوض.** كشرط مسبق لتطوير فهم كيفية تأثير ممارسات الأمن السيبراني على المنظمة، تشكل المعرفة الرقمية الأساسية لدى كل فرد من القوى العاملة نقطة بداية غير قابلة للتفاوض. فتوفر القدرة على العمل في البيئة الرقمية لم يعد أمراً اختيارياً لأي شخص منتسب بأي شكل من الأشكال إلى الأمم المتحدة وعملها في القرن الحادي والعشرين. ويتعين أن تتوفر لدى كل مستخدم للبنية التحتية الرقمية للمنظمات إمكانيةُ التنقل المريح بين المعدات والتطبيقات الإلكترونية القياسية، سواء كان ذلك المستخدِم من الموظفين أو الأفراد المنتسبين أو الخبراء العاملين في مهمة أو المندوبين في المؤتمرات أو أي شخص آخر يتصل بالمصادر السيبرانية الداخلية أو يستخدمها. ولا يمكن إلا بعد تلبية هذا الشرط الأساسي المضي لتذكير الموظفين بأن الحفاظ على سرية المعلومات والأصول المؤسسية وسلامتها وتوافرها جزءٌ لا يتجزأ من وظيفة كل فرد ومسؤولياته. على أن الخطوة التالية الأكثر تحدياً قد تتمثل في الانتقال من التوعية بقواعد الأمن السيبراني ومسؤولياته وأدواته والتوجيهات حول الممارسات السيبرانية الصحية إلى تحقيق تغيير سلوكي مستدام وتحولٍ في المواقف الفردية والجماعية.

98- **الاعتراف بأهمية التدريب.** تشكل برامج التدريب والتوعية القوية واحداً من السبل التي تمكّن من إحداث تحول في العقليات باتجاه التسليم بالمخاطر السيبرانية وتطوير موقف صحي إزاء الأمن السيبراني. وهناك تأكيد على هذه النقطة في الكتابات المهنية وفي تقارير لجان المراجعة والرقابة الموجهة إلى الإدارة التنفيذية في عدد من مؤسسات منظومة الأمم المتحدة. وهناك مفارقة معينة تتمثل في أن الآليات التقنية الشاملة والمتعددة الطبقات لحماية البنية التحتية والأنظمة غالباً ما تكون موجودة، ومع ذلك فإن قدرة جميع أفراد القوى العاملة على إظهار معرفة باستخدام تلك الآليات والقدرات ترقى إلى مستوى الممارسين يبدو أنها متخلفة، على الأقل في بعض المنظمات، وفقاً للمقابلات مع المسؤولين. وكلما كانت الأنظمة أشد متانة، زاد تحول المخاطر نحو المستخدِمين، ومن بين هؤلاء، يتمثل أكبر الخطر في المستخدِمين الذين يعانون من ضعف الصحة السيبرانية. وكما ذكرت اللجنة الاستشارية المستقلة للمراجعة في الأمانة العامة للأمم المتحدة، فإن "الافتقار إلى الوعي يمكن أن يؤدي إلى الإضرار بأنظمة تكنولوجيا المعلومات والاتصالات، وبسرية المعلومات، وسلامتها"[(22)].

99- **يُظهر تحديد فرص التدريب للموظفين وضعاً مشجعاً.** دأبت شبكة تكنولوجيا المعلومات والاتصالات، على مر السنين، على تأكيد أهمية التدريب الموجه لمجتمع الأمم المتحدة في مجال معرفة أمن المعلومات، وقد بذلت المنظمات المشارِكة جهوداً لتعزيز ما تقدمه في هذا الصدد[(23)]. ويمثل الشكل السابع المعلومات التي تم جمعها بشأن أربع فئات من المجموعات المستهدفة، ويؤكد وجود دورات تدريبية إلزامية للموظفين في غالبية المنظمات، ولكنه يوضح أيضاً أن هذه الدورات في بعض المنظمات لا تزال اختيارية. ويركز محتوى التدريب عادةً على الاستخدام الصحيح لحسابات البريد الإلكتروني لأغراض أعمال المنظمة في مقابل الأغراض الشخصية، ومخاطر فتح المرفقات الواردة من مصادر غير معروفة، والتوجيهات المتعلقة باختيار كلمات المرور والتعامل معها، أو السلوك الآمن عند دخول مواقع شبكية خارجية. وخلال السنوات الأخيرة، نبهت لجان المراجعة والرقابة المنظمات المشارِكة إلى الحاجة إلى تعزيز معدل الامتثال للدورات التدريبية الإلزامية، وهو تطور مرحَّب به من حيث المبدأ. على أن المفتشين يودون التأكيد على

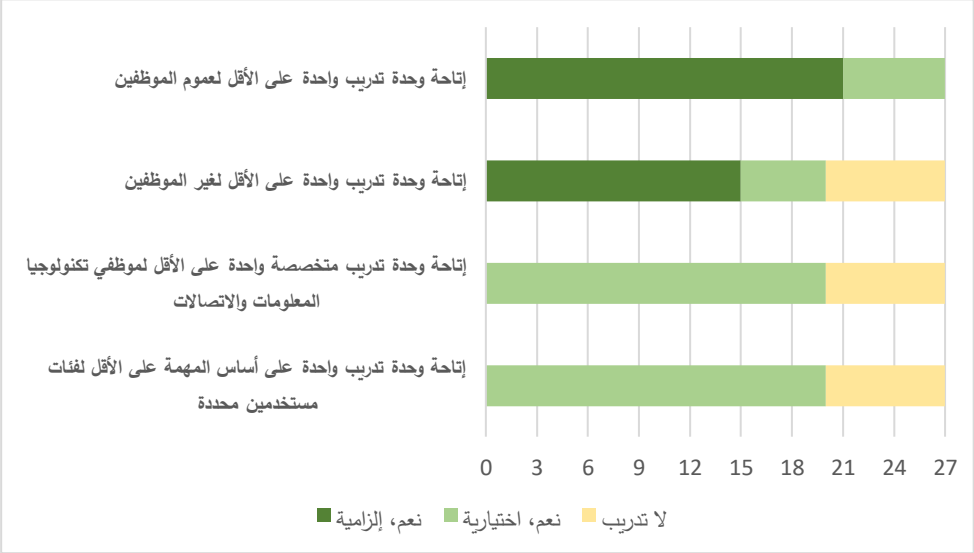
(22) A/73/304، الفقرة 51.

(23) أنظر على سبيل المثال CEB/2011/3 وCEB/2018/HLCM/ICT/10.

أن الامتثال للتدريب الإلزامي وحده نادراً ما يكون مؤشراً مفيداً على الوعي، كما أنه لا يوفر ضماناً كافياً فيما يتعلق بإحداث تغيير فعلي في السلوك. ولعل المؤشر الأكثر صلة، مع أن من المحتمل أن يكون تتبعه وتحليله أكثر تعقيداً، هو مقارنة عدد المستخدِمين الذين يمارسون سلوكيات غير محبذة (مثل النقر على رابط أو مرفق في رسالة للتصيد الاحتيالي تأتي عن طريق البريد الإلكتروني) خلال فترة زمنية معينة، خاصة قبل التدريب أو إطلاق تدخلات التوعية وبعد ذلك. وتشمل بعض الممارسات الجيدة الملاحَظة فيما يتعلق بالتدريب الإلزامي فرض تاريخ لانتهاء التدريب على الموظفين المنضمين حديثاً إلى القوة العاملة من أجل الحد من فترة التعرض لزيادة المخاطر بسبب عدم الوعي، وكذلك مطالبة الموظفين بالاشتراك في جلسات تنشيطية سنوياً للحفاظ على أثر التعلم مع الوقت.

الشكل السابع

التدريب الخاص بالتوعية بأمن المعلومات في عام 2020، حسب وحدة التدريب وعدد المنظمات المشارِكة في وحدة التفتيش المشتركة



المصدر: استبيان وحدة التفتيش المشتركة 2020.

100- **وجوب إيلاء اهتمام خاص للفئات الأخرى من الموظفين وللمستخدِمين العرضيين.** نحو نصف المنظمات المشارِكة فرضت التدريب على أساس إلزامي على أمن المعلومات لفئات أخرى من موظفيها، في حين أن نصفها الآخر إما وفّر هذا التدريب على أساس اختياري أو، ببساطة، لم يوفر هذه الفرصة. ويكتسي الانتباه إلى فئات الأشخاص غير الموظفين أهمية بالغة بالفعل. فكثيراً ما يضطر أعضاء هذه الفئات، بسبب قيود الموارد، إلى استخدام أجهزتهم الشخصية للدخول إلى البنية التحتية المؤسسية. وعلاوة على ذلك، فإن من غير المرجح أن يكون المستخدِمون غير المنتظمين للأنظمة والبنى التحتية المؤسسية على دراية باستخدامها الصحيح والآمن وفقاً لسياسات المنظمة وممارساتها المعمول بها. ويمكن للافتقار إلى آليات إنفاذ فعالة تتعلق بالأشخاص الذين لا يعدّون من ملاك العاملين بشكل مباشر، الأمر الذي يضعهم خارج نطاق الولاية التأديبية الكاملة للمنظمات، أن يؤدي إلى تثبيط الامتثال وتفاقم أوجه الضعف الموجودة فعلاً. وتبرز هذه التحديات بقوة أكبر في المنظمات التي يعتمد تكوين القوى العاملة فيها اعتماداً كبيراً على الاستشاريين والمتعاقدين والموظفين لفترات قصيرة. **ويذكّر المفتشون بأن مبادرات التدريب والتوعية يجب أن تشمل القوى العاملة بأكملها. فالتهديدات لا تميز بين أنواع المستخدِمين المختلفة. ولذلك يقترح المفتشون أن يتخذ الرؤساء التنفيذيون للمنظمات التي لم تجعل هذه الوحدات التدريبية إلزامية الإجراءات المناسبة.**

101- **التحديات المتعلقة بالتدريب.** تم إطلاع المفتشين على سلسلة من التحديات التي تواجهها المنظمات المشارِكة والتي يمكن أن تؤثر على تنفيذ البرنامج التدريبي الفعال في مجال الأمن السيبراني. وأشارت عدة منظمات إلى القيود المالية التي تحد من قدرتها على تطوير فرص التدريب أو توفير الوصول إليها، وقد اضطر بعضها إلى اختيار فئات معينة من المستخدِمين ليتم تدريبهم دون غيرهم، وهو ما يثير القلق. وتبرز الجوانب المالية بشكل أكبر بسبب طبيعة الموضوع السريعة التطور، والتي يمكن أن تجعل محتوى الدورة التدريبية قديماً بسرعة، مما يتطلب تحديثه وتوسيعه، وغالباً بتكلفة كبيرة. ويكمن التحدي الآخر في سأم المستخدِمين من التدريب، مما قد يؤثر على فعالية البرنامج. ويضيف ارتفاع معدل تبدُّل الموظفين والافتقار إلى السلطة على فئات معينة من العاملين مستويات إضافية من التعقيد. ويمكن أن تواجه الكيانات المنتشرة على المستوى الميداني مجموعة صعوبات خاصة بها، تماماً كما في أي فرص أخرى للتعلم. على أنه لا يمكن استكشاف هذا البعد بالكامل في سياق الاستعراض الحالي. أخيراً، أشار مسؤولو الأمن السيبراني إلى النقص العام في الإنفاذ في حالة عدم الامتثال لمتطلبات التدريب وربطوا ما يمكن من انعدام الفعالية في كثير من البرامج التدريبية بغياب العقوبات بصورة تجعل حتى التدريب الإلزامي اختيارياً بحكم الأمر الواقع. **ولضمان تحسين الإنفاذ، يقترح المفتشون أن ينظر الرؤساء التنفيذيون في إقامة رابط رسمي بين إكمال التدريب على أمن المعلومات وإجراءات الموافقة المؤسسية الأخرى.** ويمكن أن يشمل ذلك ربط الموافقة الأمنية على نشر العاملين ميدانياً ومنح أو تمديد حقوق الوصول إلى نظام تكنولوجيا المعلومات والاتصالات بتقديم الدليل على استكمال التدريب، بما في ذلك دورات "تجديد المعلومات". وهناك بالفعل سابقة لهذا النهج في مجال اعتبارات السلامة المادية قبل السفر في مهام رسمية، حيث يكون السفر مرهوناً بإكمال التدريب الأساسي على الأمن الميداني، وتُرفض الموافقة على السفر بدون ذلك التدريب.

102- **مبادرات التوعية في منظومة الأمم المتحدة.** هناك العديد من مبادرات التوعية السيبرانية في منظومة الأمم المتحدة بشأن مخاطر الأمن السيبراني والتدابير الموصى بها. ومن الأمثلة على ذلك أسبوع أكتوبر/تشرين الأول لأمن المعلومات، وهو مبادرة انضمت إليها عدة منظمات في مختلف أنحاء العالم تشمل جلسات تفاعلية وألعابا وجلسات إعلامية. وقد أشير إلى برامج منظمة العمل الدولية والمنظمة العالمية للملكية الفكرية على أنها مبتكرة وفعالة بشكل خاص، ويُعترف لبعضها بذلك في سياق المراجعات الخارجية. ومن الأفكار الإضافية التي تستحق المتابعة تركيز جلسات التوعية على المخاطر السيبرانية التي تؤثر على المجال الخاص (على سبيل المثال، المخاطر التي يواجهها الأطفال أو الصور العائلية الملتقطة للحصول على فدية) على أمل أن يجتذب ذلك مزيداً من الاهتمام وأن تنتقل الدروس المستفادة بشكل طبيعي إلى المجال المهني في العمل. وتنظم بعض المنظمات إحاطات شخصية يقدمها رئيس موظفي أمن المعلومات للموظفين الجدد، بينما تعزز منظمات أخرى الدروس المستفادة من خلال توزيع رسائل فيديو موجزة على الموظفين الذين وقعوا ضحية لهجوم سيبراني. وتعدّ حملات محاكاة التصيد الاحتيالي من أكثر وسائل التوعية شيوعاً ويُذكر أنها تحقق النتائج (الإطار 5).

الإطار 5

حملات محاكاة التصيد الاحتيالي تحقق النتائج

يشير التصيد الاحتيالي إلى إرسال رسائل بريد إلكتروني احتيالية تزعم أنها من مصدر حسن السمعة من أجل حمل الأشخاص على الكشف عن معلومات حساسة. ثم يستخدم المهاجمون هذه المعلومات للتمكن من الوصول غير المأذون به إلى أنظمة المنظمة، وذلك بقصد الاحتيال على المنظمة لتحقيق مكاسب مالية أو لدوافع تعطيلية أخرى.

وتحاكي حملات محاكاة التصيد الاحتيالي استراتيجيات القراصنة الحاسوبيين الواقعية وتساعد على تحديد المستخدِمين الأكثر عرضة للخداع ولحملهم على النقر على الروابط الضارة أو فتح المرفقات المصابة. وتستخدم هذه المحاكاة أيضاً لاختبار المهارات المكتسبة من خلال التدريب. ويتعين، لكي تكون أكثر فعالية، أن تكون مصحوبة بخدمات موجهة للمستخدِم مثل تحديد نقطة اتصال واضحة وإجراءات بسيطة ومعروفة على نطاق واسع يستطيع الموظفون استخدامها للإبلاغ عن الرسائل المشبوهة. وعلى سبيل المثال، قامت بعض المنظمات المشارِكة بإدراج آلية للإبلاغ عن رسائل التصيد الاحتيالي بالنقر على زر يوجد بشكل مباشر في تطبيق التراسل الإلكتروني الذي يستخدمه الموظفون.

وتوضح الأرقام التي عُرضت على المفتشين فائدة حملات محاكاة التصيد الاحتيالي هذه، حيث لاحظ مسؤولو أمن المعلومات عموماً انخفاضاً في نسبة المستخدِمين الذين يفتحون رسائل ومرفقات مشبوهة، وذلك نتيجة للحملات المتتالية. ولأغراض السياق، فإن الحصة المقبولة عموماً من المستخدِمين الداخليين غير الممتثلين، من أصل مجتمع المستخدِمين الأوسع، هي نحو خمسة في المائة من القوة العاملة، وفقاً لبعض مسؤولي الأمن السيبراني.

وتُنفَّذ حملات محاكاة التصيد الاحتيالي بشكل متكرر كأحد مكونات جهود اختبار الاختراق الأكثر شمولاً. وكثيراً ما تختصر هذه الجهود باعتبارها اختباراً للاختراق (pen ”testing“)، يتألف من سلسلة من التدريبات العملية التي تستهدف شبكة المنظمة وأنظمتها ومواردها البشرية لتحديد أوجه الضعف، ولقياس مستويات الامتثال للسياسات والإجراءات، وتقييم فعالية الدفاعات وإجراءات التعافي.

103- **الانتقال من الوحدات التدريبية إلى برامج التوعية المتسقة.** بدلاً من الاستمرار في تقديم فرادى الوحدات التدريبية للجميع دون الاسترشاد برؤية استراتيجية، **يشير المفتشون على المنظمات بأن تسعى إلى تطوير برنامج شامل للتدريب والتوعية له أهداف واضحة ومحددة لكل فئة من أصحاب المصلحة، وفقاً للمخاطر التي يمكن أن يمثلونها بالنسبة للمنظمة.** ومن شأن اتباع نموذج كهذا أن يضع المنظمات في موقع يمكّنها من أن تبتعد عن استهداف معدلات إكمال التدريب كمؤشر للامتثال وأن تنتقل إلى استخدام التدريب كأداة استباقية لتغيير ثقافة الأمن السيبراني الداخلية. ومن الناحية المثالية، يتعين أن يستخدم البرنامج طرقاً مبتكرة للتنفيذ تجمع بين العديد من النهُج والرسائل المكيفة لكل فئة. ولزيادة الشعور بالملكية وتيسير استيعاب التعلم بشكل أفضل في هذا المجال، قد ترغب المنظمات أيضاً في التفكير في إنشاء نظام للدعم من جانب الأقران، وتحديد الأفراد في جميع الإدارات الذين يمكن تدريبهم ليصبحوا أفراداً مرجعيين في تنفيذ البرنامج، وتوفير المساعدة العملية لأعضاء القوى العاملة الآخرين عندما، وحيثما، تدعو الحاجة.

طاء- تحقيق الاستفادة الأمثل من تخصيص الموارد المالية للأمن السيبراني

تقدير المستوى الحالي للموارد المكرسة للأمن السيبراني

104- موارد الأمن السيبراني المتاحة داخل منظومة الأمم المتحدة هي أقل عموماً من الموارد المتاحة للمؤسسات خارج المنظومة، ولكن يصعب تحديدها كمياً. يكاد يكون من الشائع القول إن الموارد المتاحة تحت تصرف مؤسسات منظومة الأمم المتحدة لتخصيصها لتكنولوجيا المعلومات والاتصالات بشكل عام،

وعلى وجه الخصوص للأمن السيبراني، تقل عن الموارد المقابلة لدى الكيانات ذات الحجم المماثل سواء في القطاع العام أو القطاع الخاص. على أنه يصعب تحديد الثغرة من حيث القيمة المطلقة والنسبية. فعلى سبيل المثال، يُقدَّر أن "أقل من واحد في المائة من إنفاق الأمم المتحدة يوجه إلى تكنولوجيا المعلومات والاتصالات، وأقل من واحد في المائة منه مخصص لأمن المعلومات، مقارنة بمتوسط صناعي يبلغ نحو سبعة في المائة"[(24)]. وفي محاولة لتقديم لمحة موجزة للوضع بالاستناد إلى الأدلة، أجرت وحدة التفتيش المشتركة استقصاءً للمنظمات المشاركة فيها حول مسألة تخصيص الموارد لكل من تكنولوجيا المعلومات والاتصالات والأمن السيبراني. ولعله ليس من المستغرب أن المفتشين توصلوا إلى نفس النتيجة التي توصلت إليها محاضر اجتماعات ندوة الفريق المختص بأمن المعلومات لعام 2018، والتي تفيد بأن تحديد الأرقام لا يزال بعيد المنال بالنسبة للمنظومة ككل.

105- **تعقيد تقدير الإنفاق على الأمن السيبراني والفائدة منه.** هناك عدة عوامل تجعل تحديد الموارد المتاحة للأمن السيبراني أمراً صعباً. فتتبع تكاليف الأمن السيبراني (الإطار 6) لا يجري عموماً كبند منفصل أو كفئة متميزة للنفقات. ويمكن أن يرد التمويل المتعلق بالأمن السيبراني مصنفاً تحت بند واحد أو تحت عدة بنود في الميزانية (مثل التكاليف التشغيلية أو تكاليف الموظفين أو تكاليف البنية التحتية أو المعدات) أو تحت بنود المجالات المواضيعية (على سبيل المثال داخل مظروف تكنولوجيا المعلومات والاتصالات أو خارجه). وتتفاقم صعوبة العثور على المعلومات حول موارد الأمن السيبراني ومستويات الإنفاق في وثائق الميزانية والبيانات المالية بسبب تنوع هياكل الميزانية، مما يتجلى في التعايش بين الميزانيات العادية والمساهمات الطوعية (الخارجة عن الميزانية)، والتي قد يشمل بعضها صناديق للاستثمار الرأسمالي قائمة بذاتها وتُستخدم في مشاريع البنية التحتية الواسعة النطاق للمنظمات. كما تميز عدة منظمات بين تكاليف الاستثمار (لمرة واحدة) والتكاليف التشغيلية (المتكررة)، مما يضيف مزيداً من الفروق الدقيقة إلى الصورة. وقد وُجد لدى إحدى المنظمات أن جزءاً كبيراً من موارد تكنولوجيا المعلومات والاتصالات موحدٌ عبر الميزانيات البرنامجية لوحدات الأعمال التي تحتفظ بقدرات تكنولوجيا المعلومات والاتصالات. وفي ظل هذه الخلفية، فإن تقديم أي بيان موثوق حول إجمالي الموارد المتاحة للأمن السيبراني يعدّ في حكم المستحيل. وعلى أي حال، فإن القيام بذلك معقد لدرجة لا تتناسب مع ما يُتوخى منه من فائدة: فمستوى الموارد المخصصة للأمن السيبراني في أية منظمة له قيمة إرشادية محدودة فيما يتعلق بمستوى الحماية المقدمة.

الإطار 6

تكاليف الأمن السيبراني

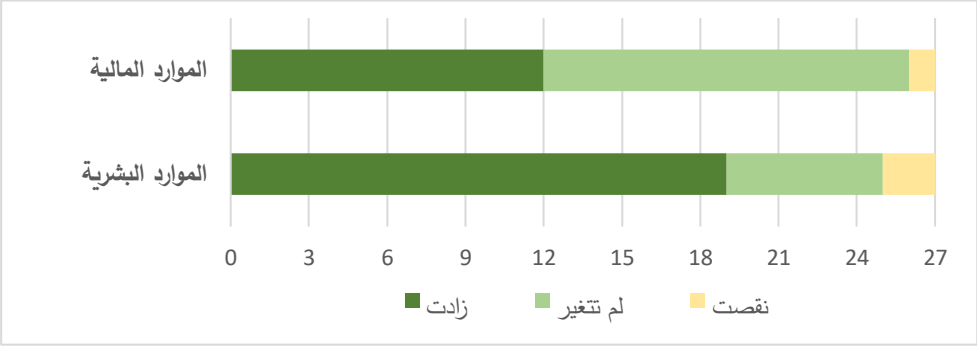
- **التكاليف المباشرة.** تتراوح التكاليف الواضحة (المباشرة) للأمن السيبراني من نفقات العاملين (من موظفين ومقاولين) والنفقات المتعلقة بالبنية التحتية مثل شراء الأجهزة والبرمجيات (تكاليف الاستثمار والصيانة ورسوم الترخيص) إلى الخدمات (مثل اشتراكات استخبارات التهديدات والخدمات الخارجية التي يوفرها مقدمو الخدمات التجاريون أو مركز الأمم المتحدة الدولي للحوسبة). وتختلف نسب توزيع هذه التكاليف بين المنظمات وهي تعكس خيارات كل منظمة في الموازنة بين القدرة الداخلية والاستعانة بمصادر خارجية.
- **التكاليف غير المباشرة.** بالإضافة إلى ذلك، هناك تكاليف أخرى (غير مباشرة) يتعين أخذها في الاعتبار عند تحديد تكلفة الأمن السيبراني. وفي الواقع، يرتبط الأثر المالي الكبير عادة بالتدابير المتخذة للحد من الضرر في أعقاب وقوع حادث، والتي تشمل تعبئة قدرات مخصصة لإعادة تشغيل الخدمات المعطلة، وإصلاح أوجه الضعف المكتشفة حديثاً، وخسائر الإنتاجية أثناء تعطل الأنظمة، وتدريب الموظفين على الوقاية من الخروقات والاستجابة لها بشكل أفضل، والحفاظ على صلاحية القدرات المتخصصة القائمة (البشرية والتكنولوجية).

(24) CEB/2018/HLCM/ICT/4.

106- **تشهد الآونة الأخيرة اتجاهاً نحو زيادة التمويل، ولكن القيود على القدرات لا تزال مستمرة.** يلاحظ المفتشون أن معظم المنظمات المشارِكة أشارت إلى زيادة في الموارد المخصصة للأمن السيبراني في السنوات الأخيرة (الشكل الثامن). وللوهلة الأولى، قد يبدو هذا اتجاهاً واعداً. على أنه، وكما يتضح من الرسم البياني، لا يبدو أن الزيادة المبلّغ عنها في الموارد المالية قد تُرجمت تلقائياً إلى زيادة في قدرات الموارد البشرية. وفي الواقع، حذرت الغالبية العظمى من المنظمات المشارِكة من أن المستوى الحالي للموارد المتاحة لا يزال يشكل عقبة أمام بناء إطار عمل فعال للأمن السيبراني، حتى أن إحدى المنظمات ذكرت أن تكاليف أمانها وحمايتها من التهديدات السيبرانية المتزايدة قد تضاعفت ثلاث مرات خلال فترتي السنتين الماضيتين. وقد وجدت التقييمات التي أجرتها المنظمات نفسها، أن القيود على الموارد أثرت بشدة على قدرات الموارد البشرية وتوافر الخبرات الداخلية، وعلى القدرة على القيام باستثمارات مناسبة في البنية التحتية لتكنولوجيا المعلومات والاتصالات، والقدرة على استبدال التطبيقات المتقادمة. بالإضافة إلى ذلك، في المنظمات التي تعمل في ظل قيود شديدة على الموارد أو في حدود ميزانيات ينعدم النمو فيها، يمكن أن تأتي الموارد المخصصة حديثاً للأمن السيبراني نتيجة لإعادة توزيع داخلي للموارد، وربما على حساب استثمارات أخرى، وهي في الغالب في مجال تكنولوجيا المعلومات والاتصالات دون أن تقتصر عليه وحده. ونظراً لأن ذلك قد لا يكون مستداماً على الأجل الطويل، فإن المفتشين يشعرون بالقلق إزاء كون الموارد المتاحة، حتى في حال زيادتها، ربما لم تشهد نمواً يواكب وتيرة التقدم التكنولوجي للمهاجمين وهيمنة تكنولوجيا المعلومات والاتصالات في عمل مؤسسات منظومة الأمم المتحدة. وعلى نحو ما أورده بدقة الفريق المختص بأمن المعلومات، فإن الاعتماد المتزايد على الخدمات الممكّنة سيبرانياً لم تقابله زيادة في الموارد لوظيفة أمن المعلومات[25].

الشكل الثامن

تطور موارد الأمن السيبراني وفق ما أفادت به المنظمات المشارِكة في وحدة التفتيش المشتركة (2015-2020)



المصدر: استبيان وحدة التفتيش المشتركة 2020.

107- **مصادر التمويل.** وفقاً للمعلومات المجموعة، تأتي موارد الأمن السيبراني في معظم المنظمات المشارِكة من ميزانيتها العادية بشكل أساسي. ويعتمد عدد منها على مزيج من الموارد العادية والموارد الخارجة عن الميزانية، في حين أن قلة منها تعتمد حصرياً على الموارد الخارجة عن الميزانية. ويمكن أن تساهم القدرة النسبية على التنبؤ بموارد الميزانية العادية في استدامة قدرات الأمن السيبراني، لكن هذا النهج يتطلب تخطيطاً استراتيجياً يضمن توفر الموارد المطلوبة عند لزومها. وفي الوقت نفسه، يمكن للموارد الخارجة عن الميزانية أن تتيح قدراً أكبر من المرونة وقد تكون أكثر جاذبية للمانحين الراغبين في تخصيص هذه الموارد للأمن السيبراني. ولدى قلة من المنظمات صندوق خاص، إما مكرس للبنية التحتية لتكنولوجيا المعلومات والاتصالات (منظمة الصحة العالمية) أو يمكن تعبئته للمشاريع المؤسسية الكبرى

(25) المرجع نفسه.

(المنظمة العالمية للملكية الفكرية والوكالة الدولية للطاقة الذرية). وكما أشير أعلاه في سياق خرائط الطريق الطويلة الأجل لتحسين إطار عمل الأمن السيبراني لدى المنظمات، تميل استثمارات هذا المجال بطبيعتها إلى أن يكون لها بُعد متعدد السنوات. ويعني ذلك أن دورات الميزانية الحالية قد تكون أقصر من أن تسمح بترسخ الاعتبارات الإستراتيجية الطويلة الأجل، وهي، مع ذلك، لا تتمتع بما يكفي من المرونة لتحريك الأموال بسرعة لمعالجة المتطلبات المخصصة القصيرة الأجل التي قد تنشأ في مجال تكنولوجيٍ ومشهدٍ للتهديدات، مثل الأمن السيبراني، يتميز بسرعة وتائره. ويمكن للصناديق الخاصة أن تسد هذه الثغرة، شريطة أن تمكنها مبادئ الحوكمة والشروط الخاصة بها، والتي وافقت عليها الهيئات التشريعية والإدارية، من القيام بذلك.

نحو تحقيق الاستفادة المثلى من استثمارات الأمن السيبراني

108- **وجوب تقديم دراسة جدوى تدعم طلبات الموارد الموجهة إلى الهيئات الإدارية.** من الواضح أن المنظمات لا يمكن أن تتوقع نجاح الطلبات التي تقدمها إلى الهيئات الإدارية لتخصيص الموارد إذا لم تتوفر المبررات المناسبة لإعطاء أولوية لاستثمارات الأمن السيبراني تتجاوز أولويات الإنفاق على مجالات أخرى في المنظمة. **وكنقطة انطلاق، يوصي المفتشون بأن تستند طلبات الموارد إلى تقييم شامل للمخاطر وإلى دراسة جدوى توضح بالتفصيل التكاليف والفوائد والمخاطر والوفورات المتوقعة وتشير إلى الآثار المالية المحتملة لعدم القيام بالاستثمار.** وتزداد فعالية هذا النهج عندما يقترن بخطة وجدول زمني مُقترحين للتنفيذ، على شكل خارطة طريق مثلاً، كما ذُكر في مكان آخر في هذا التقرير، وعندما يكون الإبلاغ عن التقدم المحرز منتظماً. ولاحظ المفتشون أن الهيئات الإدارية تصبح أكثر استعداداً لدعم هذا المسعى بتخصيص الموارد عندما تقدم الإدارة التنفيذية دراسة جدوى مقنعة تتضمن أهدافاً ومعايير واضحة للتحسين وتُدلل على ما للاستثمار من أهمية حاسمة، وهو ما حدث في السنوات الأخيرة في منظمة الطيران المدني الدولي، ومنظمة العمل الدولية، ومفوضية الأمم المتحدة لشؤون اللاجئين، والمنظمة العالمية للملكية الفكرية وغيرها من المنظمات. والممارسة هذه مشجعة، خاصة وأن من المرجح أن يتطلب تزايد تعقد تهديدات الأمن السيبراني زيادةً في الموارد، وليس تخفيضاً لها.

109- **يمكن بل ينبغي تحديد حجم نفقات الأمن السيبراني بدقة.** غني عن البيان أن وجود إطار قوي للأمن السيبراني محمي جيداً له ثمن، وإذا كانت مؤسسات منظومة الأمم المتحدة جادة بشأن حماية معلوماتها وأنظمتها وأصولها الرقمية، فإن عليها أن توفر الموارد المناسبة لأطر أمنها السيبراني. ولم تسفر محاولات تحديد المستوى المناسب للموارد المتعلقة بالأمن السيبراني كنسبة مئوية من الميزانيات المؤسسية لتكنولوجيا المعلومات والاتصالات عن نتائج مفيدة. إن فكرة التعبير عن كفاية الموارد من الناحية النقدية لا ينبغي أن تكون مقدسة، فالمال وحده لن يحل المشكلة. وقد طرح غارتنر المسألة بصراحة عندما قال إن كمية المال المنفق على الأمن السيبراني لا تعكس مستوى الحماية[(26)]. والأهم من السؤال عن كمية المال الذي ينبغي إنفاقه على الأمن السيبراني هو السؤال عن المجال الذي ستخصص له الموارد بحيث يكون لها أثر أكثر جدوى. وتشير الردود على استبياني وحدة التفتيش المشتركة إلى عدم الاتساق في نهُج تحديد أولويات الإنفاق على الأمن السيبراني، مما يزيد من مخاطر الاستخدام غير الفعال للموارد الشحيحة أصلاً. ومن الخيارات المُقنِعة للغاية، وإن كانت معقدة نوعاً ما ويتعين تهيئتها حسب الحال لتحديد حجم نفقات الأمن السيبراني بدقة، اتباع منهجية صارمة مثل هيكلية شيروود التطبيقية لأمن الأعمال (أو أي أداة أخرى مماثلة)، وهي هيكلية تستند إلى فكرة التتبع الثنائي الاتجاه. أي أن هيكلية الأمن المؤسسي بموجب هذا النهج تُعدّ بحيث يعالج كل شرط من شروط الأعمال من خلال عنصر مقابل واحد على الأقل من عناصر الضبط

(26) غارتنر، *الحاجة الملحة لمعاملة الأمن السيبراني كقرار خاص بالأعمال*، شباط/فبراير 2020.

الأمني، ويمكن رد كل عنصر من هذه العناصر إلى الاحتياجات المعلنة لأمن الأعمال[27]. وتستخدم المنظمة العالمية للملكية الفكرية بالفعل هذه المنهجية، وقد نوقشت أيضاً في سياق الفريق المختص بأمن المعلومات، **ويرى المفتشون أنها تستحق المزيد من الاستكشاف كوسيلة للحفاظ على تأسيس استثمارات الأمن السيبراني على احتياجات الأعمال وممارسات الإدارة السليمة للمخاطر، وربطها بها، وبالتالي تجنب الإفراط في الاستثمار، أو نقص الموارد، في وظيفة رئيسية لاستمرارية الأعمال.**

الإطار 7

يمكن أن توفِّر الحلول المفتوحة المصدر بدائل فعالة من حيث التكلفة

البرمجيات المفتوحة المصدر هي نموذج لتطوير البرمجيات وتوزيعها أصبح جزءاً أساسياً من صناعة تكنولوجيا المعلومات والاتصالات. وتُستخدم على نطاق واسع في مجال الأمن السيبراني بعضُ الأدوات المستندة إلى برمجيات مفتوحة المصدر، وتشمل جوانب مثل تبادل المعلومات الاستخبارية عن التهديدات، وإدارة الهوية والوصول، وتحليل الشبكات، وكشف القرصنة الحاسوبية والوقاية منها، والاستجابة للحوادث، والاستدلال الجنائي. وتشتهر بعض أمثلة البرامج مفتوحة المصدر بأنها موارد رائدة ضمن الفئات التي تنتمي لها.

وبينما تشير الردود على استبيان وحدة التفتيش المشتركة إلى أن بعض المنظمات المشارِكة تستكمل بالفعل حلولها المشتراة تجارياً والمطورة داخلياً ببرمجيات مفتوحة المصدر، فقد تتوفر فرصة لزيادة استخدام هذه الخيارات في كيانات الأمم المتحدة. ذلك أن هذه المصادر يمكن أن توفر حلولًا مناسبة، لا سيما للمنظمات التي تعمل في وضع يتميز بقلة الموارد.

وكما هو الحال مع أي منتج مسجل الملكية، ينبغي تقييم الحلول المفتوحة المصدر استناداً إلى مزاياها الخاصة، ولكن هناك بعض المزايا العامة التي ترتبط بشكل متكرر بمنتجات البرمجيات المفتوحة المصدر المصانة جيداً، مثل الشفافية والأمان وانخفاض تكلفة التراخيص والرسوم، واستخدام المعايير المفتوحة، والخطر المحدود المتمثل في التبعية لبائعين معينين.

ومع أن استخدام البرمجيات مفتوحة المصدر لا ينطوي عادةً على تكاليف تتعلق بالترخيص، إلا أن هذا لا يعني أنها مجانية تماماً. فتركيبها وتكوينها وصيانتها، وما يرتبط بها من إتقان تقني مطلوب، يعني ضمناً وقت الموظفين وبالتالي تكاليفهم. وقد لا تكون التكلفة الكاملة لملكية هذه المنصات واضحة بالنسبة للمنظمات ذات الموارد التقنية والخبرة المحدودة في استخدام هذه التطبيقات، مع أن هذا القيد غالباً ما ينطبق – بدرجات متفاوتة – على المنتجات التجارية أيضاً.

ولا يتعين على المنظمات أن تكتفي بالتفكير من منظور الملكية المسجلة البحتة أو النماذج المفتوحة المصدر الخالصة. فهناك منتجات تعتمد على نموذج هجين يهدف إلى الجمع بين أفضل ما في العالَمين، أي حرية وشفافية نهج المصدر المفتوح والدعم المنظم المقدم من موردين يتمتعون بمرونة الحركة. ويتمثل خيار آخر في استخدام كل من الأدوات المسجلة الملكية والبرمجيات مفتوحة المصدر لوظائف وأغراض مختلفة داخل المنظمة.

(27) يتوفر مزيد من المعلومات حول هيكلية شيروود التطبيقية لأمن الأعمال التطبيقية على الموقع التالي: https://sabsa.org/sabsa-executive-summary.

ياء- الاستثمار في موارد بشرية مكرسة ومتخصصة

وظيفة أمن المعلومات غير موجودة في جميع المنظمات المشارِكة

110- **تتجاوز المسؤوليات المرتبطة بالأمن السيبراني الدراية التقنية.** استثمرت غالبية المنظمات المشارِكة في التعاقد مع أصحاب الخبرات المتخصصة لتغطية أبعاد الأمن السيبراني المختلفة، وهم يوضعون أحياناً تحت قيادة رئيس موظفين مكرس لأمن المعلومات. وتشمل الجوانب الأساسية التي تدخل في مسؤولية الوظيفة ذات الصلة وضع الضوابط على المستوى التشغيلي من ناحية وتوجيه الإدارة على المستوى الاستراتيجي من ناحية أخرى، بهدف تحقيق أهداف حماية الأمن السيبراني على النحو المبين في التعريف المشار إليه في هذا التقرير. وبذلك فإن نطاق الوظيفة يتجاوز المجال الرقمي ولا يقتصر على توفير المعرفة التقنية. فهو ينطوي على مهام متنوعة، منها على سبيل المثال إنشاء إطار تنظيمي مؤسسي والتعريف به (وضع السياسات والتواصل)؛ وإسداء المشورة حول سبل تحديد المخاطر وإدارتها (إدارة المخاطر)؛ والتعاون مع وحدات الأعمال على إجراء تقييمات المخاطر وتحليل الأثر على سير الأعمال (الدور التنسيقي والتحليلي)؛ والتحقيق في الانتهاكات الجسيمة (قدرات التحقيق والتحليل)؛ والتوصية بإدخال تحسينات رقابية مناسبة وكذلك تنفيذها (الخبرة التشغيلية والتقنية)[28]. ويشير وصف المهام هذا إلى أن الدور يتضمن بُعداً إدارياً، سواء داخل بيئة تكنولوجيا المعلومات والاتصالات أو خارجها، ويتطلب العمل بتعاون وثيق مع مجموعة واسعة من أصحاب المصلحة، ولا سيما وحدات الأعمال في المنظمات. ولذا، فإن السلطة المفوضة إلى رئيس موظفي أمن المعلومات (وخبراء الأمن السيبراني بشكل عام) للتعريف بالتدابير وإنفاذها عبر المنظمة تكتسي أهمية قصوى.

111- **هناك تباين بين القدرات الداخلية.** وفقاً لبحوث أجرتها وحدة التفتيش المشتركة، هناك 16 منظمة مشاركة على الأقل قامت ببناء قدرات متخصصة ومكرسة داخلية في مجال الموارد البشرية، وهي قدرات تتراوح بين موظف وحيد لأمن المعلومات، معيّن أحياناً بدوام جزئي فقط، وبين وحدة تنظيمية أكبر يرأسها رئيسٌ لموظفي أمن المعلومات، بشكل عام برتبة ف-4 أو ف-5 (المرفق الخامس). وفي المقابل، في 10 منظمات مشارِكة، يتعامل مع مهام الأمن السيبراني بشكل رئيسي موظفو تكنولوجيا المعلومات والاتصالات من بين واجباتهم الأخرى. وهناك نسبة عالية من استخدام الخبراء الخارجيين بسبب الطبيعة التقنية المعقدة للمجال، والتي تتطور باستمرار وتتطلب درجة كبيرة من التخصص، مما يمثل تحدياً ويتطلب تكلفة لإبقائه متوفراً ومحدثاً على أساس دائم. ونتيجة لذلك، غالباً ما تُستكمل هذه الخبرة بتعيين عاملين مؤقتين، من خبراء استشاريين ومتعاقدين، أو بالاشتراك في خدمات مقدمي الخدمات التجارية أو خدمات مركز الأمم المتحدة الدولي للحوسبة. وأشار بعض المحاورين إلى أن ندرة الممارسين ذوي الخبرة في مجال الأمن السيبراني عالمياً تتدرج بين أكبر التحديات التي تواجهها مؤسسات منظومة الأمم المتحدة في إنشاء برامجها الخاصة بالأمن السيبراني وصيانتها وإدارتها. ولتوفير بديل للكيانات التي ليست في وضع يمكنها من إنشاء وظيفة مكرسة على الفور، يرغب المفتشون في تسليط الضوء على أن مركز الأمم المتحدة الدولي للحوسبة يقدم خدمة تسمى "الحوكمة الأمنية"، ويشار إليها أحياناً باسم "رئيس موظفي أمن المعلومات كخدمة"، وتشترك فيها حالياً ست منظمات مشارِكة، وهناك أربع منظمات أخرى استفادت من هذه الخدمة في الماضي. **ويرى المفتشون أن مؤسسات منظومة الأمم المتحدة بحاجة إلى تلبية المتطلبات المستقبلية للدراية في مجال الأمن السيبراني من خلال التخطيط السليم للموارد البشرية، لا سيما وأن المعارف والمهارات والقدرات اللازمة للتصدي لمخاطر الأمن السيبراني وتحدياته محددة بذاتها وقد لا يكون من السهل اجتذابها والاحتفاظ بها.**

(28) أنظر مؤسسة إطار مهارات عصر المعلومات (*SFIA*)، الإصدار 7، 2018.

112- **الاستثمار في قدرات مكرسة مسألة تستحق أن يُنظر فيها.** إدراكاً لكون الترتيبات المؤسسية ينبغي، في الوضع المثالي، أن تعكس حجم المنظمة ومتطلباتها المحددة استناداً إلى تقييم أجرته للمخاطر وإلى البيئة السيبرانية التي تعمل فيها، فإن الحقيقة تتمثل في وجود عوامل أخرى قد تكون أكثر حسماً. وعلى وجه التحديد، فإن ما لاحظه المفتشون من فوارق في البيئة الداخلية بين المنظمات المشارِكة قد تكون أكثر دلالة على القيود التي يواجهها كل منها بدلاً من كونها اختياراً مدروساً أو استراتيجياً. والواقع أن وظيفة الأمن السيبراني، في أربع منظمات مشارِكة، اعتُبرت حديثة التكوين على الأكثر، مما قد يعرض المنظومة بأكملها للمخاطر بشكل غير مباشر. **ويعتقد المفتشون أن وجود خبرة مكرسة ومتخصصة في مجال الأمن السيبراني داخل كل منظمة لا يساهم في تعزيز وضع المنظمة المعنية وحدها بل المنظومة ككل وبالتالي فهو استثمار مجدٍ.** وكما هو حال الوظائف الأخرى المرتبطة بالأعمال الأساسية للمنظمات، فإن بناء قدرة موارد بشرية داخلية دائمة لحماية المعلومات والأصول السيبرانية، حيثما أمكن، يُفضَّل عموماً على الاعتماد على موارد بشرية مؤقتة متعاقبة، وذلك لأسباب ليس أقلها المخاطر الإضافية المرتبطة باستخدامها ومحدودية قدرة المنظمات على الإنفاذ إزاء العاملين المنتسبين إليها (الفقرة 100). وعلاوة على ذلك، **فإنه يمكن لإنشاء وظيفة دائمة لرئيس موظفي أمن المعلومات للإشراف على هذه الخبرة وإدارتها أن يحقق ما يلزم من تركيز واتساق في النهج وأن يسهم، من وجهة نظر المفتشين، في تعزيز قدرة المنظمات المعنية على الصمود في المجال السيبراني.**

113- **ليس هناك قبول عام لتحديد المكان المناسب للأمن السيبراني في المنظمة.** خضعت مسألة المكان الأنسب للأمن السيبراني من حيث التسلسل الإداري للنقاش داخل منظومة الأمم المتحدة وخارجها، وهي مسألة لم تجد حلاً نهائياً يُمكن تطبيقه في جميع المنظمات. ولا تقدم المعايير الدولية توجيهات موثوقة فالأمر متروك لكل منظمة لتحديد المكان الأنسب وفقاً لاحتياجاتها وهيكلها. وفي أغلب الحالات، توضع وظيفة الأمن السيبراني في مؤسسات منظومة الأمم المتحدة ضمن إدارة تكنولوجيا المعلومات والاتصالات، مما ينعكس عموماً في تسلسل إداري مباشر يتبع رئيس هذه الإدارة أو ما يعادله. وقد يُنظر إلى هذا الترتيب الهيكلي المهيمن على أنه إرث من الماضي ولكنه يعكس واقعاً يتمثل في أن تكنولوجيا المعلومات والاتصالات تجتذب الأمن السيبراني عادة وبشكل طبيعي، استناداً إلى المعرفة والخبرة التكنولوجية اللازمة لإدارة أنظمة المعلومات ذات الصلة وغيرها من البنى التحتية للحماية. بالإضافة إلى ذلك، غالباً ما تكون إدارة تكنولوجيا المعلومات والاتصالات هي الجهة التي تصمم الاستجابة التشغيلية وتنفذها في حال التعرض لهجوم سيبراني، وقد يؤدي الفصل بين المجالين إلى خسائر في الكفاءة.

114- **إدارة تباين الأولويات في المنظمة بين وظائف تكنولوجيا المعلومات والاتصالات والأمن السيبراني.** بغض النظر عما ورد أعلاه، فإن وضع الموظف أو الفريق المسؤول عن الأمن السيبراني تحت سلطة رئيس إدارة تكنولوجيا المعلومات والاتصالات قد يخلق توتراً بين الأهداف الرئيسية التي يسعى إليها كل من المجالين، حيث أن إدارة المخاطر وأمن المعلومات هما الشاغل الرئيسي لرئيس موظفي أمن المعلومات، في مقابل ما لدى رئيس تكنولوجيا المعلومات والاتصالات من شواغل تتعلق بالفعالية التشغيلية وفعالية التكلفة وكذلك سرعة التنفيذ. فتضارب المصالح المحتمل واضح، وإن كان من السهل أن يعالج. ومن شأن الأخذ بنهج مفرط في التفكير التشغيلي إزاء الأمن السيبراني (مثل ذلك المرتبط بمتخصصي تكنولوجيا المعلومات والاتصالات) أن يضاعف التأثير السلبي على التنفيذ في المستقبل عندما تتحقق مخاطر سيبرانية يُحتمل أنها لقيت تجاهلاً في وقت مبكر. وفي الوقت نفسه، يمكن للموقف الذي يركز بشكل مفرط على تفادي المخاطر (مثل الموقف المنسوب إلى متخصصي الأمن السيبراني) أن يؤدي إلى شل الحركة التشغيلية بشكل غير مبرر وإعاقة تنفيذ الولايات بطرق أخرى. وتعدّ إدارة وحل التوترات بين الأهداف المختلفة في المنظمة، وتحديداً الآثار المترتبة على تخصيص الموارد لتلك الأهداف، جزءاً من المهام اليومية لكل مدير، والقيادة التنفيذية هي الأفضل لتحقيق التوازن في هذا الصدد.

115- **تمكين وظيفة الأمن السيبراني.** بصرف النظر عن تحديد المكان المناسب للأمن السيبراني في المنظمة، **يؤكد المفتشون أن من الأهمية بمكان ضمان فرصة التعبير عن اعتبارات الأمن السيبراني واستماع صانعو القرار المسؤولون إليها دون قيود.** فالوظيفة ينبغي أن توضع في مكان يتيح لها أن تخاطب الإدارة التنفيذية بشكل مستقل وأن تساهم بشكل فعال في الأطر المؤسسية الأخرى مثل الإدارة المركزية للمخاطر، وإدارة المعلومات والمعرفة، والسلامة المادية والأمن، والرقابة، وهو ما يدلِّل عليه هذا التقرير كله. ويتحقق ذلك بالشكل الأكثر فعالية عندما توجد آلية حوكمة داخلية قوية لأصحاب المصلحة المتعددين تشمل جميع الإدارات ذات الصلة. وقد قدمت المنظمة العالمية للملكية الفكرية ومنظمة الطيران المدني الدولي بعض الأمثلة المُفصلة جيداً لآليات حوكمة لأصحاب المصلحة المتعددين وللمستويات المتعددة.

116- **التدريب المتخصص.** بغض النظر عمن يُعين مسؤولاً عن الأمن السيبراني داخل المنظمة وما إذا كانت الوظيفة مركزة في شخص واحد أو في فريق أو موزعة بين عدة موارد بدوام جزئي، فإن من الأهمية بمكان أن يظل التدريب المتخصص متاحاً لجميع موظفي تكنولوجيا المعلومات والاتصالات الذين لديهم مسؤوليات متعلقة بالأمن، وذلك لضمان التحديث المستمر للمعرفة والمهارات. ويُذكر أن هذا التدريب لموظفي تكنولوجيا المعلومات والاتصالات، مثل مطوري البرمجيات أو مديري الأنظمة، متاح بالفعل في معظم المنظمات وينبغي مواصلة تشجيعه (الشكل السابع). ومن الناحية المثالية، ينبغي أن يتوفر برنامج تدريبي متين في مجال الأمن السيبراني، وأن تتوفر، عند الاقتضاء، عملية لإصدار الشهادات لموظفين مختارين من موظفي تكنولوجيا المعلومات والاتصالات، وذلك كعنصر أساسي في خطة عمل إدارتهم، على أن يُستكمل ذلك بميزانية مضمونة. فبدون تخصيص بعض الموارد لأغراض التطوير المستمر للمهارات، فإن الحفاظ على المعرفة المهنية لموظفي تكنولوجيا المعلومات والاتصالات يُترك لمبادرتهم الخاصة أو لمشاركتهم في التجمعات المهنية، وهو نهج يعتمد بشكل كبير على المواقف المهنية الفردية ولا يُرجح أن يتصف بالاستدامة. ويرحب المفتشون ببيانات عدة منظمات حول نيتها تعزيز هذا المجال، لكنهم يلاحظون أنه حتى في الحالات التي يسمح فيها مستوى الموارد بتقديم هذا التدريب المتخصص، فإنه يتحقق في معظم الأوقات على أساس مخصص بدون أهدافٍ تدريبية طويلة الأجل أو دون الأخذِ بنهج منهجي. وعلى وجه الخصوص، في الحالات التي لا تُخصص فيها قدرة موارد بشرية مكرسة لإدارة الأمن السيبراني بطريقة متسقة، تزداد أهمية إتاحة فرص التدريب الكافية للموظفين الذين يُطلب منهم تغطية المكونات ذات الصلة.

من شأن وجود مركز للعمليات الأمنية أن يوفر الاتساق في استجابة الأمن السيبراني التشغيلية

117- **الوظائف الرئيسية لمركز للعمليات الأمنية.** مركز العمليات الأمنية هو وحدة في المنظمة تركز على عمليات الأمن السيبراني اليومية. وفي حين أن هناك بالضرورة اختلافات بين أشكاله المختلفة، فإن أوسع ولاية ممكنة للمركز تجعله مسؤولاً عن مراقبة أمن الكيان من خلال منع حوادث الأمن السيبراني واكتشافها وتحليلها والاستجابة لها. وكثيراً ما يقول خبراء الأمن السيبراني إن مركز العمليات الأمنية يتألف من الأشخاص والتكنولوجيا والعمليات وهو المحور المركزي لجمع تدفقات المعلومات من مصادر مختلفة، وللربط بينها وتحليلها، في الوقت الفعلي. ويمكن أن تتضمن المعلومات الداخلية التي يجمعها ويعالجها هذا المركز بيانات من مصادر من قبيل الأجهزة الشبكية والخوادم والتطبيقات المستضافة وأجهزة الحاسوب المكتبية والأجهزة المحمولة وأنظمة الأمن المادي وأجهزة الأمن المتخصصة. كما يقوم مركز العمليات الأمنية بجمع ومعالجة المعلومات الاستخبارية عن التهديدات من المصادر الخارجية، وهو يرجع عادةً إلى مجموعة من المصادر المفتوحة (بما في ذلك المعلومات الحكومية المتاحة للجمهور) واستخبارات التهديدات التجارية، والتي تُربط ببيانات تُجمع وتُحلل داخلياً بحثاً عما يشير إلى تهديدات ناشئة. ونظراً لتعقيد المهام والخبرات المتنوعة المطلوبة، فإن إنشاء وصيانة مركز للعمليات الأمنية مجهز وعامل كلياً يمكن أن يكون مهمة معقدة ومكلفة. ويتعين على كل منظمة أن تجيب، في ضوء متطلباتها الخاصة، على الأسئلة حول ما إذا كان هذا المركز ضرورياً، وفي هذه الحالة، ما إذا كان ينبغي إنشاؤه داخلياً أو شراؤه من مقدم خدمات خارجي.

118- **الحلول الداخلية أو الخارجية أو المختلطة لمراكز العمليات الأمنية: يلاحظ وجود ترتيبات متنوعة عبر المنظمات.** هناك آراء متباينة بين المنظمات المشارِكة حول مزايا وعيوب الحلول الداخلية مقابل الحلول الخارجية، وهو ما يدل عليه تنوع الترتيبات والممارسات التي وجدها المفتشون أثناء استعراضهم. وتعتمد بعض المنظمات على مركز عمليات أمنية افتراضي أو موزع بمعنى أن بعض وظائفه منتشرة عبر مجموعة لا مركزية من موارد الموظفين. وقد اتخذ عدد من الكيانات قراراً بإنشاء مركزها الداخلي، في حين أن بعض الكيانات الأخرى تستخدم مركزاً خارجياً يوفره مقدمو الخدمات التجاريون أو يجري تقاسم المركز مع كيانات أخرى من خلال خدمة متصلة بمركز الأمم المتحدة الدولي للحوسبة، إما بشكل حصري أو بالاقتران مع وجود قدرة داخلية أساسية. وفي بعض الحالات، قامت المنظمات التي تستخدم هذه الحلول المختلطة برسم خط بين الوظائف الإستراتيجية والوظائف المتعلقة بالرقابة، والتي تظل مُدارة داخلياً، في حين أن الرقابة التشغيلية، لا سيما عند الحاجة إلى الرصد على مدار الساعة ("7/24")، تُترك لمقدمي الخدمات الخارجيين. بل إن هناك قلة من المنظمات تستخدم أكثر من مركز واحد للعمليات الأمنية، مما يتيح لها فصل أجزاء معينة من البيانات ذات الحساسية الخاصة عن مجموعات البيانات الموكلة إدارتها لجهات خارجية. ولاحظ المفتشون أن بضعة منظمات مشارِكة تنظر حالياً في إنشاء مركز للعمليات الأمنية كخيار.

119- **عناصر يُنظر فيها لأغراض ترتيبات مركز العمليات الأمنية.** تشمل الحجج المؤيدة لإنشاء مركز داخلي القدرةَ على الاستجابة بسرعة أكبر للتهديدات وأوجه الضعف ولممارسة رقابة أفضل على أجهزة الاستخدام النهائي، مع أن التكلفة أعلى. ويذكر أن ذلك يتحقق من خلال زيادة الرؤية المباشرة لهذه الأجهزة وحالتها، مع إمكانية المعالجة الآنية لوضعها من حيث تعرضها للمخاطر. وعلاوة على ذلك، يُعتبر المركز الداخلي وسيلة فعالة لإضفاء المركزية على وظائف الأمن السيبراني، مما يؤدي، وفقاً لإجماع واسع في الصناعة، إلى تحسين قدرة المنظمة على الصمود في المجال السيبراني بشكل عام. وبالنسبة للعديد من مؤسسات منظومة الأمم المتحدة، فإن تكلفة تشغيل مركز داخلي للعمليات الأمنية يمكن أن تكون باهظة، وقد لا تتناسب الفوائد المحققة مع وضع الأمن السيبراني لهذه المنظمات ومتطلبات الحماية المرتبطة به. ولا يستطيع سوى عدد قليل من كيانات الأمم المتحدة تحمل تكاليف الاحتفاظ ببرنامج كامل للأمن السيبراني لمواجهة التهديدات والاستجابة لها بشكل مستقل بالاعتماد على القدرات الداخلية وحدها. علاوة على ذلك، وحتى لو تمكنت هذه الكيانات من إنشاء هياكل مناسبة، فإن من الممكن ألا تتمكن من الحفاظ على قوة دائمة تحت الطلب من خبراء الأمن السيبراني المتعددي المهارات والمدربين الذين يمكنهم الاستجابة للهجمات السيبرانية المعقدة، وهي أميل لأن تكون غير متواترة أو منتظمة، مما يعني ضمناً بعض التقلبات فيما يلزم توفره من الخبرات. بالإضافة إلى ذلك، تعتبر بعض المنظمات أن الحفاظ على قدرة داخلية كاملة لإدارة جميع المهام التشغيلية لا يمكن أن يضاهي خبرة مقدمي الخدمات الخارجيين المتخصصين، الذين يميلون أيضاً إلى الحصول على موارد أفضل للاستثمار في التطوير والبحث الذي يعتبر لا غنى عنه لمجال الأمن السيبراني الدينامي. وفي الوقت نفسه، وحتى عندما تختار الكيانات الاستعانة بمصادر خارجية، يُدلّل على الحاجة لوجود مستوى كافٍ من القدرات الداخلية ولتمثيل بعض وظائف الأمن السيبراني الأساسية داخل الكيان، والتي توفر معرفة متخصصة بسير العمل الداخلي والعمليات الداخلية ويمكن أن تكون أيضاً بمثابة واجهة فعالة للتعامل مع مقدم الخدمات الخارجي. وفي الحالات التي تُستخدم فيها مراكز خارجية للعمليات الأمنية، تصبح إدارة الباعة أيضاً شاغلاً رئيسياً ويجب ضمان فحصهم الدقيق، وإدراج بنود للحماية القانونية المناسبة في العقود، وتجنب التبعية أو "الارتهان" للباعة. كما يمكن لبعض الاعتبارات المؤيدة أو المعارضة للاستعانة بمصادر خارجية لمهام مركز العمليات الأمنية، أن تنطبق فيما يتعلق بالقرارات الأخرى المتصلة باستخدام القدرات الداخلية مقابل القدرات الخارجية لإدارة الأمن السيبراني، ويرد تلخيص لها في الإطار 8.

الإطار 8

استخدام مقدمي الخدمات الخارجيين للحصول على خدمات مركز العمليات الأمنية وخدمات الأمن السيبراني الأخرى

الايجابيات:

- يضمن توافر مجموعات وأدوات المهارات المتنوعة والحديثة والعالية التخصص
- يمكن أن يؤدي إلى كفاءة التكلفة
- يوفر إمكانية التوسع فيه أو تخفيض حجمه وفقاً لطبيعة التهديدات المتغيرة باستمرار ومتطلبات القدرات المتقلبة
- الحياد والنزاهة الملحوظان

السلبيات:

- التعرض للتبعية ("الإرتهان") للباعة
- إمكانية مواجهة صعوبات في تهيئة خدمات وحلول موحدة، مما يؤدي إلى الأخذ بحلول غير مرنة ودون المستوى الأمثل
- زيادة الاعتماد على موظفين غير معروفين أو غير خاضعين للتدقيق يوضعون تحت سيطرة المديرين المباشرة
- ما يُحتمل من إطلاع أطراف ثالثة على البيانات الحساسة
- محدودية الشفافية فيما يتعلق بالإبلاغ عن الحوادث
- التكاليف

120- **من شأن وجود مركز للعمليات الأمنية أن يُحسِّن اتساق استجابة الأمن السيبراني.** ينبغي على كل منظمة أن تقيّم ما إذا كانت ستنشئ هذا المركز استناداً إلى تحليل للتكلفة والعائد يتضمن معايير مثل مستوى التعقيد في بيئتها الخاصة بهيكلية تكنولوجيا المعلومات والاتصالات، وعدد الأصول والعمليات الحيوية المدارة ونوعها، والحجم الإجمالي لتدفق البيانات، وبالتالي تواتر التهديدات، مما قد يعني مستويات مختلفة من الحاجة إلى الرصد والحماية المستمرين. ويود المفتشون أن يسلطوا الضوء على أن أحد الجوانب المهمة لإنشاء مركز رسمي للعمليات الأمنية – بغض النظر عن حجمه وقدرته – يتمثل في التركيز والاتساق الذي يوفره للرصد اليومي والعمليات اليومية في المنظمة. وحتى لو كان الفريق صغيراً جداً ويحتاج إلى الاستعانة بموظفين لتكنولوجيا المعلومات والاتصالات موجودين في مكان آخر في المنظمة، أو بمقدمي الخدمات الخارجيين، فإنه يبقى قادراً على أداء دور التنسيق والمزامنة الحاسم وعلى التوعية في المنظمة. **لذلك يقترح المفتشون أن ينظر الرؤساء التنفيذيون في خيار إنشاء مركز للعمليات الأمنية أو تجميع القدرات الموجودة في آلية معادِلة استناداً إلى استعراض نقدي لاحتياجاتهم المؤسسية وللقدرات الداخلية والخارجية المتاحة فعلاً تحت تصرفهم، وأن يتأكدوا من أنهم قادرون على إثبات الأسباب التي يستند إليها قرارهم بتأسيس، أو بعدم تأسيس، مركز للعمليات الأمنية.**

كاف- التفكير في الجهود المبذولة على نطاق المنظمة من أجل تحسين القدرة على الصمود في المجال السيبراني، والإبلاغ عن هذه الجهود

121- تؤثر درجة انعكاس العناصر الواردة تفاصيلها في هذا الفصل في نهج المنظمة إزاء الأمن السيبراني تأثيراً مباشراً على موقفها وقدرتها على تحديد التهديدات السيبرانية ومنعها واكتشافها، فضلاً عن قدرتها على الاستجابة للحوادث والتعافي منها. وإدراكاً لأن الترتيبات القائمة قد تكون مدفوعة بخيار استراتيجي أو تشغيلي أو تمليها اعتبارات أخرى، ينبغي للرؤساء التنفيذيين أن يبادروا بإجراء استعراض على نطاق المنظمة ككل لدراسة مدى إدراج كل عنصر من هذه العناصر في سياسات منظمتهم وممارساتها.

122- ويُنتظر أن يؤدي تنفيذ التوصيتين التاليتين إلى تعزيز فعالية استعداد مؤسسات منظومة الأمم المتحدة واستجابتها في مجال الأمن السيبراني.

التوصية 1

ينبغي للرؤساء التنفيذيين لمؤسسات منظومة الأمم المتحدة أن يُعدّوا، على سبيل الأولوية وفي موعد لا يتجاوز عام 2022، تقريراً شاملاً عن إطار عملهم الخاص بالأمن السيبراني وأن يقدموه إلى هيئاتهم التشريعية ومجالسهم الإدارية في أقرب فرصة، على أن يغطي العناصر التي تسهم في تحسين القدرة على الصمود في المجال السيبراني على النحو المطروح في هذا التقرير.

123- وينبغي إبلاغ الهيئات التشريعية والإدارية بالاستنتاجات التي يخلص إليها هذا الاستعراض الداخلي، مع مراعاة أوجه القوة والضعف التي يتم تحديدها، فضلاً عن تقديم مقترحات لاتخاذ التدابير الكفيلة بزيادة تعزيز القدرة على الصمود في المجال السيبراني. ويرى المفتشون أن ذلك يضع الهيئات التشريعية والإدارية في وضع أفضل لتوفير التوجيه الاستراتيجي الرفيع المستوى بالإشارة إلى إصدار بيان صريح بشأن درجة تقبل المخاطر فيما يتعلق بمسائل الأمن السيبراني، ولتخصيص الموارد لبلوغ المستوى المطلوب من الحماية. وكما ورد أعلاه، ينبغي أن تنظر الإدارة التنفيذية في تقديم تقارير منتظمة عن مسائل الأمن السيبراني إلى الهيئات التشريعية والإدارية. ويقر المفتشون بأن جانباً من المعلومات المقدمة في مثل هذا التقرير قد تكون حساسة وقد يتعين أن تعالج بمستوى مناسب من السرية. **ولذا، تُنبّه الإدارة التنفيذية إلى وجوب توخي أقصى درجات الحذر في اختيار شكلٍ وقناةٍ للإبلاغ يوفران معلومات كافية للهيئة التشريعية والإدارية المعنية دون تعريض دفاعات المنظمة للخطر.**

التوصية 2

ينبغي للهيئات التشريعية والإدارية في مؤسسات منظومة الأمم المتحدة أن تنظر في التقارير المتعلقة بالعناصر التي تسهم في تحسين القدرة على الصمود في المجال السيبراني والتي أعدها الرؤساء التنفيذيون، وأن تقدم توجيهات استراتيجية بشأن ما يتعين تنفيذه من تحسينات أخرى في منظماتهم، حسب اللزوم.

رابعاً- الأمن السيبراني من منظور المنظومة ككل

ألف - الأمن السيبراني - هل هو أولوية على نطاق المنظومة ككل؟

124- **التعاون على نطاق المنظومة ككل في مجال الأمن السيبراني - أولوية معلنة منذ زمن طويل.** دأبت الدول الأعضاء ومسؤولو الأمم المتحدة على أعلى المستويات الممكنة، منذ سنوات طويلة، على القول إن تعزيز وضع الأمن السيبراني لمنظومة الأمم المتحدة يحظى بالأولوية. من ذلك مثلاً أن الجمعية العامة، في عام 2008، شجعت الأمين العام، بصفته رئيس مجلس الرؤساء التنفيذيين، على تعزيز التنسيق والتعاون بشكل أعمق فيما بين منظمات الأمم المتحدة في جميع المسائل المتعلقة بتكنولوجيا المعلومات والاتصالات، والتخطيط المركزي للموارد، ولا سيما في مجالات الأمن والتعافي من الكوارث واستمرارية العمل[29]. وفي عام 2013، شجعت اللجنة الاستشارية لشؤون الإدارة والميزانية الأمين العام، في سياق استعراضها لتقرير عن التقدم المحرز في تنفيذ التوصيات المتعلقة بتعزيز أمن المعلومات والأنظمة في الأمانة العامة، على مواصلة التعاون على نطاق المنظومة والتماس جميع الخيارات لزيادة التعاون وتبادل الحلول فيما يتعلق بأمن المعلومات بين مؤسسات منظومة الأمم المتحدة[30]. ومؤخراً، في عام 2019، في سياق اختتام مناقشةٍ على مستوى مجلس الرؤساء التنفيذيين، شدد الأمين العام نفسه على أهمية تعزيز قدرة منظومة الأمم المتحدة على حماية نفسها من الهجمات السيبرانية[31]. ويتمثل الافتراض الأساسي في هذا الصدد في أن زيادة التعاون على مستوى المنظومة، بما في ذلك النهُج المشتركة والحلول التشغيلية المشتركة، هي من العوامل الرئيسية لتحقيق مستوى أفضل من الحماية للمنظومة ككل.

125- **محاولات التوصل إلى نهج استراتيجي مشترك.** على النحو المذكور، تواجه مؤسسات منظومة الأمم المتحدة في الغالب نفس التحديات والتهديدات في البيئة السيبرانية، مما يمكن أن يعني أن هناك إمكانية لابتكار نهج مشترك إزاء الاستجابة. بالنظر إلى أن أمن المنظومة يعتمد، جزئياً على الأقل، على أمن فرادى مؤسساتها الأعضاء نظراً للترابط بينها على مختلف المستويات، فإن هناك أيضاً سبباً قوياً لتحقيق ذلك. وأثناء التحضير لهذا الاستعراض، دعت عدة منظمات مشارِكة إلى وضع استراتيجية مشتركة تملكها وتنفذها وتبلغ عنها الوكالات كشركاء يعملون بشكل متضافر يدفعهم هدف مشترك يتمثل في تحقيق مستوى معين من النضج في المنظومة ككل، على أساس مجموعة من المعايير الدنيا التي يتعين أن يستوفيها الجميع. وقد ورد في محاضر شبكة تكنولوجيا المعلومات والاتصالات لعام 2017[32] طلبٌ لوضع استراتيجية للأمن السيبراني على مستوى المنظومة من أجل المساعدة في التأسيس لممارسات متسقة للأمن السيبراني للمنظومة ككل. غير أنه لا يبدو أن هذه المبادرة تحققت أو توبعت بأي معنى ملموس. وهناك محاولة أخرى لتعزيز نهج منسق تضمنت اقتراحاً بإجراء استقصاء سنوي للمنظمات بشأن تدابير الأمن السيبراني الخاصة بها، وذلك بهدف إعداد معيار داخلي للنضج وتحسين تقييم تعرض المنظومة العام للمخاطر. وعلى الرغم من الأعمال التحضيرية الهامة التي تضمنت جولتين لاستقصاء تجريبي شملتا نحو 20 منظمة خلال عامي 2018 و2019، فإن الاقتراح لم يجتذب دعماً جماعياً على مستويات الإدارة العليا في ذلك الوقت. وتمثلت الحجج الرئيسية التي طُرحت عند رفض جهود المقارنة هذه، من ناحية، في تنوع هياكل المنظمات والسياقات التي تحد من قيمة التقييم الجماعي، ومن ناحية أخرى، في محدودية استعداد الكيانات لتبادل تقييماتها الداخلية لأمنها السيبراني خارج منظمتها، مع التدليل

(29) قرار الجمعية العامة 262/63.

(30) A/68/7/Add.11، الفقرة 6.

(31) CEB/2019/2، الفقرة 39.

(32) CEB/2017/HLCM/ICT/9، الصفحتان 7-8.

بفعالية على كون مخاطر الأمن السيبراني هي العقبة الرئيسية أمام متابعة التقييم، وحتى التقييم التراكمي. وأشارت الآراء المعرب عنها خلال المقابلات إلى أن جائحة كوفيد-19 ربما أحدث تغييراً في التصورات والعقليات فيما يتعلق بالأمن السيبراني وأن المقترحات التي كانت تعتبر سابقاً طموحة أو غير واقعية قد تحظى بفرصة أكبر لتوليد الاهتمام والترحيب اليوم. والواقع، أن النقاش حول فرصة تطبيق نموذج نضج مرجعي مشابه للنموذج الذي اعتمده مؤخراً منتدى إدارة المخاطر التابع لمجلس الرؤساء التنفيذيين، يبدو أنه قد عاود الظهور في سياق اجتماع خبراء الأمن السيبراني الأخير المشترك بين الوكالات.

126- **المسؤولية الجماعية عن ضمان توفر حدٍ أدنى من الدفاع.** قد يكون السعي لتحقيق التنسيق الكامل على نطاق المنظومة، لا سيما استناداً إلى استنتاجات تُستخلص من تقييم مقارن للنضج بين المنظمات، مفرطاً جداً في الطموح وحتى خارج الموضوع. وكما ذكر مجمع الفكر غارتنر، فإن محاولة المقارنة بين ترتيبات وتدابير الأمن السيبراني لدى المنظمات قد تخلص إلى بيانات بشأن النضج النسبي لكل منظمة ولكنها لا تعطي أي إشارة موثوقة حول المستوى المطلق لحماية أي منها[33]. على أن التبعية المتبادلة للسمعة والعمليات بين مؤسسات منظومة الأمم المتحدة تجعل من مسؤوليتها الجماعية رفع الحد الأدنى إلى أعلى مستوى ممكن للجميع ومساعدة بعضها بعضاً لبلوغه. وتجدر الإشارة إلى أن المنظمات التي تتمتع بإطار متقدم للأمن السيبراني وقدرات داخلية أو خارجية قوية،، كانت، هي تحديداً، الأكثر دعماً للجهود ذات الصلة. وإقامة التوازن المطلوب أمر صعب، ولكن من الأهمية الحاسمة أن تجد المنظومة التوازن الصحيح بين متطلبات كل من المنظمات المشارِكة، وترتيباتها الحالية، وأن تأخذ بنهج على مستوى المنظومة ككل لتحديد الحد الأدنى من المعايير الذي يتعين على كل المنظمات تحقيقه ولصالحها جميعاً. **ويرى المفتشون أن تحديد المستوى الأساسي للحماية ومتطلبات الدفاع الدنيا لمؤسسات الأمم المتحدة، وبالتالي للمنظومة ككل، يظل هدفاً صالحاً يستحق المتابعة.**

127- **الجهود المبذولة لإنشاء قدرة مشتركة على المستوى التشغيلي.** نوقشت عدة مرات وعلى مستويات مختلفة مسألة القدرة الموحدة على مستوى المنظومة لمنع التهديدات والهجمات السيبرانية واكتشافها والاستجابة لها. فمنذ ما يقرب من 10 سنوات، أصدرت شبكة تكنولوجيا المعلومات والاتصالات خارطة طريق لإنشاء فريق استجابة للحوادث الحاسوبية تابع للأمم المتحدة[34]. ولم تنفذ تلك المبادرة، إذ أنه لم يتم التوصل إلى اتفاق بشأن نموذج التمويل في ذلك الوقت. وفي الآونة الأخيرة، استأنف الفريق المختص بأمن المعلومات عمله بشأن تقييم جدوى إنشاء مركز للعمليات الأمنية مشترك بين كيانات الأمم المتحدة، غير أن المناقشة بين أعضاء الفريق سلطت الضوء على مجموعة من التحديات المتبقية (توزيع التكاليف، والمواءمة مع القدرات المتنوعة الموجودة مسبقاً، والاتفاق على النطاق المتوقع للدعم، وأولوياته، في حال وقوع هجوم واسع النطاق، وما إلى ذلك). واستندت هذه الجهود إلى توقع أن قدرات الاستجابة للحوادث على نطاق المنظومة ككل ستتمتع بإمكانية تحقيق مكاسب كبيرة في الكفاءة مع توفير حماية أكبر في الوقت نفسه، خاصة للمنظمات التي لا تستطيع الاحتفاظ بقدرة احتياطية بانتظار وقوع هجوم قد يحدث في أي وقت. على أن هذه المحاولات توضح أن الأهداف، مع أنها واضحة وتحظى بدعم جيد، تواجه صعوبات أكبر مما يمكن أن نتوقعه في ترجمتها إلى ممارسة عملية. وتُظهر التجربة أنه في اللحظة التي تصل فيها الأهداف إلى مستوى ملموس معين، فإن تنفيذها يصبح بعيد المنال.

128- **التدريب والتوعية كمرشح متناقض للجمع بين الموارد على نطاق المنظومة ككل.** يعتبر التدريب والتوعية في مجال الأمن السيبراني مثالاً على الاقتراح الواعد الذي ثبت أنه متناقض إلى حد ما

(33) غارتنر، *الحاجة الملحة لمعاملة الأمن السيبراني كقرار خاص بالأعمال*، شباط/فبراير 2020.

(34) CEB/2013/5، الفقرتان 38-39.

عند الفحص الدقيق. وقد استعرض تقرير صدر مؤخراً عن وحدة التفتيش المشتركة التعاون في برامج التعلم في منظومة الأمم المتحدة[35]. وخلص أحد استنتاجات التقرير إلى وجود ازدواج كبير في الجهود المبذولة في إنشاء برامج مماثلة من جانب منظمات مختلفة. وللوهلة الأولى، تبدو موارد التدريب والتوعية في مجال الأمن السيبراني خياراً طبيعياً للتعاون ولتجميع الموارد على مستوى المنظومة. واستناداً إلى افتراض أن معظم التدريب الموجه للمستخدِمين النهائيين يمكن أن يكون موحداً، نظراً لأن جانباً كبيراً من مواد التعلم ذات الصلة ليس محدداً بمنظمة معينة بسبب طبيعة التهديدات المشتركة، فقد انطوى أحد المشاريع المشتركة الأولى التي أكملها الفريق المختص بأمن المعلومات على تطوير مكونات أساسية لمنهج مشترك للأمن السيبراني لتكييفها واستخدامها من جانب أعضاء الفريق. ويبدو أن النهج القائم على وضع منهج مشترك اكتسب بعض الزخم لدى عدد من المنظمات، واختارت هذه المنظمات اعتماد الوحدة التدريبية للتوعية بأمن المعلومات عبر الإنترنت المعمول بها في الأمانة العامة للأمم المتحدة، أو استخدمت مركز الأمم المتحدة الدولي للحوسبة وخدمة التوعية بأمن المعلومات التابعة له لتكييف وتهيئة المحتوى ذي الصلة. غير أن المفتشين لم يكتشفوا أي توافق قوي في الآراء بين المنظمات المشارِكة فيما يتعلق بفائدة اتباع نهج مشترك إزاء التدريب. والواقع أن عدة منظمات اعترضت بقوة على اتباع نهج موحد، مستشهدة على وجه التحديد بالخصوصيات المتعلقة بالولاية أو القيود التي تفرضها عملية التطوير الجماعية الطويلة في كثير من الأحيان والتي تؤدي إلى تقادم سريع للمحتوى المطور بشكل مشترك، ولا تيسر استبداله، في حين أنه بالضرورة يدور حول نهج "القاسم المشترك الأدنى" وقد لا يرقى إلى مستوى توقعات المستخدِمين واحتياجاتهم دون الحاجة إلى استثمارات كبيرة لاحقة للمزيد من التكييف والتوسع. وفي ضوء هذه الاعتبارات، طور عدد من المنظمات وحدات تدريبية خاصة بها، أحياناً بالتعاون مع مقدمي خدمات خارجيين، وبتكلفة ليست بالضئيلة. **والمفتشون باقون على قناعتهم بأن مؤسسات منظومة الأمم المتحدة ستستفيد من قدر من التدريب المنسق، حتى ولو كان من الضروري تكييفه وفقاً لاحتياجات بعض المنظمات.**

129- **تحقيق الاستفادة الأمثل من موارد الأمن السيبراني.** كان هناك توافق في الآراء بين جميع الخبراء والمديرين الذين تمت مقابلتهم حول حقيقة أن كيانات الأمم المتحدة، بشكل فردي وجماعي، هي جهات فاعلة صغيرة مقارنة بكيانات من القطاع الخاص، وأن الموارد المتاحة لها لمواجهة الهجمات الخارجية الأكثر تعقيداً والتي تشنها الجريمة المنظمة أو الهجمات المدعومة الأخرى هي موارد محدودة في أحسن الأحوال. وفي الوقت نفسه، غالباً ما تخصص المنظمات المشارِكة الموارد للأمن السيبراني بمعزل عن غيرها ولأغراض خاصة بها، وأحياناً تحت ضغط الاستجابة لحدث معين. وهناك شعور قوي داخل المنظومة بأن هناك كفاءات يمكن اكتسابها من خلال التعامل مع الأمن السيبراني بطريقة مشتركة. على أن الردود الواردة من المنظمات المشارِكة في وحدة التفتيش المشتركة بشأن المجالات التي يمكن أن يكون فيها تجميع الموارد مجدياً ومفيداً أدت إلى ردود فعل متباينة. ويتمثل أحد المجالات التي حظيت بالدعم، كمصدر لتحقيق وفورات محتملة في التكاليف، في تحقيق تنسيق أوثق فيما يتعلق بالتعاقد مع مقدمي الخدمات الخارجيين، وتحديداً الكيانات التجارية وكيانات القطاع الخاص. وأكد كثير من المنظمات أنها تستخدم مقدمي الخدمات هؤلاء، وذكرت غالباً أسماء نفس الشركات لنفس الخدمات أو لخدمات مماثلة، بما في ذلك تقييمات المخاطر أو أوجه الضعف، أو المراجعات المتعلقة بالمعيار 27001، أو لحلولِ برمجيات محددة، مما يعني ضمنياً أن كل منظمة أخضعت الشركات للفحص الداخلي الخاص بها ولإجراءات إدارة الباعة لديها، كما أنها دفعت تكاليف تلك الشركات بشكل منفصل. وعلى الرغم من وجود اتفاق اعتراف متبادل وقعته 20 منظمة، فقد أشارت قلة قليلة فقط من المنظمات إلى أنها استفادت من مذكرات التفاهم أو الترتيبات المماثلة فيما بينها للاعتماد على عمليات الشراء أو عقود الخدمات المتعلقة

(35) JIU/REP/2020/2.

بالحماية والاستجابة في مجال الأمن السيبراني. ويدرك المفتشون أن هناك عوامل تحد من التنفيذ الواسع النطاق لهذه المبادرات المشـــتركة، بيد أن هذه المبادرات، مع ذلك، تتطلب مزيداً من الاهتمام لتحقيق مكاســب في الكفاءة. وحدد المفتشــون، من خلال المقابلات والاســتبيان، عدداً من التحديات التي تواجه الشـراء المشـترك والشـراء التعاوني بشـكل عام. فإجراءات الشـراء وقواعده المختلفة في المنظومة تشـكل حواجز في وجه تطبيق الشـــراء التعاوني وتحدّ منه. على أن بعض العقبات لا تتعلق مباشـــرة بالقواعد والإجراءات بل بالثقافة التشـــغيلية لدى المنظمات، والتي قد لا تســـمح بالتعاون المفتوح، بل تفضـــل أن تسيطر المنظمة بشكل صارم على شؤونها الخاصة. وفي هذا السياق، تشمل بعض الحواجز فوارق في الفلسفة التشغيلية بين المشتريات الشديدة المركزية والمشتريات اللامركزية، وفوارق في طرائق التمويل (من قبيل المدفوعات المسبقة)، والافتقار إلى المواءمة في أنظمة تكنولوجيا المعلومات والاتصالات وفي أنظمة الحسابات المستحقة الدفع، على النحو المبين في تقرير وحدة التفتيش المشتركة بشأن المسائل المتعلقة بالمشتريات[36]. وعلى أقل تقدير، فإنه ينبغي على المنظمات المشارِكة، في حال ثبوت عدم جدوى الشراء المشترك لخدمات معينة، أن تبذل كل ما في وسعها لتنسيق جهودها قدر الإمكان. فبخلاف لذلك، ومن خلال ممارسات الشراء غير المتسقة، فإنها تخاطر بتحفيز مقدمي الخدمات التجاريين على فرض رسوم مختلفة على نفس الخدمة عبر المنظومة، مما يخلق شكلاً من أشكال المنافسة التي لا تفيد إلا مقدمي الخدمات هؤلاء بينما تُضر بالمصالح المالية للمنظمات المعنية.

130- **لا تُبذل جهود متضـــافرة حقاً على مســـتوى المنظومة ككل بما يتجاوز التنســـيق والحلول التشـــغيلية الجزئية**. يمكن القول إن الأهمية الكبيرة والزخم اللذين اكتسبهما الأمن السيبراني على أعلى المستويات قد خلقا الظروف المثلى لزخم قوي باتجاه إنشاء قدرة على مستوى المنظومة ككل. ومع ذلك، وعلى الرغم من وجود عدد من الموارد والآليات والمبادرات الهامة المتاحة داخل المنظومة، بما في ذلك ما يبدو من توفر الإرادة السياسية، فإن الأدلة على التقدم في جعل هذه التصريحات الطموحة حقيقة واقعة لم تكن واضحة على الإطلاق. وفي الوقت الحالي، لا يوجد كيان واحد مكلف رسمياً بقيادة مسألة النهج المنسق إزاء الأمن السيبراني، ولا بوضع حلول مشتركة لمؤسسات منظومة الأمم المتحدة وتنفيذها. فالجهود المبذولة على نطاق المنظومة بشأن الأمن السيبراني تتركز مؤسسياً، في الوقت الحاضر، حول آليات التنسيق المشتركة بين الوكالات في إطار مجلس الرؤساء التنفيذيين، وهي تتلقى الدعم التشغيلي، إلى حد ما، من مركز الأمم المتحدة الدولي للحوسبة كمقدمٍ لبعض الخدمات المشتركة لعدد من مؤسسات منظومة الأمم المتحدة. وفي هذا الفصل، يبحث المفتشون في الترتيبات المؤسسية والتشغيلية لدى المنظمات، بما في ذلك ما يبدو أنه درجة من الانفصام بينها، وفي الديناميات السائدة المشتركة بين الوكالات بشأن هذه المسألة (المرفق السادس). ويسعى المفتشون كذلك إلى تحديد التقدم المحرز حتى الآن، والفوائد والقيود المتأصلة في التكوين الحالي، والمجالات التي قد تتوفر فيها إمكانية لاتخاذ إجراءات جماعية أقوى لاستنباط استجابات لمنظومة الأمم المتحدة ككل، بقدر ما يكون ذلك عملياً ومعقولاً.

باء- الآليات المشتركة بين الوكالات للتعامل مع الأمن السيبراني

131- **تاريخ طويل من الاهتمام من جانب الآليات المشتركة بين الوكالات**. برز الأمن السيبراني، تحت عنوان "أمن (أنظمة) المعلومات" في الخطاب المعني بتكنولوجيا المعلومات على مستوى المنظومة منذ أيام لجنة التنسيق الإدارية. ففي وقت مبكر من عام 1994، عُهد إلى فرقة عمل أنشأها سلف شبكة تكنولوجيا المعلومات والاتصالات (ما يُعرف منذ عام 2018 باسم الشبكة الرقمية والتكنولوجية) باستعراض مجموعة

(36) أنظر JIU/REP/2013/1.

من "المبادئ التوجيهية لأمن نظام المعلومات لمنظمات الأمم المتحدة" كانت قد نُشـــرت في عام 1992[37]، مما يشير إلى وجود قدر كبير من الاهتمام بهذه المسألة ومن الجهود المستثمرة فيها حتى قبل ذلك التاريخ. وتجدر الإشـارة إلى أن المبادئ التوجيهية تمثل جهداً شـاملاً وتدريجياً بشـكل مدهش لتحديد الأبعاد المتنوعة للأمن السـيبراني، وتقديم توجيهات بشـأنها، على المسـتويين الإداري والتشـغيلي، وينبغي ألا تَصـرف المصـطلحات المسـتخدمة في الوثيقة، وهي قديمة إلى حد ما، الانتباه عن حقيقة أن جزءاً لا يسـتهان به من محتوياتها وتوصياتها لا يزال ذا صلة حتى بعد مرور 30 عاماً.

132- **اسـتمرار الاهتمام بنهج منسـق إزاء الأمن السـيبراني**. بقيت فكرة الاسـتجابة المنسـقة للتهديدات السيبرانية ظاهرة في الوثائق الرسمية بعد 10 سنوات من ذلك، أي في عام 2002، عندما أدرك أعضاء مجلس الرؤسـاء التنفيذيين أنه "في حين أن الاحتياجات الأمنية للمنظمات تتدرج في فئات مختلفة (إذ أن لدى بعضـها مصـارف بيانات شـديدة السـرية والحسـاسية)، فإن هناك مسـائل مهمة مشـتركة بين جميع المنظمات لا بد من معالجتها على وجه السـرعة"[38]. وفي عام 2010، بدا أن مصـطلح "أمن المعلومات" قد اسـتُبدل بمصـطلح "الأمن السـيبراني" الذي اكتسـب زخماً كبيراً عندما جرى التدليل مرة أخرى على وجوب تحديد "مخطط عام لنهج على مستوى المنظومة ككل" إزاء الأمن السيبراني، يصف تداعيات التهديدات السيبرانية على "جميع القطاعات" باعتبارها "تسـونامي سـيبراني محتمل"[39]. وفي السـنوات اللاحقة، وردت بيانات مماثلة على مسـتوى اللجنة الإدارية الرفيعة المسـتوى فيما يتعلق باكتشـاف "أرضـية مشـتركة واسـعة فيما يتعلق بأفضـل طريقة لحماية [مؤسـسـات منظومة الأمم المتحدة] من تعطل الأعمال والتهديدات الأمنية"[40]، بينما ذكرت شـبكة تكنولوجيا المعلومات والاتصالات أن "تعزيز قدرة الوكالات على مقاومة التهديدات السيبرانية يجب أن يظل أولوية"[41].

133- **في عامي 2013 و2014، اعتُمدت وثائق تاريخية للمنظومة ككل بشـأن الأمن السـيبراني والجريمة السـيبرانية**. وفي عام 2010، كلف مجلس الرؤسـاء التنفيذيين اللجنة الإدارية الرفيعة المسـتوى واللجنة الرفيعة المسـتوى المعنية بالبرامج بمناقشـة هذه المسـألة بشـكل مشـترك تحت قيادة الاتحاد الدولي للاتصـالات ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، وانضـم إلى هذا العمل لاحقاً مؤتمر الأمم المتحدة للتجارة والتنمية وبرنامج الأمم المتحدة الإنمائي واليونسـكو. وتُوجت هذه المبادرة الجامعة بالموافقة على الإطار الشـامل للأمم المتحدة ككل بشـأن الأمن السـيبراني والجريمة السـيبرانية في عام 2013[42]، واسـتناداً إلى ذلك الإطار، أعِدَّت في عام 2014 خطة التنسـيق الداخلي لمنظومة الأمم المتحدة بشـأن الأمن السيبراني والجريمة السيبرانية[43]. وفي حين أن كلتا الوثيقتين ركزتا أساساً على البعد "المواجه للخارج" لعمل الأمم المتحدة (أي الأنشطة البرنامجية المصممة لدعم الدول الأعضاء في مساعيها بشأن هذا الموضوع)، فقد وفرتا نقطة انطلاق قوية لتأطير البعد "المواجه للداخل" للأمن السـيبراني في المنظومة (الإطار 9). ومع ذلك، يلاحظ المفتشـون أن أية منظمة مشـاركة لم تشـر لا إلى إطار العمل ولا إلى الخطة أثناء التحضير للاستعراض. وبينما لا يبدو أن الخطة في حد ذاتها قد أصبحت نقطة مرجعية دائمة للمنظومة، فقد كان هناك تأكيد للمفتشين على أن المبادئ والعناصر الأساسية الواردة فيها لا تزال توجه خطة عمل الهيئات ذات الصلة المشتركة بين الوكالات النشطة في هذا المجال.

(37) اللجنة الاستشارية لتنسيق أنظمة المعلومات، "المبادئ التوجيهية لأمن أنظمة المعلومات لمنظمات الأمم المتحدة"، نيويورك، 1992.

(38) CEB/2002/HLCM/10، الفقرة 8.

(39) CEB/2010/1، الفقرة 53.

(40) CEB/2013/5، الفقرة 36.

(41) CEB/2013/2، الفقرة 58

(42) المرجع نفسه، الفقرة 85 والمرفق الثالث (الإطار الشامل للأمم المتحدة ككل بشأن الأمن السيبراني والجريمة السيبرانية).

(43) خطة التنسيق الداخلي لمنظومة الأمم المتحدة بشأن الأمن السيبراني والجريمة السيبرانية، تشرين الثاني/نوفمبر 2014، وثيقة داخلية.

الإطار 9

إطار العمل وخطة التنسيق الداخلي على مستوى المنظومة ككل بشأن الأمن السيبراني والجريمة السيبرانية

يرسي إطار العمل الشامل للأمم المتحدة ككل بشأن الأمن السيبراني والجريمة السيبرانية الذي أقره مجلس الرؤساء التنفيذيين في دورته العادية الثانية لعام 2013، الأساس للتنسيق بين مؤسسات منظومة الأمم المتحدة استجابة لشواغل الدول الأعضاء فيما يتعلق بالجريمة السيبرانية والأمن السيبراني.

إطار العمل:

- يقدم بعض التعاريف المشتركة للمفاهيم الأساسية ويحدد نطاق الموضوع
- يسلط الضوء على التقاطع بين الولايات ذات الصلة لدى الكيانات المعنية
- يُرسي مبادئ أساسية للتطوير البرنامجي والمساعدة التقنية فيما يتعلق بالجريمة السيبرانية والأمن السيبراني
- يتضمن توجيهات بشأن تعزيز التعاون في تقديم المساعدة التقنية للدول الأعضاء في هذا الصدد.

واستناداً إلى هذا الإطار، وُضعت خطة التنسيق الداخلي لمنظومة الأمم المتحدة بشأن الأمن السيبراني والجريمة السيبرانية في عام 2014 لتوجيه التنسيق الداخلي بين مؤسسات منظومة الأمم المتحدة في مجال الأمن السيبراني والجريمة السيبرانية، وهي تتمحور حول خمسة مواضيع أبرزَها الأمين العام التماساً لما يمكن من عمل مشترك في المنظومة ككل. وحددت الخطة لكل موضوع مجموعةً من المبادئ المشتركة ونقاطاً للعمل ودُعيت المنظمات لاعتمادها. وشُجع الرؤساء التنفيذيون، على وجه الخصوص، على إعداد وإطلاق دورة تدريبية حاسوبية إلزامية بشأن الأمن السيبراني للموظفين، تستند إلى منهج تدريبي توافق عليه شبكة تكنولوجيا المعلومات والاتصالات، وعلى إنشاء فريق مشترك بين المنظمات للتصدي للحوادث الحاسوبية. وقد اعتبر رئيس اللجنة الإدارية الرفيعة المستوى أن نقاط العمل هذه ذات صلة أيضاً بعمل اللجنة (CEB/2014/5، الفقرة 72).

وللموضوع التالي صلة خاصة بهذا الاستعراض:

الموضوع 1: ضمان التحضير الداخلي الفعال للتعامل مع التهديدات السيبرانية، على مستوى فرادى الوكالات ولمنظومة الأمم المتحدة ككل، بما في ذلك العقبات أمام السياسات والموارد والتي قد تمنع الوكالات من العمل المشترك معاً لحماية منظومة الأمم المتحدة، وبصورة أفضل، من خلال أمور منها، على سبيل المثال، إدراج الأمن السيبراني في الأطر الخاصة بتقييم المخاطر وبإدارة المخاطر.

134- **الفريق المختص بأمن المعلومات باعتباره منتدى الخبراء الرئيسي على نطاق المنظومة ككل بشأن الأمن السيبراني.** بشكل عام، تبين أن الآلية المشتركة بين الوكالات التي تتعامل مع الأمن السيبراني في منظومة الأمم المتحدة مترسخة منذ زمن طويل وتعمل عموماً بشكل فعلي. فالفريق المختص بأمن المعلومات، الذي أُنشئ في عام 2011 باعتباره الآلية الرئيسية داخل منظومة الأمم المتحدة لتعزيز التعاون والتشارك بين الوكالات لتحسين أمن المعلومات داخل المنظمات الأعضاء، وهو مسؤول أمام الشبكة الرقمية والتكنولوجية ويتلقى التوجيهات منها، ويعمل بتوجيه عام من الجنة الإدارية الرفيعة المستوى. واستناداً إلى اختصاصاته، فإن عضويته تقتصر حصراً على رؤساء موظفي أمن المعلومات في المنظمات الأعضاء في مجلس الرؤساء التنفيذيين أو ما يعادلهم. وفي الحالات التي لا توجد فيها هذه الوظيفة، فإن موظف تكنولوجيا المعلومات والاتصالات هو الذي يمثل المنظمة المعنية عادة. وتشمل طرائق عمل الفريق تنظيم ندوة سنوية بمشاركة متحدثين خارجيين، وعقد جلسة تنفيذية لاتخاذ القرارات

الرسمية خلال الندوة السنوية، وتشكيل أفرقة عاملة محددة زمنياً مع منظمات رائدة تتطوع لقيادة المداولات حول الموضوعات ذات الأهمية. وتشارك عدة منظمات غير أعضاء في مجلس الرؤساء التنفيذيين في أعمال الفريق المختص بأمن المعلومات كمراقبين لا يتمتعون بحق التصويت، بينها مركز الأمم المتحدة الدولي للحوسبة. ويرأس الفريق على أساس التناوب أحد أعضائه الرسميين، وكان يضطلع بهذا الدور وقت كتابة هذا التقرير مكتب تكنولوجيا المعلومات والاتصالات التابع للأمانة العامة للأمم المتحدة.

135- **تأكيد فائدة وجود هيئة رئيسية مشتركة بين الوكالات كمنتدى للتبادل.** اكتسب الفريق المختص بأمن المعلومات مصداقية مهنية كبيرة باعتباره المنتدى الرسمي الذي يجتمع فيه ممارسو الأمن السيبراني في الأمم المتحدة على أساس منتظم لمناقشة التحديات والفرص والممارسات الجيدة للمنظومة ككل. ويؤكد تحليل محتوى التقارير الأخيرة لندوات الفريق أن هناك نقاشاً واهتماماً ثريين داخل الفريق فيما يتعلق بمجموعة واسعة من القضايا التشغيلية والاستراتيجية، مثل الأمن السحابي وإدارة المخاطر السحابية، وإدارة الهوية الرقمية، ومعايير قياس النضج في الأمن السيبراني، والتدريب على التوعية بأمن المعلومات، ومؤخراً فكرة إنشاء مركز مشترك للعمليات الأمنية، بالإضافة إلى توحيد الخدمات الاستخباراتية الخاصة بالتهديدات. والواقع أن حوالي ثلثي المنظمات المشارِكة، ذكرت في ردها على استبيان وحدة التفتيش المشتركة، أنها تعتبر الفريق المختص فعالاً في تعزيز التعاون والتآزر بين كيانات الأمم المتحدة وتقدر مساهمات أعضائه الفنية فضلاً عما يُتيحه من فرص للتبادل مع الخبراء الخارجيين، بما في ذلك القطاع الخاص. وأشاد العديد من الأعضاء بجهود رئيس الفريق في تيسير النقاش المهني والدفع بعجلة التقدم في خطة عمله. وقد نوقشت بالفعل بعض الجوانب الأكثر ضعفاً في عمل الفريق، مثل انخفاض تواتر ندواته وقلة التفاعل بين الدورات، وهو تفاعل يرى بعض الأعضاء وجوب زيادته لتيسير المزيد من الحوار المتواصل غير الرسمي. واستجابة للحاجة الواضحة في هذا الصدد، أنشئت قناة مكرسة للرسائل الفورية للتبادل غير الرسمي المباشر بين أعضاء الفريق من أجل التواصل السريع وتبادل المعلومات عند الضرورة. وقد أشار رؤساء موظفي أمن المعلومات بشكل إيجابي إلى الجهود الداعمة للتبادلات اليومية، كما أكدوا استخدامهم لهذه القنوات بنشاط في عملهم اليومي.

136- **الأجهزة المشتركة بين الوكالات تبقي الأمن السيبراني قيد النظر الفعلي على جميع المستويات.** ابتداء من الفريق المختص بأمن المعلومات نفسه وإلى الشبكة الرقمية والتكنولوجية واللجنة الإدارية الرفيعة المستوى، كان هناك ما يدل على أن الأمن السيبراني محلُّ نقاش نشط ويُعترف بأهميته البالغة. وعلى مستوى الشبكة الرقمية والتكنولوجية، التي تجمع رؤساء إدارات تكنولوجيا المعلومات والاتصالات وتتلقى تقارير وتوصيات الفريق المختص بأمن المعلومات لإقرارها وإحالتها إلى اللجنة الإدارية الرفيعة المستوى، يدرج "أمن المعلومات والأمن السيبراني" بين أهداف الشبكة العشرة المحددة في اختصاصاتها المنقحة عام 2019[(44)]. وعلى صعيد الممارسة العملية، يمكن القول إن الشبكة الرقمية والتكنولوجية تقدر بشكل عام عمل الفريق، فهي لم تخرج إلا في قلة من الحالات عن موقف الفريق الخاص، وقد أقرت معظم توصياته، مع تعديلها في بعض الأحيان. وعلى مستوى اللجنة الإدارية الرفيعة المستوى، التي لعبت دوراً مهماً في تطوير إطار العمل لعام 2013 وخطة التنسيق لعام 2014، ظهر الأمن السيبراني في الخطط الاستراتيجية للجنة، بما في ذلك أحدثها (2017-2020)، كعنصر من عناصر الأولوية الاستراتيجية لإدارة المخاطر وبناء القدرة على الصمود. وتتضمن الخطط الاستراتيجية الأخيرة بياناً يشير إلى أن اللجنة الإدارية الرفيعة المستوى ستنخرط في جهد متجدد لتعزيز رصد التهديدات السيبرانية والاستجابة لها، بما في ذلك تنفيذ تدابير التخفيف على مستوى المنظومة[(45)]. على أن محاضر اللجنة الإدارية الرفيعة

(44) CEB/2019/HLCM/DTN/03/R1، صفحة 2.

(45) CEB/2016/HLCM/15، صفحة 13.

المستوى، مع أنها تعترف بوضوح بالأمن السيبراني كمسألة مثيرة للقلق بشكل عام، تُظهر أن التوصيات والبنود المحددة المتعلقة بالموضوع نادراً ما تصل إلى اللجنة. وفي هذا السياق، لاحظ المفتشون أن ثلث المنظمات المشارِكة فقط ذكرت في معرض ردها على استبيان وحدة التفتيش المشتركة، أنها تعتبر الفريق المختص فعالاً في توليد الزخم للعمل على المستويات العليا من آلية مجلس الرؤساء التنفيذيين.

137- **يعتمد تنفيذ مشورة وتوجيه الفريق المختص بأمن المعلومات على أعضائه.** وجد المفتشون، في سياق هذا الاستعراض، أن التنسيق والتعاون بين الوكالات بشأن الأمن السيبراني في منظومة الأمم المتحدة لم يسفر بعد عن أية نتائج متوقعة منه. وفي حين أنه يُحرز قدرٌ كبير من العمل المفاهيمي على أساس سنوي من خلال الفريق، ومع أن هذه المسألة تحظى باهتمام الإدارة العليا، إلا أن هناك تباطؤاً في تحقق تقدم نحو الحلول المشتركة والنهُج المشتركة أو المنسقة والمشاريع المشتركة. ولأغراض السياق، تجدر الإشارة إلى أن الصيغة الأخيرة لاختصاصات الفريق، المنقحة في عام 2018[(46)]، تعكس التزامه بتقاسم المعرفة والخبرات والحلول وتشمل بشكل خاص تنفيذ المشاريع المشتركة. والواقع أنه في وقت لاحق من ذلك العام، بمناسبة تحول شبكة تكنولوجيا المعلومات والاتصالات لتصبح الشبكة الرقمية والتكنولوجية، وإعادة النظر في ولايات كل فريق من أفرقتها الفرعية، ذهبت الشبكة المعادة تسميتها إلى أبعد من ذلك، إذ قررت أن على الفريق المختص، بالإضافة إلى دفعه بعجلة التعاون وتبادل المعرفة المشترك بين الوكالات في مجال أمن المعلومات، أن يصبح أكثر نشاطاً في تصميم الحلول والابتكارات المشتركة وتنفيذها[(47)]. على أنه لا يبدو أن رؤية الشبكة الرقمية والتكنولوجية لانخراط فريقها الفرعي في تطوير حلول أكثر عملية لصالح المنظومة تتفق مع تزويده بأي مستوى من القدرات التشغيلية بشكل مستقل عن الموارد الداخلية لأعضائه والمستوى الفردي للعمل في هذا الصدد. ويفتقر الفريق المختص بأمن المعلومات في الواقع إلى آلية فعالة لتيسير التنفيذ والتفعيل المشترك للحلول الموضوعة أو للاتفاقات المبرمة في السياق المشترك بين الوكالات. ومع ملاحظة أنه ليس من مسؤولية هيئة للتنسيق في المقام الأول أن تهتم بتنفيذ توصياتها الخاصة، فإن المفتشين يرون أن الافتقار إلى "ذراع تشغيلية" مرخص لها رسمياً للمنظومة ككل تخضع لتوجيه مجموعة من رؤساء موظفي أمن المعلومات وتخدم المصلحة المشتركة، يشكل أحد العوامل الرئيسية التي تعوق التقدم نحو التوصل إلى نهج إزاء الأمن السيبراني على نطاق المنظومة ككل. وتتناول الفروع التالية من هذا التقرير بمزيد من التفصيل مسألة ما إذا كان بإمكان آليات أو هيئات أخرى قائمة أن تسدّ بشكل معقول الثغرة في التنفيذ.

138- **تمكين رؤساء موظفي أمن المعلومات كأفراد وكجماعة.** تبين للمفتشين أن أعضاء الفريق المختص بأمن المعلومات ليسوا على نفس المستوى، فمشاركتهم تتراوح بين مستوى العمل وبين المستوى الاستراتيجي، إذ أن بعض رؤساء موظفي أمن المعلومات يشغلون مناصب مبتدئة في الفئة الفنية في حين أن آخرين منهم يؤدون أدواراً إدارية متوسطة إلى عليا أو يرأسون إدارات بأكملها. وإلى جانب الخبرة التقنية وثقافة المناقشة الصريحة التي تميز النقاش داخل الفريق، وفقاً لأعضائه، فقد ذُكر أن عدم التجانس في العضوية يؤثر على ديناميات العمل داخل الفريق ويؤثر بصورة مباشرة على قدرته على تزويد المنظومة بتوجيهات موثوقة. ونظراً لأن تمكين كل عضو يختلف باختلاف هياكل المنظمات والقيود المرتبطة فيما يتعلق بإلزام الكيان في السياقات المشتركة بين الوكالات، فإن الفرص محدودة للقيام بدور تحويلي، سواء داخل منظمة العضو المعني أو بشكل جماعي من خلال العمل المتضافر عبر المنظومة. وتواجه الفريق كهيئة معنية بالتنسيق نفس التحديات التي تعترض أي آلية أخرى مشتركة بين الوكالات تغيب فيها سلطة اتخاذ القرار لفرض العمل مباشرة على مستوى المنظومة، ولذا بالذات فإن من غير الواقعي أن نتوقع أن

(46) CEB/2018/HLCM/ICT/3/Rev.1.

(47) CEB/2018/HLCM/ICTN/18، صفحة 6.

يتحقق التنفيذ في هذا المنتدى. وفي الوقت نفســـه، ليس للفريق أثر يذكر على كيفية نقل نتائج عمله إلى الإدارة العليا داخل كل منظمة. ويتضــح من محاضــر الشــبكة الرقمية والتكنولوجية أن هذه القيود مفهومة جيداً، وهو ما تدلّ عليه دعوة الشـبكة لأعضــائها – رؤســاء إدارات تكنولوجيا المعلومات والاتصــالات – لتمكين رؤساء موظفي أمن المعلومات، من بين آخرين، من خلال تفويضـهم بسـلطة إضـافية[48]. وتجدر الإشارة أيضـاً إلى أن الفريق نفسه مسؤول أمام الشبكة الرقمية والتكنولوجية، وهو بالتالي يعكس الترتيبات السائدة وما يرتبط بها من تحديات لوحظت في معظم المنظمات حيث يُعتبر رئيس موظفي أمن المعلومات مسؤولاً أمام رئيس إدارة تكنولوجيا المعلومات والاتصالات في منظمته. وللتصدي للآثار التقييدية للترتيبات الحالية، يكرر المفتشـــون دعوتهم إلى زيادة التمكين الداخلي لوظيفة رئيس موظفي أمن المعلومات حيثما وجدت، بما يشمل توسيع نطاقها الإداري واستقلالها عن تكنولوجيا المعلومات والاتصالات إلى أقصى حد ممكن، وإنشـــاء هذه الوظيفة في حال عدم وجودها. وفيما يتعلق بتمكين رؤســـاء موظفي أمن المعلومات كمجموعة، لاحظ المفتشون محدودية تقبُّل رفع مستوى الفريق المختص بشكل عام داخل الآلية المشتركة بين الوكالات عن طريق فصـــله عن الشـــبكة الرقمية والتكنولوجية ومنحه وضـــعاً يمكنه من رفع تقاريره مباشرة إلى اللجنة الإدارية الرفيعة المستوى. فمن ناحية، تضمنت الحجج ضد هذا التحول كثرة الشبكات وفرق العمل ومنتديات التنسـيق عموماً ضـمن آلية مجلس الرؤسـاء التنفيذيين، وهو تحول يُعتبر، في حد ذاته، أنه لا يُحتمل أن يسـهم في النهوض بالمسـألة أو إعطائها الأولوية بشـكل فعال. ومن ناحية أخرى، يبدو أن الرأي الســـائد هو أن الفريق لديه بالفعل قناة كافية وقوية لإدراج اعتبارات الأمن الســـيبراني في طليعة المناقشات الاستراتيجية على مستوى المنظومة ككل من خلال الشبكة الرقمية والتكنولوجية واللجنة الإدارية الرفيعة المستوى. **ويؤكد المفتشون مجدداً أن الفريق المختص بأمن المعلومات قد حسّن بشكل فعال تبادل المعلومات بشـأن الأمن السـيبراني في منظومة الأمم المتحدة، وينبغي أن يسـتمر في أداء دوره دون تغيير التكوين الهيكلي الحالي. على أن المفتشـين يشـيرون إلى الحاجة إلى اسـتنباط آلية تضـمن للفريق أن يتمكن – ككيان منفصـل – من تقديم التوجيه الاسـتراتيجي لصـالح مجلس الرؤسـاء التنفيذيين ومنظومة الأمم المتحدة.**

جيم- مركز الأمم المتحدة الدولي للحوسبة كمقدم لخدمات الأمن السيبراني

139- **إعادة النظر فيما لم يتحقق من إمكانات مركز الأمم المتحدة الدولي للحوســـبة.** في ســـياق تقريرها عن الحوسبة السحابية في عام 2019، كانت وحدة التفتيش المشتركة قد دعت فعلاً إلى مزيد من فحص الظروف لتحسين الاستفادة مما لم يتحقق من إمكانات مركز الأمم المتحدة الدولي للحوسبة وحافظة خدماته المتنوعة المقدمة لمنظومة الأمم المتحدة في مجال تكنولوجيا المعلومات والاتصـــالات. في ذلك الوقت، سُلّط الضوء على الأمن السيبراني كأحد المجالات التي تعتبر فيها هذه الإمكانات مهيأة للمزيد من الدراسة. ومع ذلك، ومع مراعاة المنظور الأوسع لإصلاح عمليات تسيير الأعمال في الأمم المتحدة، يرى المفتشون أن هناك مجالاً لإجراء استعراض منفصل وأكثر شمولاً لمركز الأمم المتحدة الدولي للحوسبة، ولعمله العام ونموذج عمله وهيكل حوكمته وولايته، ربما حتى خارج حدود دوره الثابت كمقدم لخدمات تكنولوجيا المعلومات والاتصالات لعملائه، والذين يشملون حالياً، على سبيل المثال لا الحصر، مؤسسات منظومة الأمم المتحدة. ومنذ إنشائه في عام 1971، والذي سبقه تقرير مراجعة خارجية تفصيلي صدر بتكليف من الأمين العام بصفته رئيس آلية التنسيق المشتركة بين الوكالات ذات الصلة، بولاية تشمل دراسة مرافق التجهيز الإلكتروني للبيانات واحتياجات الأمم المتحدة والوكالات المتخصصة والوكالة الدولية

(48) أنظر على سبيل المثال CEB/2017/HLCM/ICT/9، صفحة 8.

للطاقة الذرية، ووُجِّه إلى الجمعية العامة[49]، لم يتم إجراء مثل هذا الاستعراض لتتبع تطور مركز الأمم المتحدة الدولي للحوسبة وإجراء فحص دقيق لقدراته وإمكاناته المتأصلة للاستجابة للاحتياجات المعاصرة لدى المنظومة. ويشير المفتشون إلى الدعوات السابقة التي وجهتها وحدة التفتيش المشتركة للكشف عن العوائق المحتملة في هذا الصدد، وهُم، دون المساس بتنفيذ التوصيات الرسمية الواردة في هذا التقرير، **يتوخون إمكانية إجراء تحليل شامل لمركز الأمم المتحدة الدولي للحوسبة في المستقبل، ولا سيما بهدف تحديد الظروف الهيكلية والمالية والإدارية التي من شأنها أن تمكنه من تحقيق كامل إمكاناته كشريك استراتيجي ومورد مرجعي لمنظومة الأمم المتحدة ككل.** ولأغراض هذا الاستعراض، تمثل أحد الأسئلة التي استرشد بها المفتشون في دراسة ما يعرضه مركز الأمم المتحدة الدولي للحوسبة من خدمات في مجال الأمن السيبراني على وجه الخصوص، فضلاً عن ترتيباته وما لديه من رؤية بشأن موقعه في هذا المجال المحدد، في ما إذا كانت الظروف موجودة بالفعل، وإلى أي مدى، ليصبح المركز مجمعاً للأمن السيبراني لمنظومة الأمم المتحدة.

التفويض ونموذج العمل

140- **تطوُّر مركز الأمم المتحدة الدولي للحوسبة من عام 1971 إلى عام 2021.** عملاً بقرار الجمعية العامة 2741 (د-25)، أُنشئ مركز الأمم المتحدة الدولي للحوسبة بموجب مذكرة اتفاق أبرمت في عام 1971 بين الأمم المتحدة وبرنامج الأمم المتحدة الإنمائي ومنظمة الصحة العالمية. وكمرفق مشترك بين المنظمات أنشئ في الأصل لتوفير "خدمات معالجة البيانات الإلكترونية" لأعضائه المؤسسين الثلاثة ولمستخدِمين آخرين، شهدت قائمة خدماته وقاعدة عملائه تطوراً كبيراً منذ السبعينيات. واشتهر المركز بخدمات الاستضافة والبنية التحتية المشتركة لتكنولوجيا المعلومات والاتصالات التي يوفرها لدعم أنظمة الإدارة المركزية للموارد للعديد من عملائه، وقد توسع نطاق نشاط المركز ليشمل مجالات على درجة عالية من التنوع مثل الحوسبة السحابية وأتمتة العمليات الروبوتية، وتطوير برمجيات الكتل المتسلسلة، واستشارات تكنولوجيا المعلومات والاتصالات، والأمن السيبراني. وبالمثل، نمت قاعدة عملاء المركز بشكل كبير. فقد صُمم منذ البداية كمرفق سينضم إليه عملاء إضافيون، وتضاعف عدد عملائه من 3 في البداية إلى أكثر من 25 من مؤسسات منظومة الأمم المتحدة بحلول عام 2003 وإلى نحو 70 عميلاً في عام 2021، منها كيانات من أسرة الأمم المتحدة ومنظمات منتسبة فضلاً عن عدة منظمات حكومية دولية غير منتسبة ومنظمات غير حكومية دولية ومنظمات مالية دولية. وعُدِّل الصك التأسيسي للمركز في عام 2003 لتوفير أساس قانوني أوسع وقواعد مشاركة أكثر تفصيلاً لعمله، وأضيفت وثيقة "ولاية" جديدة لتضفي صفة ملموسة على الأحكام الأساسية القليلة الواردة في الوثيقة الأصلية وللتوسع فيها. واعتمدت جميع المنظمات الشريكة هذه الوثيقة بشكل منفصل من خلال لجنة إدارة مركز الأمم المتحدة الدولي للحوسبة وأنشئ هيكل لحوكمة المركز ونموذج لعمله وحُددت الشروط الأساسية للمشاركة. وتتمثل الوظيفتان الرئيسيتان للمركز، على النحو المبين في تلك الوثيقة، في تقديم خدمات تكنولوجيا المعلومات، بما في ذلك الخدمات التشغيلية والتدريب، والسعي إلى ضمان أن يعكس نطاق خدماته احتياجات المنظمات الشريكة له.

141- **المبادئ الأساسية لولاية مركز الأمم المتحدة الدولي للحوسبة ونموذج عمله.** عزز مركز الأمم المتحدة الدولي للحوسبة، من خلال اختصاصاته المحدثة، الغرض الأصلي من إنشائه كمقدم خدمات لمؤسسات منظومة الأمم المتحدة، ورُبط عرضه للخدمات بشكل وثيق بالطلب الملموس الذي يولده عملاؤه. وفي الوقت نفسه، مكنته إعادة صياغة وظائفه الرئيسية من أن يكون طليقاً قدر الإمكان في سعيه لتولي

(49) A/8072.

مجالات عمل جديدة تتجاوز النطاق التقييدي لمعالجة البيانات، مما يوفر له، في جملة أمور، الحرية في تقديم خدمات الأمن السيبراني حتى بدون إشارة صريحة إلى ذلك في ولايته. ويتمثل أحد العناصر التي أعيد التأكيد عليها وعولجت بمزيد من التفصيل في الوثيقة الجديدة في فكرة البنية التحتية المشتركة والخدمات المشتركة، والهدف منها تحقيق وفورات الحجم لعملاء المركز. ويشار إلى ذلك بنموذج الخدمات المشتركة التي يقدمها المركز، والذي يمكّنه من خفض تكاليف خدماته بما يتناسب بشكل مباشر مع الزيادة في عدد العملاء المشتركين في الخدمة المعنية. وفي المقابل، تشمل العناصر التي ظلت دون تغيير خلال الخمسين عاماً من وجود المركز ما يلي: (أ) نموذج استرداد التكاليف، الذي يتطلب فعلياً أن يمول عملاء المركز جميع منتجاته مسبقاً على أساس الاحتياجات المحددة والموافقة الجماعية، دون توليد أي فائض في الإيرادات أو أي مجال في الميزانية لأنشطة البحث والتطوير؛ و(ب) الطابع الطوعي لقائمة خدماته، وبموجبه يمكن للمنظمات أن تختار استخدام تلك الخدمات، أو عدم استخدامها، في مقابل رسوم، أو أن تقرر ما تختاره على أساس كل خدمة على حدة؛ و(ج) اعتماده المركز على "منظمة مضيفة" (منظمة الصحة العالمية)، يظل المركز مرتبطاً بها إدارياً وقانونياً، ويعتمد على ما توفره من تسهيلات ومن قدرات إدارية وإطار تنظيمي يمكّنه من التعاقد والتوظيف وتخصيص الأموال والعمل من الناحية العملية.

142- **يعكس هيكل الحوكمة المعقد دور مقدم الخدمات المستند إلى العملاء.** ضماناً لجعل حافظته ملائمة للعملاء الذين يخدمهم، يطور مركز الأمم المتحدة الدولي للحوسبة قائمة خدماته بالتعاون الوثيق مع ممثلي المنظمات الشريكة من خلال لجنة إدارة المركز. ولا تمثل هذه الهيئة التي تضم 41 عضواً جميع العملاء الذين يخدمهم المركز، حيث يتم التمييز بين المنظمات الشريكة ومستخدمي خدمات المركز، ويشار إليهما معاً باسم العملاء[(50)]. فالمنظمات الشريكة وحدها هي التي تتمتع بعضوية لجنة إدارة المركز وبحق التصويت فيها والتي لها رأي في نوع خطوط الخدمة التي يؤذن للمركز بتطويرها، أما العملاء الذين ليسوا منظمات شريكة (أي الذين هم "مستخدِمون" لا غير) فيمكنهم الاشتراك فقط في الخدمات القائمة التي تم تطويرها. بالإضافة إلى ذلك، في إطار نموذج اختيار كل خدمة على حدة، ليس كل أعضاء لجنة الإدارة عملاء لخدمة الأمن السيبراني، والعكس بالعكس (المرفق الثامن). وينطوي ذلك على مخاطر نظرية تتمثل في إعاقة تطوير أو تعزيز خدمات قد تحتاج إليها بشكل ملموس بعض مؤسسات منظومة الأمم المتحدة وليس كلها. وفيما يتعلق بخدمات الأمن السيبراني تحديداً، أنشئ فريق استشاري غير رسمي في عام 2020 يضم أكبر ثلاثة مساهمين في تمويل خدمات الأمن السيبراني (هم حالياً برنامج الأمم المتحدة الإنمائي ومفوضية الأمم المتحدة لشؤون اللاجئين ومنظمة الأغذية والزراعة)، بغرض مراقبة الخدمات التي يعرضها المركز من حيث الجودة والأهمية، وتحديد أية فرص إضافية لحلول مشتركة. ولدى الفريق الاستشاري قناة تواصل مباشرة مع رئيس خدمات الأمن السيبراني في المركز، مع أن القول الفصل فيما يتعلق بتطوير الخدمات لا يزال يقع على عاتق لجنة إدارة المركز. وبشكل عام، وُجد أن هيكل الحوكمة في المركز معقد ويعكس الطابع المتعدد الطبقات لنموذج عمله الحالي. على أن الإجابة لم تكن واضحة على السؤال عما إذا كان هذا الهيكل، في شكله الحالي، قادراً على استيعاب دور أكثر بروزاً، بل حتى على استيعاب دور إلزامي، لصالح المنظومة دون الحاجة إلى إدخال بعض التعديلات المهمة، وعلى الوفاء بذلك الدور بشكل مناسب. ويستكشف الفرع دال من هذا الفصل بعض التحديات في هذا الصدد بمزيد من التفصيل.

(50) وفقًا لتعديل عام 2003 لمذكرة الاتفاق التأسيسي، فإن مصطلح "منظمة شريكة" يعني أي مؤسسة في منظومة الأمم المتحدة تستخدم خدمات مركز الحوسبة وتقبلها لجنة الإدارة كمنظمة شريكة، في حين أن مصطلح " المستخدمون "يعني الحكومات والمنظمات الحكومية الدولية بخلاف المنظمات الشريكة، والمنظمات غير الحكومية والكيانات الحكومية الأخرى التي يوافق المدير عليها لأغراض الاستفادة من خدمات المركز.

143- **مزايا وعيوب نموذج أعمال مركز الأمم المتحدة الدولي للحوسبة.** عند تطوير خدمة معينة، يدفع جميع العملاء المشتركين في تلك الخدمة رسوم استخدام، تحددها لجنة الإدارة وتجري استعراضاً لها على أساس سنوي، حيث تعدل عادة بتخفيضها لتعكس وفورات الحجم مع انضمام مزيد من العملاء إليها وتقليل تكلفتها للجميع. وفي هذا الصدد، فإن النموذج الصارم لاسترداد التكاليف الذي يعمل المركز بموجبه منذ إنشائه له ميزة تتمثل في ضمان درجة عالية من الشفافية في تقدير تكلفة الخدمات، وهو يفرض التنسيق المستمر مع العملاء، ويحافظ على نطاق ما يعرضه من خدمات من خلال اشتراط أقرب مواءمة ممكنة بين ما هو مطلوب حقاً وما يتم تطويره وإنتاجه استجابة لذلك. وبالتالي، يمكن استبعاد أي مصلحة تجارية مدفوعة بالربح كلياً، وهذا أحد الجوانب التي تميز مركز الحوسبة عن الباعة الآخرين. وفي الوقت نفسه، لا توجد ميزانية مكرسة لمواصلة الوظائف التنفيذية والإدارية الأساسية[51]، مما يعني أن هذه التكاليف يجب أن تُدرج في الرسوم المفروضة على الخدمات المقدمة. وقد أثبت نموذج أعمال المركز، الذي يجمع بين مبدأ استرداد التكلفة ومبدأ الخدمات المشتركة، أنه عامل تمكين لتحقيق رؤية المركز في أن يصبح مجمعاً للأمن السيبراني للمنظومة، غير أنه يشكل في الوقت نفسه عقبة أمام تحقيق تلك الرؤية. فقد أوجد هذا النموذج وضعاً يعتمد فيه عرض خدمات المركز على العملاء الذين يقدمون تمويلاً أولياً لتغطية تكاليف تطوير خدمة جديدة لتلبية الطلب، في حين أن جهات أخرى كثيرة لا تستطيع سوى شراء الخدمة التي يتم تطويرها على هذا النحو عقب تحقق كتلة حرجة من العملاء المشتركين بالفعل. ويمكن لهذا الجانب أن يُضرّ بشكل منهجي بالوكالات الأقل قوة من الناحية المالية، والتي قد تختلف احتياجاتها في مجال الأمن السيبراني عن احتياجات أقرانها ممن لديه مساحة أكبر في الميزانية لتقديم تمويل مسبق لخدمات محددة.

قائمة خدمات الأمن السيبراني

144- **مركز الأمم المتحدة الدولي للحوسبة كجهة فاعلة رئيسية في مشهد الأمن السيبراني للأمم المتحدة.** خلال السنوات القليلة الماضية، أثبت المركز نفسه كصاحب مصلحة ومورد مرجعي رئيسي للأمن السيبراني في منظومة الأمم المتحدة. وكما يشهد كثير من عملائه، اكتسب المركز خبرة وقدرة كبيرة في مجال الأمن السيبراني ووسّع نطاق ما يعرضه من خدمات تدريجياً ليشمل 13 خدمة متخصصة في هذا المجال، تُعرف باسم العلامة المتميزة "الأمان المشترك" ("Common Secure") (الشكل التاسع والمرفق السابع). وتغطي الخدمات كلاً من البعد الخاص بحوكمة الأمن السيبراني والجوانب التشغيلية ويقدمها مركز الحوسبة بصفته مقدماً لخدمة استضافة البنى التحتية يدير أيضاً الجوانب الأمنية للبيانات والأنظمة والتطبيقات المستضافة؛ أو كمقدم لخدمات الأمن السيبراني المكرسة؛ أو كمستشار في المسائل الإستراتيجية والإدارية؛ أو كمستجيب عملي للحوادث، وذلك رهناً بنوع الخدمات التي تشترك فيها المنظمة المعنية. ويعكس تنوع خدمات المركز في مجال الأمن السيبراني ما شهده الطلب على هذه الخدمات من نمو كبير بين عملائه. ومع أن المنتجات المتعلقة بالأمن السيبراني لا تمثل إلا جزءاً بسيطاً من قائمة خدمات المركز و6,1 في المائة فقط من حجم التمويل الإجمالي (في كانون الثاني/يناير 2021)، فإن قاعدة العملاء (الحاليين والسابقين) لهذه المنتجات تضم 45 منظمة، 21 منها منظمات أعضاء في مجلس الرؤساء التنفيذيين (من أصل 31 منظمة)، و20 منها منظمات مشارِكة في وحدة التفتيش المشتركة (من أصل 28 منظمة). وعلى الرغم من أن نحو ثلث المنظمات المعنية غير مشمولة بخدمات الأمن السيبراني التي يقدمها المركز، وأبرزها الأمانة العامة للأمم المتحدة، فإنه يصعب أن نفكر في الأمن السيبراني في منظومة الأمم المتحدة اليوم دون النظر في دور المركز ومساهمته.

(51) تقرير مدير مركز الأمم المتحدة الدولي للحوسبة والبيانات المالية لفترة السنتين 2016-2017، نُشر في نيسان/أبريل 2018، صفحة 46.

الشكل التاسع

نظرة عامة على خدمات الأمن السيبراني التي يقدمها مركز الأمم المتحدة الدولي للحوسبة (2021)

الخدمات	*عدد المنظمات المشـــارِكة في وحدة التفتيش المشـتركة (العملاء السابقون والحاليون)*
الأمان المشترك – المعلومات الاستخباراتية للتهديدات	17
خدمة التوقيع الإلكتروني المشتركة	14
الاستجابة للحوادث	11
خدمات الحوكمة ودعم رئيس موظفي أمن المعلومات	11
التوعية بأمن المعلومات	10
إدارة أوجه الضعف	7
اختبار الاختراق	7
خدمات محاكاة التصيد الاحتيالي	6
خدمة العمليات الأمنية المشتركة	5
تقييم الأمن السحابي	5
البنية التحتية العامة الرئيسية المشتركة	3
إدارة الهوية والوصول	3
الأمان المشترك – إدارة المعلومات والأحداث	1

145- **خدمة الأمان المشترك – المعلومات الاستخباراتية للتهديدات باعتبارها الخدمة الرئيسية التي يقدمها مركز الأمم المتحدة الدولي للحوسبة في مجال الأمن السيبراني.** من بين 13 خدمة يقدمها المركز في مجال الأمن السـيبراني، اجتذب بعضـها بالفعل عدداً كبيراً من العملاء داخل منظومة الأمم المتحدة وخارجها، في حين أن هناك خدمات أخرى لا يزال يتعين عليها أن تؤمن قاعدة عملاء لها. وتتمثل إحدى الخدمات المرغوبة بشكل خاص، والتي تضم 17 مشتركاً من بين المنظمات المشارِكة، في خدمة الأمان المشترك – المعلومات الاستخباراتية للتهديدات، والتي يمكن اعتبارها خدمة الأمن السيبراني الرئيسية التي يقدمها المركز والمشهود لها بالفائدة. وتحظى هذه الخدمة بتقييم إيجابي متميز لدى أغلبية واضحة من عملاء المركز وتلبي حاجة جماعية طويلة الأجل طالما وردت وتكررت على مسـتوى المنظومة. وتجمع الخدمة مختلف المصـادر الاسـتخباراتية الداخلية والخارجية، بما في ذلك التجارية والحكومية، للمعلومات المتعلقة بالتهديدات، والتي يقوم المركز بتحليلها وفرزها بغية إنتاج حزم معلومات قابلة للفهم ومصممة خصيصاً لتناسب بيئة الأمم المتحدة وجمهورها. وقد وافقت لجنة إدارة المركز في جلسة خاصة حول الأمن السيبراني، عقدتها في تشرين الأول/أكتوبر 2020، على قرار يطلب إلى جميع المنظمات الشريكة والعملاء تقاسم المعلومات الاستخبارية للتهديدات والحوادث الأمنية، إما مقترنة بإسنادها أو مع إبقائها مجهولة المصدر، مع فريق الأمان المشترك بهدف تحليلها وإطلاع أسرة الأمم المتحدة الأوسع عليها. ويرحب المفتشون بهذا القرار غير أنهم يلاحظون أنه، وفقاً للمعلومات الواردة، لا يزال يُنتظر تنفيذه من جانب جميع الجهات. وقد اعتبرت معظم المنظمات المشارِكة التي شملها استقصاء وحدة التفتيش المشتركة أن هذا المجال هو الأكثر قبولاً لتوثيق التعاون فيه على مستوى المنظومة بأكملها، وقد لاحظ بعضها أنه، بالإضافة إلى تبادل المعلومات الاستخبارية عن التهديدات، وعلى وجه الخصوص، مؤشرات الاختراق، من المفيد أيضاً تبادل المعلومات بشأن الاستجابة الملموسة وتدابير التعافي المتخذة. غير أن الجانب الأخير لم يحظ بتأييد

موحد بين الخبراء الذين أجرى المفتشون مقابلات معهم، مما يرجع أساساً إلى مخاوف تتعلق بالسرية. ومع ذلك، يمكن اعتبار خدمة الأمان المشترك – المعلومات الاستخباراتية للتهديدات الخدمة الأكثر تبشيراً بمستقبل واعد في مجال الأمن السيبراني من حيث القدرة على تحقق الانضمام إليها بشكل كامل، وبصورة طبيعية، على مستوى المنظومة وتحقيق مكاسب حماية فعلية للمنظومة تتجاوز ما تحققه اليوم بالفعل. ولا يمكن أن تُعزى نفس الإمكانيات بسهولة إلى مجموع حافظة خدمات الأمن السيبراني التي يقدمها مركز الحوسبة.

146- **يتسم تقييم خدمات الأمن السيبراني التي يقدمها مركز الأمم المتحدة الدولي للحوسبة بالتفاوت.** على الرغم مما يمارسه عملاء مركز الحوسبة من سيطرة قوية – من الناحية الهيكلية – على الخدمات المقدمة لهم، فإن ردود فعل المنظمات المشارِكة فيما يتعلق برضاها عن الخدمات المذكورة كانت متفاوتة إلى حد ما، وتتراوح من "راضية جداً" إلى "غير راضية على الإطلاق". ويمكن أن يعزى ذلك إلى عدة عوامل. فمن ناحية، من بين المنظمات المشارِكة العشرين التي تشترك حالياً أو اشتركت في الماضي في خدمة واحدة على الأقل من خدمات الأمن السيبراني التي يقدمها المركز، هناك بعض الاختلاف فيما يتعلق بعدد الخدمات المشترك بها وأيها، ومن ثم في تصنيف كل من المنظمات لها بأنها مرضية أم لا. كما يمكن أن يؤثر التباين في نضج إطار عمل الأمن السيبراني للمنظمة المعنية على درجة تمكّنها من استيعاب جميع جوانب الخدمة المقدمة والاستفادة منها بشكل كامل. ومن ناحية أخرى، فإن بعض الخدمات التي تُدرج حالياً كخدمات منفصلة كانت مجمّعة وتقدَّم كحزمة، الأمر الذي كان يولّد بعض الانتقادات بسبب اضطرار الكيانات إلى الاشتراك في أجزاء من الحزمة ليست بحاجة إليها لكي تتمكن من الاستفادة من الأجزاء الأخرى المطلوبة أو المرغوبة. على أنه ذُكر أن المركز أوقف هذه الممارسة في عام 2019 وهو الآن يتيح لعملائه مرونة كاملة في اختيار مستوى الخدمة ونوعها وفق ما يناسبهم. بالإضافة إلى ذلك، يمكن لدرجة الرضا الأساسية أن تعطي انطباعاً أكثر عمومية حول التفاعل أو حول جانب آخر من تجربة التعامل مع المركز، مما يجعلها أقل موثوقية ولا يكفي مستوى دقتها لجعلها قاطعة. وبالنظر إلى هذه القيود وإلى أن هدف المفتشين لم يكن تقييم فعالية كل خدمة يقدمها المركز أو قائمة خدماته ككل، فإنه لم يكن من الممكن تمييز نمط واضح فيما يتعلق بنوع المنظمات التي كانت أكثر انتقاداً أو دعماً للمركز من غيرها، أو بحجمها أو نضجها. وبشكل عام، يمكن القول إن عدداً من المنظمات، الكبيرة والصغيرة، أعربت عن تقديرها الكبير للمركز كمقدم لخدمات الأمن السيبراني، في حين أن عدداً مساوياً من المنظمات اتخذت موقفاً شديد الانتقاد تجاه المركز. ويمكن أن يعكس هذا الانتقاد، في بعض الحالات، أوجه قصور تاريخية قد تجاوزتها التطورات اللاحقة، وبالتالي ينبغي ألا يحجب الإمكانات الحالية والمستقبلية للمركز كمقدم لخدمات الأمن السيبراني. ومع ذلك، يمكن جداً أن تكون التحفظات المعرب عنها معاصرة، أو صالحة باستمرار، أو حتى متكررة مع مرور الوقت، وينبغي بالتالي أن تؤخذ على محمل الجد كلياً. وعلى أي حال، يمكن أن توفر تقييمات رضا العملاء المنتظمة والتفصيلية رؤى قيمة حول المجال الذي يُنصح فيه المركز ببذل المزيد من الجهود للاستجابة لمخاوف عملائه وقد يجتذب عملاء إضافيين في الوقت المناسب. علاوة على ذلك، قد يكون إجراء تقييم شامل لمركز الحوسبة كمقدم لخدمات الأمن السيبراني مفيداً في توفير ضمانات أكثر موضوعية للجودة الشاملة لمجموعة خدمات المركز في هذا المجال ولملاءمتها للغرض.

147- **المزايا المتصورة للتعامل مع مركز الأمم المتحدة الدولي للحوسبة.** تضمنت أسباب التعامل مع مركز الحوسبة، كما عرضها عملاؤه، معرفته الوثيقة بمنظومة الأمم المتحدة واحتياجات مؤسساتها نتيجة لخبرته الطويلة في تطوير خدمات مخصصة لها، وخضوعه لنفس القواعد والهياكل الإدارية، وعمله مع المنتديات ذات الصلة المشتركة بين الوكالات. بالإضافة إلى ذلك، سلط المركز الضوء على عدة مزايا نسبية تميزه عن مقدمي الخدمات التجارية، وهي تشمل فيما تشمله ما يلي: الانخفاض التدريجي في تكلفة خدماته مع نمو قاعدة عملائه؛ وعدم وجود توجه للربح وما يرتبط بذلك من اهتمام بالإبقاء على أسعاره في متناول الجميع، بما في ذلك المنظمات الأقل ثراءً التي تبحث عن خيارات منخفضة التكلفة؛ والهدف

المتأصل والمشترك المتمثل في جعل المنظومة أكثر أماناً للجميع، بما في ذلك لنفسه كأحد أفراد أسرة الأمم المتحدة؛ والقدرة على مراقبة عملائه والتكيف معهم والتعلم منهم بشكل مباشر؛ وتوسيع نطاق الدروس المستفادة مباشرة لصالح المجموعة. كما أن النظرة الشاملة للمنظومة ككل ولجميع أجزائها تميز مركز الحوسبة عن مقدمي الخدمات التجاريين، الذين يميلون إلى رؤية أجزاء فقط من الصورة الأكبر، مما يضمن بالتالي للمركز أن يضيف قيمة خارج السياق الفردي لأي عميل لوحده. وهناك جانب آخر وجده المفتشون مقنعاً وهو الفكرة القائلة بأنه على الرغم من الآليات المشتركة بين الوكالات والطبقة المضافة من الحوكمة القائمة على التمثيل في لجنة إدارة المركز، فإنه لا يوجد أي كيان لديه دافع جوهري لمتابعة المصلحة الجماعية الواضحة للمنظومة بدلاً من المصالح الفردية لأعضائها أو، على الأكثر، المصالح التراكمية – والتي لا يمكن التوفيق بينها في كثير من الأحيان. وقد اعتبر المركز نفسه وسيطاً محايداً غير سياسي – نظراً لنموذج استرداد التكاليف الذي يأخذ به – ولا مصلحة شخصية له، يقدم الحلول على نطاق المنظومة ككل في هذا المضمار، مستنيراً بالصالح العام بدلاً من بعض الاعتبارات الخاصة بندرة الموارد الحادة التي قد توجّه أعضاء لجنة إدارة المركز وتورطهم في تضارب محتمل في المصالح.

148- **أوجه القصور الملحوظة في دور مركز الأمم المتحدة الدولي للحوسبة كمقدم لخدمات الأمن السيبراني.** في المقابل، أعطت عدة منظمات تقييماً أقل إيجابية لمركز الحوسبة كمقدم لخدمات الأمن السيبراني، وانتقدت تحديداً الجانب المتعلق بالقيمة مقابل المال مقارنة بما يمكن لمقدمي الخدمات التجارية تقديمه. ونقل البعض انطباعهم بأن الشركات الخارجية قادرة على توفير أحدث الخبرات والأدوات بمستوى يتجاوز القدرة التي يمكن أن يحققها المركز أو أي منظمة لوحدها حتى بعد استثمارات كبيرة. وقوبل هذا الانطباع بأصوات أخرى بين عملاء المركز أبلغت عن قفزة حقيقية في الخبرة والتأهب السيبراني حققها المركز في السنوات الأخيرة، ودللت على ذلك باستثمارات كبيرة وضعتها قيادته في مجال شهادات المنظمة الدولية لتوحيد المقاييس والامتثال لها، والتوظيف المتنوع للخبراء، وإنشاء مركز مشترك للعمليات الأمنية يعمل بدون توقف، وتوسيع قدرات مركز الحوسبة في مجال الرصد على مدار الساعة، وتعزيز قائمة خدماته. ومع ذلك، لا يمكن لهذه الجهود أن تصرف الانتباه عن استمرار التصور القائل بوجود ثغرة متواصلة في الخبرة والقيمة مقابل المال يصعب – ربما فعلاً – على المركز التغلب عليها. وأشير كذلك إلى أن خدمات مماثلة كانت متاحة بأسعار أكثر تنافسية من القطاع الخاص، واعتبر بعض المجيبين أنه على الرغم من وفورات الحجم الناجمة عن نموذج الخدمات المشتركة، فإن المركز يفرض الكثير من الرسوم على بعض خدماته، وبطريقة غير شفافة، مما يجعلها باهظة الثمن أو غامضة بالنسبة لبعض المنظمات، ولا يقابلها ما يكفي من المكاسب في مجالات أخرى بالنسبة لمنظمات أخرى. وقد اعترف المركز في الواقع بأن التنافس مع القطاع الخاص يتجاوز قدراته بل إنه يأتي بنتائج عكسية في بعض النواحي. بالنظر إلى نموذج أعماله، فإن تكلفة خدماته تنخفض بشكل عام إذا انضم المزيد من العملاء، في حين أن التكلفة، في كثير من الحالات، هي حاجز في وجه دخول منظمات ترغب في الانضمام للحصول على الخدمات في المقام الأول. ويمكن التخفيف من هذه المفارقة، على سبيل المثال، عن طريق ضخ بعض التمويل المربوط بصورة أقل في الأماكن الصحيحة، مما يسمح للمركز بتخفيض بعض رسومه، وربما إلى ما دون ما يتقاضاه مقدمو الخدمات من القطاع الخاص، دون الحاجة إلى محاولة استبدالها بالكامل. ومع ملاحظة أنه ليس من المنطقي التنافس مع القطاع الخاص في المجالات التي يضيف فيها قيمة أكبر وبكفاءة أشد، فإنه ينبغي للرؤساء التنفيذيين أن يستكشفوا ما إذا كان بوسع المركز أن يعمل كحلقة وصل بين مقدمي الخدمات التجاريين وعملائهم في منظومة الأمم المتحدة من أجل خفض الرسوم التعاقدية وتحقيق وفورات الحجم وتحسين القدرة التفاوضية في نهاية المطاف. وعلاوة على ذلك، وبالاقتران مع الاقتراح أعلاه بخصوص التقييم المستقل لخدمات الأمن السيبراني، قد يرغب المركز في إجراء تحليل نقدي لقائمة خدمات الأمن السيبراني التي يقدمها بحيث يمكن بشكل أفضل تمييز

الخدمات التي قد يكون للمركز فيها ميزة نسبية والنظر في استثمار مزيد من جهوده في تلك المجالات. ولاحظ المفتشون أنه، في نهاية المطاف، وعلى الرغم من الانتقاد القاسي أحياناً للمركز كمقدم لخدمات الأمن السيبراني، فإن المنظومة تستفيد فعلاً من خدماته.

149- **فرص التحسين ضمن الحدود الحالية لولاية مركز الأمم المتحدة الدولي للحوسبة.** في حين أن بعض المنظمات دعت إلى التعزيز الرسمي لمكانة مركز الحوسبة كمقدم لخدمات الأمن السيبراني لمنظومة الأمم المتحدة، يعتقد المفتشون أنه يمكن إنجاز الكثير في إطار ولاية المركز الحالية بصيغتها المنقحة في عام 2003، فهي توفر بالفعل أساساً سليماً لتنفيذ حلول يمكن أن تتحقق بقدر من المشاركة أكبر قليلاً من جانب أصحاب المصلحة جميعهم. وحتى إذا أصبحت التغييرات في ولايته ضرورية لأسباب وجيهة، فإنها تدخل في نطاق الاختصاص الجماعي للمنظمات المؤسسة له وللكيانات التي وقعت على تعديل صكه التأسيسي في عام 2003 ولن تتطلب اتخاذ إجراء من جانب الجمعية العامة، ريثما يتم إجراء تحليل أكثر شمولاً للمركز ككيان ولمنجزاته حتى الآن وللأسباب الهيكلية المحتملة لعدم تحقق إمكاناته والتي يمكن معالجته من خلال ذلك الإجراء. ويرى المفتشون أن أحد الجوانب الرئيسية التي يتعين أن تعالج دون تأخير أو مزيد من الشروط المسبقة يتمثل في تحديد أسباب الثغرة السائدة بين الهياكل والآليات القائمة وبعض القيود في نمط التمويل الحالي، ومعالجتها، على النحو المفصل أدناه.

دال- تحسين الروابط بين التوجيه الاستراتيجي والقدرة التشغيلية على نطاق المنظومة ككل

معالجة الانفصال المؤسسي بين الفريق المختص بأمن المعلومات ومركز الأمم المتحدة الدولي للحوسبة

150- **العلاقة بين الفريق المختص بأمن المعلومات ومركز الأمم المتحدة الدولي للحوسبة محدودة رسمياً.** بالنظر إلى التداخل الكبير بين المنظمات الممثلة في آليات التنسيق بين الوكالات من ناحية ولجنة إدارة مركز الحوسبة من ناحية أخرى (المرفق الثامن)، قد يفترض المرء أن الفريق المختص بأمن المعلومات هو الهيئة التي توفر التوجيه الاستراتيجي والإرشاد بشأن حلول الأمن السيبراني المشتركة التي يمكن أن تكون مناسبة لمؤسسات منظومة الأمم المتحدة، بينما يعمل المركز كذراع للمنظومة فيما يتعلق بالتنفيذ التشغيلي. على أنه لا يوجد ارتباط رسمي بين الكيانين، ولا يعملان بشكل مشترك في الممارسة العملية. ومن الناحية الرسمية، لا يمارس الفريق المختص بأمن المعلومات إلا دور التنسيق وتبادل المعلومات وليس مخولاً بتوجيه مركز الحوسبة بأي شكل من الأشكال، في حين أن المركز ينفذ قرارات لجنة إدارته فيما يتعلق بالخدمات التي يطورها لشركائه وعملائه، الذين لا يشملون جميع مؤسسات منظومة الأمم المتحدة. أما من الناحية العملية، فقد لا يكون الانفصال المؤسسي بين الهيئتين هو العامل الحاسم، ولكن من المحتمل أن يكون قد ساهم في خلق دينامية يمكن أن تكلف المنظومة غالياً من حيث مكاسب الكفاءة، وذلك بسبب إضاعة فرص المزيد من التعاون المباشر.

151- **ترجع التفاعلات المتوترة في الممارسة إلى سلسلة من العوامل.** الواقع أن مركز الحوسبة مُنح صفة مراقب في الفريق المختص بأمن المعلومات وهو يشارك في مناقشات الفريق دون أن يكون له الحق في التصويت أو في طرح بنود للمناقشة. على أن المركز ذكر أنه حُرم فعلياً من إمكانية الترويج لقائمة خدماته في منتدى الفريق أو التماس التعليقات المباشرة على حلوله في هذا الإطار. ويمكن تفسير هذا الموقف جزئياً بطبيعة المركز باعتباره مرفقاً مشتركاً بين المنظمات وليس كياناً يمكن أن يمنحه وضعُه عضويةَ مجلس الرؤساء التنفيذيين وبالتالي حقوق المشاركة الكاملة. وأشير أيضاً إلى أن هناك تصوراً أساسياً مفاده أن المركز هو في الأساس بائع لمؤسسات المنظومة وليس شريكاً لها، مما يزيد من إعاقة اندماجه الكامل في الآليات القائمة المشتركة بين الوكالات. ونظراً لتركيبة المركز الخاضعة للعملاء ولدوره كمورد لخدمات الحوسبة المصممة وفقاً لاحتياجات المنظمات الشريكة، فإن من الصعب إنكار أن فكرة

كونه بائعاً لها ما يبررها. وفي الوقت نفسه، يصور المركز نفسه علانية على أنه واحد من كيانات الأمم المتحدة وعضو كامل العضوية في أسرتها. وفي الواقع، تتحدث قيادة المركز بصوت عال حول استعدادها لتشكيل مركز الحوسبة كمجمّع للأمن السيبراني لمنظومة الأمم المتحدة إذا أُتيحت لها الفرصة للقيام بذلك، حتى أن بعض المنظمات ترى أن المركز ينبغي أن يجعل الأمن السيبراني عمله الأساسي. ومع ذلك، وبانتظار معالجة التحديات وإيجاد حلٍ لها، فيما يتعلق بالديناميات بين الآليات المشتركة بين الوكالات المكلفة بولايات في المنظومة ومركز الحوسبة كمقدم متميز لخدمات الأمن السيبراني لديه إمكانية تولي دور الذراع التشغيلية للمنظومة في هذا المجال، فإن من المرجح أن يظل هذا السيناريو بعيداً عن المتناول.

152- **هيكلان متوازيان بحكم الأمر الواقع.** من الأمثلة التي توضح كيف أن الدينامية بين الآلية المشتركة بين الوكالات ومركز الحوسبة قد دفعت إلى إيجاد حلول عفوية للاحتياجات المحددة، ولكنها خلقت في نفس الوقت ازدواجية في مجال الأمن السيبراني، حالةُ مؤتمر الأمان المشترك الذي يستضيفه المركز. ومنذ عام 2019، يتيح المؤتمر وسيلة لعملاء خدمة الأمن السيبراني في المركز لتبادل المعلومات حول مسائل الاهتمام المشترك على المستوى التشغيلي وتقديم التعقيبات على الخدمات المقدمة. وقد أصبح المؤتمر حدثاً متكرراً على تقويم أنشطة الأمن السيبراني يحظى باحترام كبير، وولّد كثير من الثناء بين المشاركين فيه، وكثير منهم من مؤسسات منظومة الأمم المتحدة الممثلة أيضاً في الفريق المختص بأمن المعلومات. وبمعنى ما، يمكن القول إن مؤتمر الأمان المشترك سد ثغرة في مركز الحوسبة الذي سعى إلى التعامل مع المنظمات من خلال الفريق المختص بشكل مباشر ولكنه لم يكن قادراً على القيام بذلك بطريقة مثمرة وملموسة كما كان يتمنى فيما يتعلق بهدفه المتمثل في تحسين شراكته مع المنظومة وبالجوانب التشغيلية لعرض خدماته. حتى أن البعض يمكن أن يقولوا إن المؤتمر أصبح بحكم الأمر الواقع المنتدى الرائد لقطاع كبير من المنظومة كنتيجة مباشرة لعدم قدرة آلية التنسيق الحالية للفريق المختص بأمن المعلومات على التوصل إلى تفعيل مناقشةٍ أكثر توجهاً نحو الحلول. ويتمثل الجانب السلبي لهذه التطورات الاستباقية والمبتكرة في أن المؤتمر ربما يكون قد حوّل بعض المناقشات التي كان من الممكن إجراؤها ضمن الفريق المختص إلى منتدى آخر، وهو منتدى مفتوح، من الناحية النظرية، لعملاء مركز الحوسبة بشكل أساسي وليس للمنظومة ككل. إن وجود هذين الهيكلين – المتوازيين وغير المتكاملين في الواقع – لخدمة أغراض متشابهة جداً، أحدهما تحت رعاية مجلس الرؤساء التنفيذيين والآخر تحت إشراف مركز الحوسبة، ينطوي على مخاطر إيجاد مزيد من الانفصال والتنافس، مما يؤدي إلى عدم الفعالية والازدواجية والتداخل. وهذا هو أحد الآثار الجانبية الضارة الناتجة عن الإدارة غير المُرضية للدينامية بين الكيانين.

153- **هناك حاجة إلى مزيد من التآزر.** ينبغي أن تسترشد بهذه الملاحظات إجراءات كلا الكيانين في محاولة تحسين سبل التعامل بينهما. فمن ناحية، يحتاج الفريق المختص إلى تكثيف جهوده كمجموعة للوفاء بولايته بمعنى أكثر استراتيجية، لتحديد المجالات التي تصلح فيها الحلول المشتركة، إن لم يكن للمنظومة ككل، فعلى الأقل لمجموعات من المنظمات التي يؤدي تحسين وضع الأمن السيبراني فيها إلى الارتقاء بمستوى المنظومة ككل. أما إذا فشل في القيام بذلك، مستفيداً من الصوت الرسمي الذي يحمله نيابة عن المنظومة، فإن من المحتمل أن يضطر مركز الحوسبة إلى التدخل وشغل تلك المساحة بطريقة تظل مقتصرة على دائرة العملاء الذين يقدم لهم خدماته. وفي الوقت نفسه، فإن استغلال مركز الحوسبة فرصة الفراغ الذي أحدثه الفريق المختص بأمن المعلومات عن غير قصد هو، من حيث المبدأ، مفيدٌ للمنظومة نظراً لإمكانيات المركز المبتكرة، ولكن هذا ينبغي ألا يحدث بمعزل عن هيئة رسمية مسؤولة عن التنسيق والتعاون في مجال الأمن السيبراني على مستوى المنظومة. ويتحمل كلا الكيانين مسؤولية البحث بشكل استباقي عن طرق لتحسين الدينامية بينهما، سواء من خلال تدابير رسمية أو غير رسمية. وفي الواقع، يُعتبر عدد من خدمات الأمن السيبراني التي يقدمها المركز لعدد كبير من العملاء مستوحاة من تبادلات أجريت في سياق الفريق المختص أو انبثقت عنه مباشرةً، حتى بدون أي تكليف من هذا الأخير

بأي معنى رسمي. وإذا ظل مركز الحوسبة ملتزماً بمواصلة مسيرته ليصبح مجمّعاً للأمن السيبراني للمنظومة وليس لعملائه وحدهم، فإنه لا يمكنه تحمل البقاء منفصلاً عن مجتمع الخبراء الذي يمثل الاحتياجات الجماعية للمنظمات التي سيخدمها ذلك المجمّع. علاوة على ذلك، فإن الفريق المختص يُمسك كمجموعة بجزء من مفتاح تيسير المزيد من التعاون البناء في هذا الصدد. إن إمكانية التآزر وزيادة التكامل قائمة ولكنها لم تتحقق بالكامل حتى الآن.

154- **على المنظمات المشارِكة إعادة النظر في استخدام خدمات الأمن السيبراني التي يقدمها مركز الأمم المتحدة الدولي للحوسبة** . كطريقة لمعالجة الانفصال السائد بين الكيانين، اقترح البعض جعل استخدام خدمات الأمن السيبراني التي يقدمها مركز الحوسبة إلزامياً لمؤسسات منظومة الأمم المتحدة. وذُكر أن من شأن ذلك أن يسرّع أيضاً ما يُحتمل من مكاسب الكفاءة وخفض التكاليف من خلال تعزيز نطاق عمل المركز وزيادة قدرته كمقدم للخدمات المشتركة. ولا يشترك الجميع في هذه الرؤية وقد تؤدي في الواقع إلى نتائج عكسية. فمن ناحية، ستزيل قدرة مؤسسات منظومة الأمم المتحدة على تقييم عروض الخدمات التي تناسب احتياجاتها وعلى البتّ بشأنها، وذلك من خلال فرض وتنفيذ احتكار مصطنع يُمنح لمقدمي الخدمات وعارضيها الخارجيين. من ناحية أخرى، هناك آليات للحوكمة عاملة داخل مركز الحوسبة تسمح بالفعل بإجراء تبادل صحي بين إدارته التنفيذية وعملائه حول تشكيل خدمات الأمن السيبراني. ويرى المفتشون أنه ليس من الحكمة ولا من الضرورة التدخل في هذه الآليات. **على أن المفتشين، في عام 2019، شجعوا مؤسسات منظومة الأمم المتحدة ومركز الحوسبة على إيجاد أساس مشترك أعمّ لاستكمال القدرات الحالية للمنظمات بمزيد من الخدمات المشتركة**[52]. وعلى وجه الخصوص، يعتقد المفتشون أن بعض الأسباب التي ربما دفعت فرادى المنظمات في الماضي إلى إلغاء الاشتراك أو الامتناع عن الاشتراك في خدمات الأمن السيبراني التي يقدمها المركز قد تستحق إعادة النظر فيها. ويتعين أن يهتم قرار القيام بذلك بالتفاصيل الدقيقة، وأن ينطوي، من الناحية المثالية، على (إعادة) تقييم كل خدمة من خدمات الأمن السيبراني المقدمة استناداً إلى مزاياها الخاصة. ويمكن ألا تكون بعض الخدمات قد وصلت بالفعل إلى مستوى النضج أو أنها لا تستجيب بشكل كافٍ لاحتياجات المنظمات مما لا يمكّن جميع أعضاء المنظومة من اتخاذ قرار الاشتراك فيها. ويعود الأمر لمركز الحوسبة لمواصلة جهوده لمعالجة أي ثغرات في هذا الصدد. كما يدرك المفتشون الطابع الفردي لكل منظمة. فمسؤولية اتخاذ القرارات ذات الصلة تقع في نهاية المطاف على عاتق المنظمات استناداً إلى احتياجاتها الخاصة، ولا سيما مع مراعاة تنوع أنظمة المعلومات والتطبيقات والترتيبات التقنية الأخرى المنشأة داخلياً أو المؤطرة في ترتيبات تعاقدية مع مقدمي الخدمات الخارجيين.

استكمال تمويل الحلول المشتركة للمنظومة بتبرعات من الجهات المانحة

155- **التبرعات كوسيلة للدعم المباشر**. يرى المفتشون أن الوقت قد حان للنظر في استخدام التبرعات كآلية تمويل تكميلية لتوفير المزيد من الموارد المباشرة لحماية الوضع العام للأمن السيبراني في المنظومة. ويمكن لتوافر التبرعات المخصصة لتدابير تُتخذ على نطاق المنظومة ككل أن يزيل بعض العقبات التي تعترض سبيل تنفيذ حلول الأمن السيبراني المشتركة، حيث يحتمل أن يكون نقص الموارد داخل المنظمات المشارِكة قد أثر على استعدادها للمساهمة في مجموعة مشتركة للتمويل. ويمكن لإعطاء المنظومة إمكانية الاستفادة من مصدر تبرعات الجهات المانحة المستقل عن ميزانيات فرادى أعضائها أن يخفف بعض الضغط المفروض، من ناحية، من خلال المساحة المحدودة للغاية المضمنة في تلك الميزانيات مع وجود كثرة من الأولويات المؤسسية المتنافسة على الأموال الشحيحة بشكل متزايد، ومن ناحية أخرى، من خلال

(52) JIU/REP/2019/5.

نموذج استرداد التكاليف الذي يأخذ به المركز الدولي للحوسبة. وفيما يتعلق بهذا الأخير، سيسمح بتطوير خطوط خدمات مبتكرة للمنظمات الشريكة للمركز، لا سيما تلك التي تعتمد على قدرة داخلية أقل تطوراً أو لديها موارد أدنى لترتيبات الأمن السيبراني بشكل عام. وبالاقتران مع نموذج الخدمات المشتركة، سيستمر هذا النهج في المساهمة في كفاءة التكلفة عن طريق الحفاظ على انخفاض رسوم الخدمة، ومن المرجح أن يجتذب عملاء إضافيين، وبالتالي أن يضاعف من الآثار الإيجابية. وتمثل أحد الأسئلة التي فكر فيها المفتشون بالتشاور مع المحاورين ذوي الصلة فيما إذا كان من الأفضل وضع آلية لجمع وإنفاق هذه التبرعات تحت السلطة المباشرة للمنظومة كمجموعة، على سبيل المثال كصندوق استئماني يُنشأ تحت إدارة أمانة مجلس الرؤساء التنفيذيين ويستفيد من المدخلات الفنية التي يقدمها الفريق المختص بأمن المعلومات، أو لدى المركز الدولي للحوسبة باعتباره المقدم الفعلي لكثير من الحلول المشتركة للمنظومة. وبعد النظر في الخيارات المختلفة في هذا الصدد، قرر المفتشون أن المكان الأفضل لمثل هذا الصندوق الاستئماني سيكون لدى كيان يتطلب وضوحاً للنفقات على أساس تشغيلي وبصورة يومية في تطوير الخدمات المرغوبة، وبالتحديد مركز الأمم المتحدة الدولي للحوسبة.

156- **الصندوق الاستئماني للأمن السيبراني.** من حيث المبدأ، تتضمن ولاية مركز الحوسبة، منذ تعديله في عام 2003، أحكاماً تمكنه من جمع التبرعات، وقد شهد الماضي القريب سابقة لمشروع معين تم تمويله من خلال هذه القناة. على أن هذه الآلية لم تُستخدم بشكل كافٍ حتى الآن. وتكمن في استخدامها الاستراتيجي لأغراض التصميم الاستباقي للخدمات التي سيتم تقاسمها، سواء بين جميع مؤسسات منظومة الأمم المتحدة أو بين عدد منها، قدرةٌ على تغيير قواعد اللعب. ومن شأن الإعلان عن وجود هذا الاحتمال على نطاق أوسع وتحسين الظروف التي يمكن أن يتحقق في ظلها، أن يوفر الفرصة للدول الأعضاء الراغبة في المساهمة بشكل مباشر في تعزيز الأمن السيبراني في المنظومة ككل، بموجب شروط تطبق على المساهمة المخصصة لدعم حلول الأمن السيبراني المشتركة. كما أنه سيسهل تنفيذ توصية وحدة التفتيش المشتركة لعام 2019 بشأن آلية للتمويل تسمح لمركز الحوسبة بإجراء أنشطة البحث والتطوير خارج قيود نموذجه الخاص باسترداد التكاليف، مما يمكن أن يحقق فائدة أكبر لعملائه من مؤسسات منظومة الأمم المتحدة. ولذلك يوصي المفتشون بأن يقوم مدير مركز الحوسبة، بعد إجراء المشاورات المناسبة، بإنشاء صندوق استئماني للأمن السيبراني لغرض محدد هو تصميم وتطوير خدماتٍ مشتركة للأمن السيبراني تشتد حاجة المنظومة إليها. ولتمييز هذه الآلية عن مصادر التمويل الأخرى التي تقدمها للمركز المنظمات الشريكة والعملاء، فإن من الحكمة إنشاء صندوق استئماني مكرس، مع إرفاق شروط خاصة تضمن ألا تكرر الحوكمة الخاصة به التحيزات الهيكلية القائمة، أو تضارب المصلحة المحتمل، أو الديناميات غير المفيدة المنبثقة عن تداخل العضوية وتمايزها في لجنة إدارة المركز وفي الهيئات المشتركة بين الوكالات ذات الصلة على نطاق المنظومة ككل.

157- **تفعيل الصندوق الاستئماني.** بناءً على ذلك، تكتسي اختصاصات آلية التمويل هذه أهمية أساسية لنجاحها. فهذه الاختصاصات ينبغي أن توضح الأدوار والمسؤوليات لمختلف أصحاب المصلحة، وأنواع الخدمات التي من المفترض أن تمولها، وإجراءات تخصيص الأموال بطريقة شفافة، بما في ذلك ما يتصل بذلك من متطلبات للإبلاغ. وعلى وجه الخصوص، ينبغي تنظيم الصندوق الاستئماني بحيث يُستخدم في المقام الأول لأغراض ذات نواتج ملموسة بالنسبة لمؤسسات المنظومة. ويمكن أن يكون الهدف الرئيسي للصندوق هو تمويل البحث والتطوير بغية إطلاق خدمات للأمن السيبراني تحظى باهتمام واضح بين المنظمات ولكن لا تتوفر لها كتلة حرجة أولية من المستخدِمين المستعدين لتقاسم التمويل الأساسي المطلوب. وبالمثل، يمكن استخدام الصندوق لتوسيع نطاق أو عمق الخدمات الحالية التي يوجد طلب واضح عليها والتي تتطلب تمويلاً أولياً، أو قد يلزم خفض تكلفتها لتمكين المزيد من المنظمات من الانضمام في وقت أقرب. وفي حين أن الصندوق الاستئماني يخضع بشكل عام للقواعد واللوائح المالية لمنظمة الصحة العالمية،

التي يعمل بموجبها مركز الحوسبة، فإن هناك فرصةُ إدراج عنصر في حوكمته يُعنى بالتشاور مع الهيئات المختصة المشتركة بين الوكالات. ومن شأن ذلك أن يساعد في تشكيل حلول مشتركة يجري تطويرها لصالح المنظومة ككل وليس لصالح عملاء المركز وحدهم، ومن ثم في زيادة تحسين استخدام الموارد المتاحة. وبالنظر إلى دور الجمعية العامة في توفير الأساس لإنشاء مركز الحوسبة، فإنها مدعوة إلى الإحاطة علماً بتوصية إنشاء الصندوق الاستئماني للأمن السيبراني وإلى دعوة الدول الأعضاء إلى المساهمة فيه.

158- ومن المتوقع أن يؤدي تنفيذ التوصيتين التاليتين إلى تعزيز التنسيق والتعاون بين مؤسسات منظومة الأمم المتحدة.

التوصية 3

ينبغي لمدير مركز الأمم المتحدة الدولي للحوسبة أن يعمل على إنشاء صندوقٍ استئماني لتبرعات المانحين، في موعد أقصاه نهاية عام 2022، من شأنه أن يكمِّل قدرة المركز على تصميم وتطوير وتقديم خدمات وحلول مشتركة لتعزيز وضع الأمن السيبراني في مؤسسات منظومة الأمم المتحدة.

التوصية 4

ينبغي للجمعية العامة للأمم المتحدة أن تحيط علماً، في موعد لا يتجاوز دورتها السابعة والسبعين، بالتوصية الموجهة إلى مدير مركز الأمم المتحدة الدولي للحوسبة بإنشاء صندوق استئماني لحلول الأمن السيبراني المشتركة، وأن تدعو الدول الأعضاء الراغبة في تعزيز وضع الأمن السيبراني لمؤسسات منظومة الأمم المتحدة إلى المساهمة في ذلك الصندوق الاستئماني.

هاء- فرص تحقيق مواءمة أوثق بين الأمن المادي والأمن السيبراني

159- **لا يغطي نظام إدارة الأمن في الأمم المتحدة الأمن السيبراني.** أنشأت الجمعية العامة، في قرارها 276/59، إدارة شؤون السلامة والأمن بولاية على نطاق المنظومة ككل لإنشاء إطار للسياسة العامة والمساءلة وكذلك معايير وإجراءات تشغيلية لسلامة وأمن موظفي الأمم المتحدة وأصولها. ولعله ليس من المستغرب أن الولاية المسندة إلى إدارة شؤون السلامة والأمن في عام 2004، والتي سبقت التطورات الرئيسية التي طرأت على مستوى المنظومة في مجال الأمن السيبراني في عامي 2013 و2014، لم تتضمن أي إشارة صريحة إلى الأمن السيبراني، كما لم تتضمن إشارات إلى حماية البيانات والأصول الرقمية أو البيئة السيبرانية عموماً[53]. ومع أن إدارة شؤون السلامة والأمن أشارت إلى أن إرشادات أمن المعلومات تنطبق على نطاق المنظومة، فإن نظام إدارة الأمن في الأمم المتحدة ووثائق السياسات المرتبطة به لم توضح بعد نقاط التقارب بين الأمن المادي والأمن السيبراني بغية تحديد مسؤوليات مختلف أصحاب المصلحة في المنظومة في هذا الصدد. ويرحب المفتشون بإدراج مساحة تُملأ فيما بعد تحت عنوان "أمن المعلومات – الحساسية والتصنيف والتعامل" في دليل السياسة الأمنية لنظام إدارة الأمن في الأمم المتحدة، ويعتبرون ذلك علامة على وجود قدر من الاعتراف بأهمية اعتبارات الأمن السيبراني لوظيفة السلامة المادية والأمن. على أن الفصل ذا الصلة "لم يوضع بعد"، وقد أبدت إدارة شؤون السلامة والأمن تحفظات بشأن الحاجة إلى فصل منفصل في هذا الوقت. وفي الوقت نفسه، وكما أكد مكتب الشؤون القانونية، وعلى عكس التفسير المستقر القائل بأن من المفهوم أن الإشارات القانونية إلى حماية

(53) أشارت إدارة شؤون السلامة والأمن إلى أن الفئات المحددة للمخاطر الأمنية التي تغطيها الإدارة ونظام إدارة الأمن في الأمم المتحدة هي الاضطرابات المدنية، والنزاع المسلح، والإرهاب، والجرائم، والأخطار (غير المتعمدة).

الممتلكات والأصول في الاتفاقيات ذات الصلة وفي اتفاقات البلد المضيف تشمل الأصول الرقمية والاتصالات، فإنه لا يمكن القول بأن هناك تغطية للأمن السيبراني اليوم، لا في الولاية ولا في إطار السياسة العامة المرتبط بها واللذين ينظمان وظيفة السلامة المادية والأمن في منظومة الأمم المتحدة.

160- **الشبكة المشتركة بين الوكالات لإدارة الأمن والفريق المختص بأمن المعلومات.** كما أن اختصاصات الشبكة المشتركة بين الوكالات لإدارة الأمن، التي تدعم اللجنة الإدارية الرفيعة المستوى في استعراضها الشامل للسياسات والمسائل المتعلقة بالموارد والمتصلة بنظام إدارة الأمن في الأمم المتحدة وترصد تنفيذ جميع الجهات الفاعلة في منظومة الأمم المتحدة للسياسات والممارسات والإجراءات المتعلقة بإدارة الأمن، تفتقر أيضاً إلى إشارة محددة إلى الأمن السيبراني. وتؤكد الأبحاث التي أجرتها وحدة التفتيش المشتركة أن الشبكة المشتركة بين الوكالات لم تتناول الموضوع إلا في مناسبات نادرة، وأساساً من منظور استخدام تكنولوجيا المعلومات والاتصالات لتعزيز عمليات الأمن المادي الشاملة، من ذلك مثلاً في أغراض إدارة الهوية والوصول (مثل استكشاف خيارات بطاقات الهوية البيومترية للدخول إلى المباني المادية وكذلك إلى الفضاء الرقمي) أو في إجراءات التصديق بمساعدة تكنولوجيا المعلومات والاتصالات فيما يتعلق بالموافقات الأمنية على السفر. وفي الآونة الأخيرة، اعتمدت الشبكة الرقمية والتكنولوجية في عام 2019 توصية أصدرها الفريق المختص بأمن المعلومات بشأن إقامة تنسيق بين الفريق والشبكة المشتركة بين الوكالات "بشأن المسائل ذات الاهتمام المشترك"[(54)]. على أن المفتشين لم يتمكنوا من العثور على دليل على أن النية المعلنة تحققت خارج سياق مشاريع محددة. والآليات المعنية المشتركة بين الوكالات مدعوة لمواصلة استكشاف الطرائق العملية لإنشاء قناة للتواصل أكثر انتظاماً من أجل زيادة التعاون. وهناك اقتراح قُدِّم إلى المفتشين في هذا الصدد مفاده أن المشاركة المتبادلة لرئيسي الشبكة المشتركة بين الوكالات والفريق في اجتماعات كلا الكيانين يمكن أن تسهل تبادل الدروس المستفادة.

161- **مخطط أساسي للعمل مع السلطات الوطنية بشأن الحوادث السيبرانية.** يُعتبر العمل مع السلطات الوطنية فيما يتعلق بالهجمات السيبرانية مجالاً يمكن أن توفر فيه الإجراءات الموضوعة للسلامة والأمن المادي بعض الإلهام للعالم السيبراني. ويغطي المفتشون في الفصل الثاني (الفقرات 35-37) من هذا الاستعراض، وبشيء من التفصيل، العملية الداخلية المعقدة المؤدية إلى اتخاذ قرار بشأن ما إذا كان ينبغي الاتصال بالسلطات الوطنية، غير أنهم في ذلك الفصل لم يتعرضوا لمسألة ما سيحدث عقب اتخاذ ذلك القرار وكيف سيجري التواصل مع النظير الحكومي المعني. على أن الأمر بعيد كل البعد عن الوضوح، إذ أن النظير الأنسب على المستوى الوطني قد يختلف بين الوزارة المسؤولة التي تعمل بموجبها فرق الاستجابة (أو الاستعداد) للطوارئ الحاسوبية، والمعروفة أيضاً باسم فرق الاستجابة لحوادث الأمن الحاسوبية (مثل وزارات الداخلية أو الدفاع أو الاتصالات أو التكنولوجيا، رهناً باختصاص الوزارة المعنية) والقدرات الموازية التي قد تكون موجودة في نفس الدولة ضمن إطار وكالة الاستخبارات الوطنية ومفوضة لمتابعة الهجمات السيبرانية التي يُحتمل أن يكون لها بعد سياسي. لذلك، قد لا توجد جهة تنسيق مركزية تلقائياً على المستوى الوطني لتلقي التقارير ذات الصلة من مؤسسات منظومة الأمم المتحدة رسمياً، مما قد يؤدي إلى تعقيد توجيه المعلومات بشكل مناسب. وإرشاداً لإدارة الأزمات المتعلقة بالأمن المادي، ينص دليل السياسة الأمنية لنظام إدارة الأمن في الأمم المتحدة على أن المسؤولين المعينين "يجب أن يطلبوا من الحكومة المضيفة تعيين جهات تنسيق تتمتع بالسلطة لحشد وتنسيق الدعم عندما تؤثر أزمة ما على الأمم المتحدة في البلاد"[(55)]. ويمكن استكشاف نهج مشابه كمخطط أساسي لأغراض الحوادث السيبرانية، مع الاعتراف في نفس الوقت بأن المسؤولين المعينين سيستفيدون من مشورة الخبراء في وظيفة الأمن السيبراني المؤسسي في مثل هذه الأمور.

(54) CEB/2019/HLCM/DTN/02 وCEB/2019/HLCM/DTN/07، الصفحتان 4-5.

(55) دليل السياسة الأمنية لنظام إدارة الأمن في الأمم المتحدة، الفرع دال – العلاقات مع البلدان المضيفة حول المسائل الأمنية، الفقرة 14(د)، "إدارة الأزمات".

162- **عدم وجود آلية لإرسال المعلومات المتعلقة بالفضاء السيبراني ولتلقيها وتوجيهها داخل المنظومة.** وبالمثل، ينبغي وضع ترتيبات داخلية لتلقي المعلومات المتعلقة بالفضاء السيبراني من الحكومات، غير أن المفتشين لم يتمكنوا أثناء استعراضهم من التعرف بسهولة على ترتيبات كهذه. وأشار بعض المحاورين إلى وجود بعض الالتباس بين النظراء الحكوميين بشأن المنظمة التي يتعين الاتصال بها عندما يَتكشف هجوم سيبراني مكتشف على المستوى الوطني عن صلة بواحدة أو أكثر من مؤسسات منظومة الأمم المتحدة، وبشأن قناة الاتصال التي يجب استخدامها. وأشير إلى أن هذه المعلومات الاستخباراتية متاحة في كثير من الأحيان وجاهزة لتقاسمها، ولكن لا توجد آلية لإرسالها وتوجيهها بشكل موثوق إلى المتلقين المقصودين داخل المنظومة، ولا سيما عندما لا يكون واضحاً للكيانات الخارجية أيُ عضو من أعضاء أسرة الأمم المتحدة قد تتعلق به تلك المعلومات الاستخباراتية. وقد ذُكر أن هذا بدوره أدى في الماضي إلى ضياع فرص لحماية أصول المنظمات والدفاع عنها ضد التدخلات، لأنه لا يمكن ضمان وصول هذه المعلومات الاستخباراتية السيبرانية إلى متلقٍ لديه الخبرة اللازمة للتمكن من اتخاذ إجراء بشأنها. وعلى هذا فإن قنوات الاتصال الدبلوماسية القائمة لا تُعتبر فعالة بما فيه الكفاية، مما يؤدي إلى عدم تحقق المكاسب في مجال الأمن السيبراني لفرادى المنظمات وللمنظومة ككل.

163- **استصواب وملاءمة الأخذ بنهج منسق.** تتضمن الفقرات من 35 إلى 37 أعلاه شرحاً لبعض العوامل التي أدت إلى الممارسة الحالية غير المتكافئة بين مؤسسات منظومة الأمم المتحدة فيما يتعلق بالتعاون مع السلطات الوطنية. والسؤال الذي يطرح نفسه يدور حول ما إذا كانت التناقضات ذات الصلة تثير تحديات إضافية، بما في ذلك ما يُحتمل من مخاطر الإضرار بالسمعة في إدارة العلاقات مع البلد المضيف، لا سيما في الحالات التي يوجد فيها مقار أو حضور لعدد من منظمات الأمم المتحدة المتباينة النهُج إزاء المسألة، والتي تتعامل – أو لا تتعامل – مع نفس السلطات بشأن مسائل الأمن السيبراني. **ويطلب المفتشون إلى اللجنة الإدارية الرفيعة المستوى أن تفكر بشكل جماعي في مدى استصواب وملاءمة الأخذ بنهج منسق إزاء هذا التعاون ووضع توجيهات مناسبة في هذا الصدد.** إن الفريق المختص بأمن المعلومات، والشبكة المشتركة بين الوكالات لإدارة الأمن، وشبكة المستشارين القانونيين، في وضع جيد لتقديم الخبرات لإجراء دراسة مشتركة للمسألة وللنظر في المكاسب الأمنية المحتملة، والتحديات المرتبطة بها، وعلى وجه الخصوص، في جدوى تعيين جهات تنسيق لدى المنظمات، وكذلك على مستوى المنظومة، لإرسال المعلومات وتلقيها وتوجيهها بشأن التهديدات والمخاطر السيبرانية. ومع مراعاة أن مركز الأمم المتحدة الدولي للحوسبة يشارك في الشبكة المشتركة بين الوكالات، يلاحظ المفتشون أن المركز أعرب عن استعداده للقيام بدورٍ في تجميع المعلومات المتعلقة بحوادث الأمن السيبراني ونقلها إلى السلطات الوطنية بالنيابة عن مؤسسات منظومة الأمم المتحدة، إذا عُهد إليه رسمياً بهذا الدور. وفي حين أن تقديم التقارير والتعاون مع السلطات الوطنية مسألة تخضع لاختصاص كل منظمة، فإن المركز لديه إمكانية الوصول إلى المعلومات التي تمكّنه من تمييز الصلات والترابطات المحتملة بين الهجمات ضد المنظمات المختلفة، وهي منظمات يمكن القول إن أياً منها لا يمكنها القيام بذلك بمفردها، مما يعتبر حجةً لإمكانية زيادة دور المركز في هذه المسائل مما ينبغي استكشافه. ولذلك، ينبغي للآليات المعنية المشتركة بين الوكالات، عند نظرها في احتمال الأخذ بنهج منسق في هذا الصدد، أن تلتمس وأن تدرس مساهمات أصحاب المصلحة المعنيين، بما في ذلك المركز، لا سيما فيما يتعلق بقدرة المركز على جمع الأدلة العدلية المتعلقة بالتدخلات السيبرانية، والربط بينها وتحليلها، نيابة عن المنظومة.

164- **نحو مواءمة أوثق بين الأمن المادي والأمن السيبراني.** بشكل عام، وبالنظر إلى أن المبادئ التوجيهية لعام 1992 بشأن أمن المعلومات التي وضعها سلف الشبكة الرقمية والتكنولوجية قد تطرقت بالفعل إلى الروابط بين أمن أنظمة المعلومات والأمن المادي[56]، وأن المسألة عادت للظهور في مناقشات الهيئات

(56) المبادئ التوجيهية لأمن نظام المعلومات لمنظمات الأمم المتحدة.

ذات الصلة في عامي 2013 و2014[57]، فقد اعتبر المفتشون أن الوقت مناسب لإحياء الجهود المبذولة لإنشاء مواءمة أوثق لوظائف الأمن المادي والأمن السيبراني بغية ضمان توفير أكبر حماية ممكنة ضد التهديدات المعقدة. وتلعب إدارة شؤون السلامة والأمن، باعتبارها السلطة المركزية والكيان الذي يضع المعايير للمنظومة بأكملها، دوراً حاسماً في الاعتراف بنقاط التقارب الحالية ويمكن أن تصبح مساهماً رئيسياً نحو تحول كبير في الثقافة المؤسسية. والواقع أن التهديدات التي يتعرض لها الأمن المادي تؤخذ بالفعل على محمل الجد الكلي في منظومة الأمم المتحدة، ولا شك في ضرورة التصدي للتهديدات المادية بشكل فوري وفعال. وفي حين أن المفتشين وجدوا أن هناك إحساساً بأن التفكير المؤسسي يتطور بحذر فيما يتعلق بإضفاء نفس القدر من الإلحاح على نهج المنظمات إزاء التهديدات السيبرانية، فإن هناك حاجة إلى القيام بالمزيد من أجل التوسع في ما لدى إدارة شؤون السلامة والأمن حالياً من نهج قائم على المخاطر إزاء المجال المادي البحت، ومن استجابةٍ منظمة تركز على المساءلة في ذلك المجال، بحيث يشمل هذا النهج والاستجابة العالم السيبراني. ولا يعني ذلك أنه ينبغي تنقيح الولاية الممنوحة بالفعل لإدارة شؤون السلامة والأمن على نطاق المنظومة، لتمكينها من استيعاب الأمن السيبراني. فالمفتشون يقرّون بأن التعامل مع التحدي الحديث الذي يطرحه مرتكبو التهديدات السيبرانية يتطلب موارد وخبرات محددة لا تمتلكها حالياً إدارة شؤون السلامة والأمن، وأن نقل أي جزء من المسؤولية عن هذه المسألة لن يكون ممكناً بدون إحداث تعديلات كبيرة. فأي تحرك في هذا الاتجاه يستلزم إدخال تغييرات هيكلية تشمل فيما تشمله إجراءً من جانب الجمعية العامة، وإجراءَ تشاور وتنسيق داخليين موسعين مع مختلف أصحاب المصلحة في نظام إدارة الأمن في الأمم المتحدة، بما في ذلك الجوانب المتعلقة بالاحتياجات من الموارد الإدارية والمالية، وكذلك الحاجة إلى الارتقاء بمهارات موظفي الأمن، وهو ما ورد في موضع آخر من هذا التقرير (الفقرة 68). وفي الوقت الحاضر، يُظهر الاستعراض أن النقاش على نطاق المنظومة حول هذه المسألة ليس ناضجاً وهو بحاجة إلى جهود متجددة ودراسة أدق، استناداً إلى الخبرة المتاحة في المنظومة ولا سيما على مستوى الشبكة المشتركة بين الوكالات والفريق المختص بأمن المعلومات. ولذلك يوصي المفتشون بأن يستكشف الأمين العام الفرص لمواصلة الاستفادة من التقارب بين الأمن المادي والأمن السيبراني في منظومة الأمم المتحدة وأن يدرس مزايا وقيود السبل الممكنة للقيام بذلك. وينبغي، قدر الإمكان، أن يسترشد التقرير الذي سيقدم إلى الجمعية العامة بشأن هذه المسألة، بنتائج المشاورات التي ستُجرى بين آليات التنسيق المشتركة بين الوكالات والمعنية بالأمن السيبراني والشبكة المشتركة بين الوكالات، مع إسهام من مركز الحوسبة حسب الاقتضاء.

165- ويُنتظر أن يؤدي تنفيذ التوصية التالية إلى تعزيز فعالية استجابة منظومة الأمم المتحدة لتهديدات الأمن السيبراني.

التوصية 5

ينبغي للأمين العام أن يقدم تقريراً إلى الجمعية العامة للأمم المتحدة، في موعد لا يتجاوز دورتها الثامنة والسبعين، يستكشف المزيد من الفرص للاستفادة من التقارب بين الأمن المادي والأمن السيبراني لضمان توفير حماية أكثر شمولاً لموظفي الأمم المتحدة وأصولها، ويبين التدابير اللازمة لتعزيز الهياكل القائمة تبعاً لذلك، على أن يولي اهتماماً خاصاً لما يُمكن أن تضطلع به إدارة شؤون السلامة والأمن من دورٍ في هذا المضمار.

(57) CEB/2013/5، الفقرة 40؛ الدورة التاسعة عشرة للشبكة المشتركة بين الوكالات لإدارة الأمن (2013، وثيقة بلا رمز) والدورة العشرون للشبكة المشتركة بين الوكالات لإدارة الأمن (2014، وثيقة بلا رمز).

المرفق الأول

مسارات العمل الحكومية الدولية بشأن الأمن السيبراني والجريمة السيبرانية

المقدمة والمصطلحات المستخدمة

دأب المجتمع الدولي على مناقشة المسائل المتعلقة بالأمن السيبراني في عدد من الأطر الحكومية الدولية.

فمن ناحية، تدارست الموضوع لجان مختلفة تابعة للجمعية العامة والهيئات التابعة لها أو المرتبطة بها. وركز أحد مسارات العمل على الجريمة السيبرانية (كان يشار إليها في أوائل التسعينيات بالجرائم المتعلقة بالحاسوب)، بينما ركز مسار آخر على المعلومات والاتصالات في سياق الأمن الدولي (وهو مسار يشمل أمن تكنولوجيا المعلومات والاتصالات والمواضيع ذات الصلة).

ومن ناحية أخرى، تشمل ولايات عدد من المنظمات المشارِكة جوانب من الأمن السيبراني تخضع للعمليات الحكومية الدولية التي تدعمها تلك المنظمات، ومنها مثلاً الاتحاد الدولي للاتصالات، ومكتب شؤون نزع السلاح، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، والمنظمة العالمية للملكية الفكرية، وبرنامج الأمم المتحدة الإنمائي، ومؤتمر الأمم المتحدة للتجارة والتنمية، والوكالة الدولية للطاقة الذرية.

ولا يمكن استخدام مصطلحي "الجريمة السيبرانية" و"الأمن السيبراني" على أساس تبادلي بينهما، مع أنهما يعالجان نفس المشكلة من زوايا مختلفة. ويمكن القول إن مصطلح الجريمة السيبرانية يركز على ارتكاب الهجمات السيبرانية وعلى مسؤولية المهاجمين الجنائية عن مشاركتهم في أنشطة غير مشروعة (أنشطة ممكَّنة سيبرانياً أو قائمة على الفضاء السيبراني). وفي المقابل، يهتم مصطلح الأمن السيبراني بالدفاع ضد هذه الهجمات، وينصب الاهتمام فيه على المستهدَف بالجريمة ودفاعاته وليس على الجاني.

ويقدم هذا المرفق لمحة عامة عن مختلف مسارات العمل الحكومية الدولية على مستوى مؤسسات منظومة الأمم المتحدة، وعن أصولها وعملها الحالي، فضلاً عن العلاقة بينها، في حال وجودها.

مسار العمل الأول: الجريمة السيبرانية

الجريمة السيبرانية مطروحة على جدول الأعمال العالمي منذ التسعينيات. يعود إلى عام 1990 أولُ سجل موثق لإدراك أوساط المجتمع الدولي للحاجة إلى توجيه الاهتمام على نحو مكرس إلى البعد السيبراني للعمل البرنامجي، وكذلك إلى الاستثمار في قدرة الدول القومية على صد الهجمات السيبرانية (بدعم من المساعدة التقنية التي تقدمها مؤسسات منظومة الأمم المتحدة ذات الصلة)، وكان قد نشأ أصلاً في سياق مكافحة الجريمة العابرة للحدود. وعلى وجه التحديد، أقرت الجمعية العامة، في قرارها 121/45، توصيات مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، ولا سيما القرار المتعلق بالجرائم المتصلة بالحاسوب، الذي دُعيت فيه الدول إلى تكثيف جهودها لمكافحة الانتهاكات المتصلة بالحاسوب بشكل أكثر فعالية. ويستمر العمل في هذا الموضوع تحت عنوان "مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية"[(1)] في اللجنة الثالثة للجمعية العامة (اللجنة الاجتماعية والإنسانية والثقافية)، وتحت عنوان "الجريمة السيبرانية" في سياق لجنة منع الجريمة والعدالة الجنائية (وهي إحدى

(1) قرارات الجمعية العامة 187/73 و247/74 و539/75 والقراران الأقدمان 63/55 و121/56.

اللجان الفنية التابعة للمجلس الاقتصـــادي والاجتماعي). ويقدم مكتب الأمم المتحدة المعني بالمخدرات والجريمة الدعم الفني والإداري لهذا العمل.

العمل الجاري نحو اتفاقية دولية بشـأن الجريمة السـيبرانية. اسـتمرت الجهود المبذولة لتجميع "دراسـة شـاملة لمشـكلة الجريمة السـيبرانية" منذ عام 2010 في سـياق فريق خبراء حكومي دولي مفتوح العضـوية (يشـار إليه باسم "فريق الخبراء الحكومي الدولي المعني بالجريمة السيبرانية")، نُظم لهذا الغرض برعاية لجنة منع الجريمة والعدالة الجنائية[2]. وقد اكتســبت مجموعة الأعمال الناتجة عن ذلك زخماً تمخض عنه مسعى منفصل لوضع صك ملزم قانوناً بشأن الجريمة السيبرانية. وتشرف على عملية صياغة هذا الصك والتفاوض بشأنه لجنة مخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصـالات للأغراض الإجرامية (يشـار إليها باسـم "اللجنة المخصـصـة")، أنشـأتها الجمعية العامة في عام 2019 وبدأت عملها في عام 2020[3]. أما الناتج الذي ســتتمخض عنه هذه العملية فسـيوجَّه أسـاسـاً إلى الدول القومية كأطراف في الاتفاقية التي سـتُبرم في نهاية المطاف. ويهدف الإطار القانوني لتلك الاتفاقية بصـورة غالبة إلى تنظيم معاملة المجرمين الأفراد (مجرمو الفضـاء السـيبراني) على المسـتوى الوطني، وبالتالي ليس له تأثير مباشـر يذكر على نهج مؤسـسـات منظومة الأمم المتحدة إزاء الأمن السيبراني. ولذلك فإن المساعي ذات الصلة لا تحظى باهتمام كبير في هذا الاستعراض.

مسار العمل الثاني: المعلومات والاتصالات في سياق الأمن الدولي

في مسـار ثان للعمل الحكومي الدولي، اعتباراً من عام 1998، بدأ "النظر في التهديدات القائمة والمحتملة في مجال أمن المعلومات" في الظهور في قرارات الجمعية العامة في إطار بند جديد في جدول الأعمال أصـــبح متكرراً من ذلك الحين، وعنوانه: "التطورات في ميدان المعلومات والاتصـــالات الســلكية واللاســلكية في ســياق الأمن الدولي"[4]. وتتناول الموضـــوع هيئتان حكوميتان دوليتان تعملان في إطار اللجنـة الأولى (لجنـة نزع السـلاح والأمن الـدولي) التـابعـة للجمعيـة العـامـة، وهمـا: (أ) فريق الخبراء الحكوميين، وهو هيئة مؤلفة من عدد محدود من الخبراء يرشحهم الأمين- ويعملون بصفتهم الشخصية[5]، والفريق هو حالياً السـادس من نوعه منذ إنشـاء أول فريق من هذا القبيل في عام 2004[6]؛ و(ب) الفريق العامل المفتوح العضوية المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (مفتوح أمام جميع الدول الأعضـــاء في الأمم المتحدة، وأنشـــئ في عام 2018)[7]. وتتمثل الأهداف الرئيســية للفريقين في "النظر في التهديدات الحالية والمحتملة في مجال أمن المعلومات والتدابير التعاونية الممكنة لمواجهتها"[8] وفي "زيادة تطوير قواعد ومعايير ومبادئ السلوك المسؤول للدول [المدرجة في القرار] وطرق تنفيذها"[9]. وقد أكمل كل من الفريق العامل المفتوح العضـــوية وفريق الخبراء الحكوميين الســـادس عملهما واعتمدا تقريرين بتوافق الآراء في آذار/مارس وأيار/مايو 2021 على التوالي[10].

(2) قرار الجمعية العامة 230/65.

(3) قرار الجمعية العامة 247/74.

(4) انظر قرار الجمعية العامة 70/53 والقرارات اللاحقة وآخرها القرار 240/75.

(5) انظر قرار الجمعية العامة 32/58.

(6) انظر قرار الجمعية العامة 226/73.

(7) انظر قرار الجمعية العامة 27/73.

(8) انظر قرار الجمعية العامة 32/58، الفقرة 4.

(9) انظر قرار الجمعية العامة 27/73.

(10) انظر A/75/816.

ومن المتوقع أن ينظر الفريق العامل الجديد المفتوح العضوية والمعني بأمن واستخدام تكنولوجيا المعلومات والاتصالات للفترة 2021-2025 في عمل سلفه (الذي غطى الفترة 2019-2020) وأن يجتمع لأول مرة في عام 2021[11]. ويقدم مكتب الأمم المتحدة لشؤون نزع السلاح الدعم الفني والإداري لهاتين الهيئتين.

ولايات مؤسسات منظومة الأمم المتحدة بشأن الأمن السيبراني

تتطرق ولايات التعاون الفني والتقني لدى عدد من مؤسسات منظومة الأمم المتحدة إلى جوانب الأمن السيبراني. ومن الأمثلة على ذلك الاتحاد الدولي للاتصالات، الذي، في جملة أمور، يستضيف المنتدى السنوي للقمة العالمية لمجتمع المعلومات، وهو الوسيلة الرئيسية للدفع بمسألة تسخير تكنولوجيا المعلومات والاتصالات لأغراض التنمية، والميسر الوحيد لخط العمل C5 في القمة العالمية لمجتمع المعلومات، المعنون: "بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات". وفي سياق دوره هذا، يعمل الاتحاد مع أصحاب المصلحة الرئيسيين لمساعدة البلدان في أمور منها اعتماد استراتيجيات وطنية للأمن السيبراني، وإنشاء قدرات وطنية للاستجابة للحوادث، ونشر معايير الأمن الدولية، وحماية الأطفال على الإنترنت، وبناء القدرات. وقد أشير إلى بعض الأعمال المضطلع بها في سياق القمة العالمية لمجتمع المعلومات في قرارات الجمعية العامة المعنونة "إرساء ثقافة عالمية تكفل أمن الفضاء الإلكتروني"، والتي تتناولها بالتفصيل اللجنة الثانية التابعة للجمعية العامة (اللجنة الاقتصادية والمالية)[12]. وتشمل المنظمات الأخرى التي لديها ولايات تشمل عنصر الأمن السيبراني مكتب الأمم المتحدة المعني بالمخدرات والجريمة، والمنظمة العالمية للملكية الفكرية، وبرنامج الأمم المتحدة الإنمائي، ومؤتمر الأمم المتحدة للتجارة والتنمية، ومكتب شؤون نزع السلاح، والوكالة الدولية للطاقة الذرية، فضلاً عن العديد من المنظمات الأخرى بدرجات متفاوتة.

ويتمثل القصد من القيام، في إطار مجلس الرؤساء التنفيذيين، بتجميع موجز للولايات والأنشطة الرئيسية لمؤسسات منظومة الأمم المتحدة بشأن الأمن السيبراني والجريمة السيبرانية، في عرض معالم جميع السبل التي شاركت بها تلك المؤسسات، في إطار ولاية كل منها وتركيزها، في تقديم المساعدة التقنية ودعم صياغة السياسات في هذا المجال على مر السنين. على أن ذلك الموجز ظل وثيقة داخلية ظهر أن استكمالها في صيغتها النهائية وتحديثها مهمة ضخمة لا يمكن القيام بها. وهو يقدم قدراً كبيراً جداً من الأدلة على تنوع العمل البرنامجي لمؤسسات منظومة الأمم المتحدة، وتجزئته، في هذا الموضوع. وفي هذا السياق، أشارت اللجنة الرفيعة المستوى المعنية بالبرامج مراراً إلى ضرورة اتباع المنظومة لنهج منسق ومتسق، مع مراعاة الطبيعة التكاملية للولايات الخاصة بكل منظمة، وكذلك درجة التداخل بينها[13].

(11) انظر قرار الجمعية العامة 240/75.

(12) انظر قراري الجمعية العامة 239/57 و211/64.

(13) انظر على سبيل المثال CEB/2010/HLCP-XX/CRP.7، الفقرة 3؛ وCEB/2010/6، الفقرات 38-43؛ وCEB/2011/HLCP-XXII/CRP.6؛ وCEB/2014/6، الفقرات 42-49.

المرفق الثاني

بعض عناصر نهج قائم على المخاطر إزاء الأمن السيبراني

بالإضافة إلى إضافة الأمن السيبراني رسمياً إلى سجل المخاطر المؤسسية أو مصفوفة المخاطر في المنظمة، يرغب المفتشون في تسليط الضوء على ثلاثة جوانب لنهج قائم على المخاطر إزاء الأمن السيبراني يمكن أن يعجل بتحقيق الفوائد ذات الصلة: (أ) نهج مصمم خصيصاً ومنهجي وقابل للتكييف إزاء تقييم المخاطر؛ و(ب) بيان استراتيجي رفيع المستوى بشأن درجة تقبل المخاطر وتحملها؛ و(ج) توفر فرص كافية أمام المختصين بالأمن السيبراني ليصبّوا ما لديهم من خبرة في عملية إدارة المخاطر؛ و(د) استخدام اختبار الاختراق كأداة لإدارة المخاطر.

- **تقييمات للمخاطر مصممة خصيصاً**. يجب أن تكون تقييمات مخاطر الأمن السيبراني مصممة خصيصاً لتناسب السياق الذي تعمل فيه المنظمة، مع إيلاء الاعتبار الواجب لمعايير من قبيل ولايتها، والقدرة المالية وقدرات الموظفين، ونموذج الأعمال، ونوع المعلومات المحتفظ بها أو المملوكة، وخصوصيات المنظمة، ولا سيما كيفية تأثير حوادث الأمن السيبراني على إنجاز المهام المنوطة بها، بما في ذلك في البيئات اللامركزية أو المواقع الميدانية المتنوعة. وتستشهد بعض المنظمات المشارِكة بمعايير الصناعة لدعم عمليتها الخاصة بتقييم المخاطر، وهو ما يمكن اعتباره ممارسة جيدة، شريطة أن يتم اختيار المعايير المشار إليها على أساس مدى ملاءمتها لسياق المنظمة المعنية (الفقرات 59-64). وبالإضافة إلى جعل تقييمات المخاطر مصممة خصيصاً، يتعين تسليط الضوء على صفتها الدورية، والتي لا تيسر الأخذ بنهج منهجي فحسب، بل تضمن أيضاً قابلية إطار العمل للتكيف، وبشكل مثالي، الاستجابةَ المخصصة لمشهد التهديدات المتطور باستمرار والذي قد لا يكون متوائماً مع دورات الاستعراض المنتظمة.

- **بيان درجة تقبل المخاطر وتحملها**. يتمثل أحد المكونات الرئيسية لنهج أكثر استراتيجية إزاء إدارة مخاطر الأمن السيبراني في وضع بيان درجة تقبل المخاطر وتحملها، مما يتحقق، من الناحية المثالية، بمشاركة الهيئات التشريعية والإدارية وكذلك الإدارة التنفيذية للمنظمة (الفقرات 53-54). ويُبنى بيان درجة تقبل المخاطر وتحملها، بشكله الأكثر جدوى، على أساس تقييم شامل ودوري لمخاطر الأمن السيبراني، وهو يغطي جميع فئات تهديدات الأمن السيبراني، وليس فقط التهديدات العدائية والخارجية بالنسبة للمنظمة (الفقرات 25-29)، ويجمع المعلومات من إدارة تكنولوجيا المعلومات والاتصالات حول حالة أنظمة المعلومات المؤسسية وأوجه الضعف المعروفة في المنظمة، وكذلك من وحدات الأعمال انطلاقاً من روح نهج المنظمة بأكملها. ويكتسي تحديد الدرجة المناسبة لتقبل المخاطر أهمية قصوى عندما يستند إلى مجموعة مختارة ومصممة بعناية من مقاييس الأمن السيبراني الهادفة. والعملية هذه محددة بكل منظمة بذاتها وهي تؤدي إلى اتخاذ مزيد من القرارات الإدارية، مثل إنشاء قدرة داخلية (على خلاف الاستعانة بمصادر خارجية) للأمن السيبراني المؤسسي؛ والموارد المخصصة لها؛ والأدوات وتوجيهات السياسات المدرجة في الإطار التنظيمي؛ وقرارات الاستثمار والاستجابة للحوادث في حالة التصعيد. وفي منظمات من قبيل المنظمة العالمية للملكية الفكرية والوكالة الدولية للطاقة الذرية، اللتين تديران معلومات بالغة الحساسية، قد تكون درجة تقبل المخاطر منخفضة

بالضـــرورة. كما يمكن أن يؤدي التعرض الســـابق لحوادث الأمن الســـيبراني الكبيرة إلى خفض درجة تقبل المخاطر، على أن ذلك ينطوي على مخاطر زيادة الاســـتثمار في الدفاعات السيبرانية مما قد يخلق بدوره إحساساً زائفاً بالأمان.

- **وجوب أن تصـــبّ خبرة الأمن الســـيبراني في عمليات إدارة المخاطر.** قد يبدو توفير فرص كافية لخبراء الأمن السيبراني لإرشاد عمليات إدارة مخاطر الشركات أمراً بديهياً ولكنه بعيد عن الواقع في العديد من المنظمات. وفي حين أن شـــكل مدخلات الخبراء وتواترها ليسا العامل الحاسم، فإن وجود شكل موثوق (غير معوق وغير مخصص) لوصول متخصصي الأمن السيبراني إلى القوى المحركة لإدارة المخاطر داخل المنظمة أمر ضـــروري وينبغي تأســـيســـه بصـــورة منهجية تضـــمن أن تنعكس اعتبارات الأمن السيبراني البالغة الأهمية في مراحل التصميم والتنفيذ والرصد من إطار إدارة المخاطر في المنظمة. وفي بعض المنظمات، يشـــارك رئيس موظفي أمن المعلومات، في حال وجود هذا المنصب، في لجنة إدارة المخاطر المؤسسية، أو حتى يُعين عضواً رسمياً فيها. والتعقيبات الواردة بشـــأن هذا الترتيب إيجابية، وقد يكون من المفيد ترســـيخه كممارسة في جميع المنظمات.

- **اختبار الاختراق كأداة لإدارة المخاطر.** اختبار الاختراق (كثيراً ما يُختصر باسم اختبار "pen") هو محاكاة مأذون بها لهجوم يجري في العالم الحقيقي يســـتهدف شـــبكات المنظمات وأنظمتها ومواردها البشرية، باستخدام أدوات وتقنيات يستخدمها المهاجمون عادةً، وذلك بهدف تحديد أوجه الضعف في حماية المنظمة، وتقييم فعالية تدابير التخفيف المعمول بها، واختبار إجراءات الاســـتجابة والتعافي. ويقوم باختبار الاختراق في الغالب متعاقدون خارجيون ضمن قواعد مصممة لتمكين إجراء تقييم مصمم خصيصاً وفعال، وفي الوقت نفسه لتقليل احتمال حدوث أضرار جسيمة لأصول المنظمات وعملياتها. وتســـتفيد عدة منظمات مشـــارِكة من هذه الأداة، وفي بعض الحالات تقوم بإشـــراك متعاقدين مختلفين (على سبيل المثال بالتناوب) على مدار فترة زمنية، ويفضل أن تكون خصـــائصـــهم مختلفة. وتتمثل مهمتهم في مهاجمة المنظمة ("الفريق الأحمر") واختبار استعداد الدفاع ("الفريق الأزرق"). وأخذت إحدى المنظمات بنهج أن ينضم إلى متعاقد خارجي (يُجري محاكاة الهجوم) أعضـــاءٌ من مركز العمليات الأمنية لديها (للدفاع ضد الهجوم)، مما يتيح التواصل في الوقت الفعلي بين الفريقين فيما يتعلق بالنتائج وإجراءات التخفيف الممكنة ("الفريق البنفسجي"). وسواء كانت المنظمة تستخدم متعاقداً واحداً أو أكثر، فإن اختبار الاختراق نشـــاطٌ يتطلب إعداداً قوياً واختياراً دقيقاً لمقيّمين خبراء جديرين بالثقة (يقومون بدور المهاجمين)، إذ إن هناك مخاطر حقيقية ينطوي عليها السماح حتى بالوصول المؤقت إلى الأنظمة والمعلومات الحساسة. بيد أن هذا الاختبار أداة متطورة وفعالة لإدارة المخاطر يمكن اســـتخدامها لدعم تخطيط اســـتمرارية الأعمال، وهو طريقة صـلبة لاكتسـاب رؤية متعمقة سريعة لوضـع الأمن السيبراني للمنظمة من زوايا متنوعة، وتسليط الضوء على الثغرات في دفاعاتها الشاملة أو على أوجه الضعف المحددة في مجالات معزولة، وذلك حسب النطاق المحدد للعملية.

المرفق الثالث

معايير الأمن السيبراني الرئيسية في الصناعة والتي أشارت إليها المنظمات المشارِكة في وحدة التفتيش المشتركة

معيار المنظمة الدولية لتوحيد المقاييس رقم 27001 (المنظمة الدولية لتوحيد المقاييس، 2005)[1]

يُستخدم معيار المنظمة الدولية لتوحيد المقاييس رقم 27001 بشكل أساسي لأغراض المراجعة والامتثال، وهو يركز في المقام الأول على ما ينبغي تحقيقه فيما يتعلق بالمجالات التقنية لدفاعات الأمن السيبراني، ويقدم التوجيهات في هذا الشأن. ويتبع المعيار مجموعة عامة من الضوابط تشمل 14 عنصراً للضبط وتهدف إلى إدماج الأمن السيبراني في أهداف أعمال المنظمة وممارساتها الخاصة بإدارة المخاطر. وتغطي مجموعات الضوابط الرئيسية سياسات أمن المعلومات، وإدارة الأصول، والتحكم في الوصول، وأمن العمليات والاتصالات، وإدارة الحوادث، والامتثال. ونظراً لخصائصه، يبدو أن إطار العمل هذا هو الأنسب لاستعراض ومراجعة تدابير الأمن السيبراني في المنظمات الكبيرة ذات الموارد الجيدة.

إطار عمل المعهد الوطني الأمريكي للمعايير والتكنولوجيا، 1901[2]

من خلال تحديد أهداف المنظمة وأولوياتها وتنظيم الإجراءات المناسبة، يوفر المعهد الوطني الأمريكي للمعايير والتكنولوجيا توجيهات مرنة وقابلة للتكيف لفهم مخاطر الأمن السيبراني. وبالإضافة إلى توجيهاته الداخلية، يتضمن الإطار، الذي خضع للتحديث مؤخراً في عام 2015، إشارات إلى معايير وتوجيهات وممارسات أخرى، مثل الضوابط التي يطرحها مركز ضوابط أمن الإنترنت، والمعايير الدولية للمنظمة الدولية لتوحيد المقاييس، وأهداف الرقابة للمعلومات وما يتصل بها من تكنولوجيا، وغيرها. وتحدد خطة عمل المعهد خمس وظائف أساسية (التحديد والحماية والكشف والاستجابة والتعافي) وتصنف تدفقات المعلومات والقرارات في مستويات مختلفة ضمن المنظمة. ونظراً لنهجه الشديد الشمول، يبدو أن المعيار مناسب بشكل خاص لتحديد استراتيجيات وسياسات الأمن السيبراني للمنظمة المعنية.

أهداف الرقابة للمعلومات وما يتصل بها من تكنولوجيا (رابطة مراجعة أنظمة المعلومات ومراقبتها، 1996)[3]

تستند أهداف الرقابة للمعلومات وما يتصل بها من تكنولوجيا، وهي إطار للحوكمة والإدارة لتكنولوجيا المعلومات، إلى أفضل الممارسات التي تساعد المنظمات على تحقيق أهدافها في مجالات الامتثال وإدارة المخاطر، وعلى مواءمة استراتيجيتها الخاصة بتكنولوجيا المعلومات مع أهدافها. ويتبع نهجها مفهوم مستويات القدرة مع التركيز على تقديم خدمات مهيأة خصيصاً لاحتياجات المنظمة. وبموجب هذا المعيار الدولي، تصنف جوانب أمن المعلومات كجزء من إدارة المخاطر واستمرارية خدمات الأعمال وتوفرها. وإضافة إلى المواد الداخلية، تشير أهداف الرقابة للمعلومات وما يتصل بها من تكنولوجيا إلى معايير وأدلة أخرى، منها إطار عمل المعهد الوطني الأمريكي للمعايير والتكنولوجيا، ومعيار المنظمة

(1) متاح في www.iso.org/home.html.

(2) متاح في www.nist.gov.

(3) متاح في www.isaca.org/credentialing/cobit/cobit-foundation.

الدولية لتوحيد المقاييس رقم 27001، ومركز ضـوابط أمن الإنترنت. وتشـمل أهداف المواءمة الواردة في الأهداف والأكثر صـلة إدارة مخاطر تكنولوجيا المعلومات، وأمن المعلومات، والامتثال، واسـتمرارية خدمة الأعمال، وتوفرها. وفيما يتعلق بتوجيهات الأمن السـيبراني، يبدو أن المعيار مناسـب بشـكل خاص للمنظمات التي تسـتخدم بالفعل أهداف الرقابة هذه كإطار عمل للحوكمة والإدارة فيما يتعلق بتكنولوجيا المعلومات والاتصـالات لديها. علاوة على ذلك، يمكن توسـيع المعيار من خلال دمجه بالمعايير الأخرى التي يشير إليها (مركز ضوابط أمن الإنترنت، وإطار عمل المعهد الوطني الأمريكي للمعايير والتكنولوجيا، ومعيار المنظمة الدولية لتوحيد المقاييس رقم 27001).

مكتبة الهياكل الأسـاسـية لتكنولوجيا المعلومات (الوكالة المركزية للحاسـوب والاتصـالات في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، الثمانينيات)[4]

مكتبة البنية التحتية لتكنولوجيا المعلومات هي مجموعة من المبادئ التوجيهية لإدارة خدمات تكنولوجيا المعلومات والاتصـالات وتتألف من سلسلة من المنشورات التي تقدم توجيهات بخصـوص تنفيذ خدمات تكنولوجيا المعلومات والاتصـالات وبشـأن العمليات والموارد اللازمة التي تتطلبها المنظمات. وقد طورت هذا المعيار الوكالة المركزية للحاسـوب والاتصـالات في المملكة المتحدة خلال الثمانينيات، وهو معروض كسـلسـلة من خمسـة مجلدات، يغطي كل منها مرحلة مختلفة من دورة إدارة خدمات تكنولوجيا المعلومات والاتصـالات. وتشمل الموضـوعات الرئيسية تعريف قيمة الخدمات، وتطوير الأعمال، وأصـول الخدمات، وتحليل السـوق، وأنواع مقدمي الخدمات. واعتباراً من عام 2005، سـاهمت ممارسـات مكتبة البنية التحتية في معيار المنظمة الدولية لتوحيد المقاييس رقم 20000 وباتت متوائمة معه.

مركز ضوابط أمن الإنترنت، 2008[5]

يُعرف هذا المعيار أيضـاً باسـم ضـوابط الأمن السـيبراني الحرجة، وهو يقدم مجموعة من التوصـيات اسـتناداً إلى أفضـل ممارسـات الصـناعة. ومع أن توجهه تقني في المقام الأول، إلا أن مركز ضـوابط أمن الإنترنت لديه أيضـاً بضـعة ضـوابط تتعامل مع الجوانب الأوسـع للأمن السـيبراني في المنظمات، مثل التدريب الخاص بالتوعية، والاسـتجابة للحوادث. ويبدو أن إطار العمل عملي تماماً ومفيد جداً من حيث مجموعات التنفيذ، فهو يركز على الإجراءات التي يتعين تنفيذها وفقاً لحجم المنظمة ومهاراتها والموارد المتاحة لديها وحساسية بياناتها. وتشمل ضوابطه الرئيسية الجرد والأصول، وإدارة أوجه الضـعف، والتكوين الآمن، وحماية البريد السـيبراني ومتصـفح الويب، واسـتعادة البيانات وحمايتها، والاستجابة للحوادث، واختبارات الاختراق. وقد أثبت هذا النهج أنه مناسب بشكل خاص لتنفيذ استراتيجيات دفاع الأمن السـيبراني في المنظمات الصـغيرة والمتوسـطة الحجم التي لديها أطر عمل للمخاطر موجودة بالفعل وتشمل جوانب الأمن السيبراني.

(4) متاح في www.axelos.com/best-practice-solutions/itil.

(5) متاح في www.cisecurity.org/controls/.

المرفق الرابع

الأطر التنظيمية لمؤسسات منظومة الأمم المتحدة بشأن الأمن السيبراني

(أ) طبقات الإطار التنظيمي للأمن السيبراني

المستوى الاستراتيجي	في كثير من الأحيان وثيقة واحدة تحتوي على بيانات رفيعة المستوى مصاغة بلغة طموحة	تحدد رؤية المنظمة والأهداف والمبادئ الشاملة، وتعرض الأدوار والمسؤوليات الأساسية الخاصة بالحوكمة في المنظمة، وقد توضح الأمن السيبراني كقرار خاص بالأعمال، وتشمل البيان الخاص بدرجة تحمل المخاطر أو تقبلها	تنطبق على المنظمة على مستواها ككيان، وتتوجه بشكل أساسي إلى الإدارة العليا للتنفيذ
مستوى السياسات	سلسلة من الوثائق المستقلة تحتوي على لغة إلزامية وقابلة للتنفيذ، تُنشر عادةً كإصدارات إدارية رسمية	تعرض مبادئ المنظمة التي يقوم عليها نظام إدارة أمن المعلومات وتبين التنظيمات والقواعد الداخلية الملزمة التي تحتوي على بيانات الغرض والإجراءات المرتبطة مصنفة حسب الموضوع (مثل تصنيف المعلومات وإدارة المخاطر واستمرارية الأعمال والتعافي من الكوارث والاستخدام المقبول لبيانات وأصول تكنولوجيا المعلومات والاتصالات) وتعيين أدوار ومسؤوليات محددة	تنطبق على جميع الموظفين وتنطوي على إمكانية فرض عقوبات تأديبية في حالات عدم الامتثال
المستوى الإجرائي	سلسلة من المبادئ التوجيهية أو إجراءات التشغيل القياسية التي تدعم سياسات المستوى الأعلى من خلال وصف العمليات التي تهدف إلى التأسيس لممارسات منهجية	توفر إرشادات مفصلة حول خطوات محددة يتعين اتخاذها أو سلوكيات يتعين تجنبها (الالتزام بقواعد استخدام كلمة المرور، وإجراء عمليات فحص منتظمة لمكافحة الفيروسات والقيام بتحديثات البرمجيات، ومسح أدوات الناقل التسلسلي العام (USB) المستلمة كهدية قبل الاستخدام؛ وما إلى ذلك)	يمكن أن تنطبق على جميع الموظفين أو تكون موجهة نحو أدوار محددة (مثل موظفي تكنولوجيا المعلومات والاتصالات، ومديري المحفوظات والسجلات، والمتخصصين في المشتريات)
المستوى التقني	سلسلة من البروتوكولات التقنية التي تهدف إلى التنفيذ الصحيح والموحد	تعرض التوجيهات التفصيلية والتدريجية التي تتطلب خبرة كبيرة في الموضوع لتطبيقها وتنفيذها. ويمكن للموضوعات أن تشمل، في جملة أمور، تكوين قاعدة البيانات وأمن الشبكة والأمن السحابي	موجهة بشكل رئيسي إلى الخبراء التقنيين

المصدر: من إعداد وحدة التفتيش المشتركة.

(ب) استراتيجيات تكنولوجيا المعلومات والاتصالات والوثائق المكرسة لسياسات الأمن السيبراني في المنظمات المشارِكة

المنظمات المشارِكة	*الاستراتيجية المؤسسية لتكنولوجيا المعلومات والاتصالات التي تتضمن عنصراً للأمن السيبراني*	*الوثائق المكرسة لسياسة الأمن السيبراني*
الأمانة العامة للأمم المتحدة	نعم، تكنولوجيا المعلومات والاتصالات في الأمم المتحدة (A/69/517) وقرار الجمعية العامة 262/69	نعم، أمر توجيهي خاص بسياسة أمن المعلومات للأمانة العامة للأمم المتحدة (2013)
برنامج الأمم المتحدة المشترك المعني بفيروس نقص المناعة البشرية/الإيدز	لا، استراتيجية تكنولوجيا المعلومات والاتصالات (2017–2020) لا تشمل الأمن السيبراني	لا، يعمل برنامج الأمم المتحدة المشترك المعني بفيروس نقص المناعة البشرية/الإيدز على وضع خطة عالمية للأمن السيبراني ستتضمن أيضاً سياسة للأمن السيبراني
مؤتمر الأمم المتحدة للتجارة والتنمية	يتبع استراتيجية تكنولوجيا المعلومات والاتصالات بالأمانة العامة للأمم المتحدة	نعم، يتبع استراتيجية الأمن السيبراني بالأمانة العامة للأمم المتحدة
برنامج الأمم المتحدة الإنمائي	نعم، استراتيجية تكنولوجيا المعلومات (2020–2023)	نعم، سياسة أمن المعلومات (2016)
برنامج الأمم المتحدة للبيئة	يتبع استراتيجية تكنولوجيا المعلومات والاتصالات بالأمانة العامة للأمم المتحدة	نعم، يتبع استراتيجية الأمن السيبراني بالأمانة العامة للأمم المتحدة
صندوق الأمم المتحدة للسكان	نعم، استراتيجية تكنولوجيا المعلومات والاتصالات (2018–2021)	نعم، سياسة أمن تكنولوجيا المعلومات والاتصالات
موئل الأمم المتحدة	يتبع استراتيجية تكنولوجيا المعلومات والاتصالات بالأمانة العامة للأمم المتحدة	نعم، يتبع استراتيجية الأمن السيبراني بالأمانة العامة للأمم المتحدة
مفوضية الأمم المتحدة لشؤون اللاجئين	نعم، استراتيجية تكنولوجيا المعلومات (2020–2022) (المسودة النهائية قيد الاستعراض)	قيد التطوير حالياً
منظمة الأمم المتحدة للطفولة	نعم، استراتيجية تكنولوجيا المعلومات والاتصالات	نعم، خطة اليونيسف الإستراتيجية لأمن المعلومات (2018–2022)
مكتب الأمم المتحدة المعني بالمخدرات والجريمة/مكتب الأمم المتحدة في فيينا	يتبع استراتيجية تكنولوجيا المعلومات والاتصالات بالأمانة العامة للأمم المتحدة	نعم، يتبع استراتيجية الأمن السيبراني بالأمانة العامة للأمم المتحدة
مكتب الأمم المتحدة لخدمات المشاريع	استراتيجية تكنولوجيا المعلومات والاتصالات مدتها خمس سنوات (قيد التطوير)	نعم، أمن المعلومات
وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين في الشرق الأدنى	نعم، استراتيجية الإدارة المعنية بإدارة المعلومات (2019–2020)	هناك سياسة أمن معلومات منفصلة (في انتظار الموافقة النهائية)
هيئة الأمم المتحدة للمرأة	نعم، استراتيجية تكنولوجيا المعلومات والاتصالات (2018–2021)	نعم، سياسة أمن المعلومات
برنامج الأغذية العالمي	نعم، الاستراتيجية المؤسسية لتكنولوجيا المعلومات (2016–2020)	نعم، السياسة المؤسسية لأمن المعلومات وتكنولوجيا المعلومات (2015)
منظمة الأغذية والزراعة للأمم المتحدة	نعم، الاستراتيجية الرقمية لتكنولوجيا المعلومات والاتصالات (2017)	نعم، سياسة أمن المعلومات

المنظمات المشارِكة	*الاستراتيجية المؤسسية لتكنولوجيا المعلومات والاتصالات التي تتضمن عنصراً للأمن السيبراني*	*الوثائق المكرسة لسياسة الأمن السيبراني*
الوكالة الدولية للطاقة الذرية	نعم، الخطة الإستراتيجية لتكنولوجيا الأعمال (2015–2020)	نعم، معايير أمن المعلومات
منظمة الطيران المدني الدولي	نعم، الاستراتيجية الرقمية لتكنولوجيا المعلومات والاتصالات (2017) (قيد الاستعراض)	نعم، سياسة أمن المعلومات (2007، التنقيح 2)
منظمة العمل الدولية	نعم، استراتيجية تكنولوجيا المعلومات (2018–2021)	نعم، أمن المعلومات الإلكترونية، بيانات السياسة (2010)
المنظمة البحرية الدولية	نعم، الخطة الاستراتيجية لتكنولوجيا المعلومات والاتصالات (2019–2023)	نعم، إدارة مخاطر أمن المعلومات (2015)
الاتحاد الدولي للاتصالات	لا، يتبع الاتحاد نهجاً أكثر شمولاً بإدخال نظام إدارة قدرة المنظمة على الصمود، بما يشمل تطوير تحليل تفصيلي للأثر على الأعمال يحدد المخاطر الاستراتيجية، واستراتيجيات للأثر على الأعمال، فضلاً عن إدارة الأزمات واستمرارية الأعمال والتعافي من الكوارث في مجال تكنولوجيا المعلومات والاتصالات	لا
منظمة الأمم المتحدة للتربية والعلم والثقافة	نعم، إدارة المعرفة واستراتيجية تكنولوجيا المعلومات والاتصالات (2018–2021)	نعم، مدرج في إطار الإدارة المركزية للمخاطر وفي الدليل الإداري (سياسة أمن المعلومات وتكنولوجيا المعلومات)
منظمة الأمم المتحدة للتنمية الصناعية	الاستراتيجية المؤسسية لتكنولوجيا المعلومات والاتصالات (2021–2029)	لا
منظمة السياحة العالمية	لا، لا تشمل إستراتيجية تكنولوجيا المعلومات والاتصالات الأمن السيبراني	لا، قيد التطوير
الاتحاد البريدي العالمي	لا، ستكون إستراتيجية الاتحاد البريدي العالمي لتكنولوجيا المعلومات والاتصالات متاحة في كانون الأول/ديسمبر 2021	لا
منظمة الصحة العالمية	نعم، إدارة المعلومات واستراتيجية التكنولوجيا (2019)	نعم، استراتيجية الأمن السيبراني
المنظمة العالمية للملكية الفكرية	نعم، استراتيجية تكنولوجيا المعلومات والاتصالات (استراتيجية جديدة قيد التطوير)	نعم، سياسات ومعايير أمن المعلومات والجيل القادم من إستراتيجية أمن المعلومات (2021–2024)
المنظمة العالمية للأرصاد الجوية	نعم، استراتيجية تكنولوجيا المعلومات والاتصالات (2020–2023)	لا

المرفق الخامس

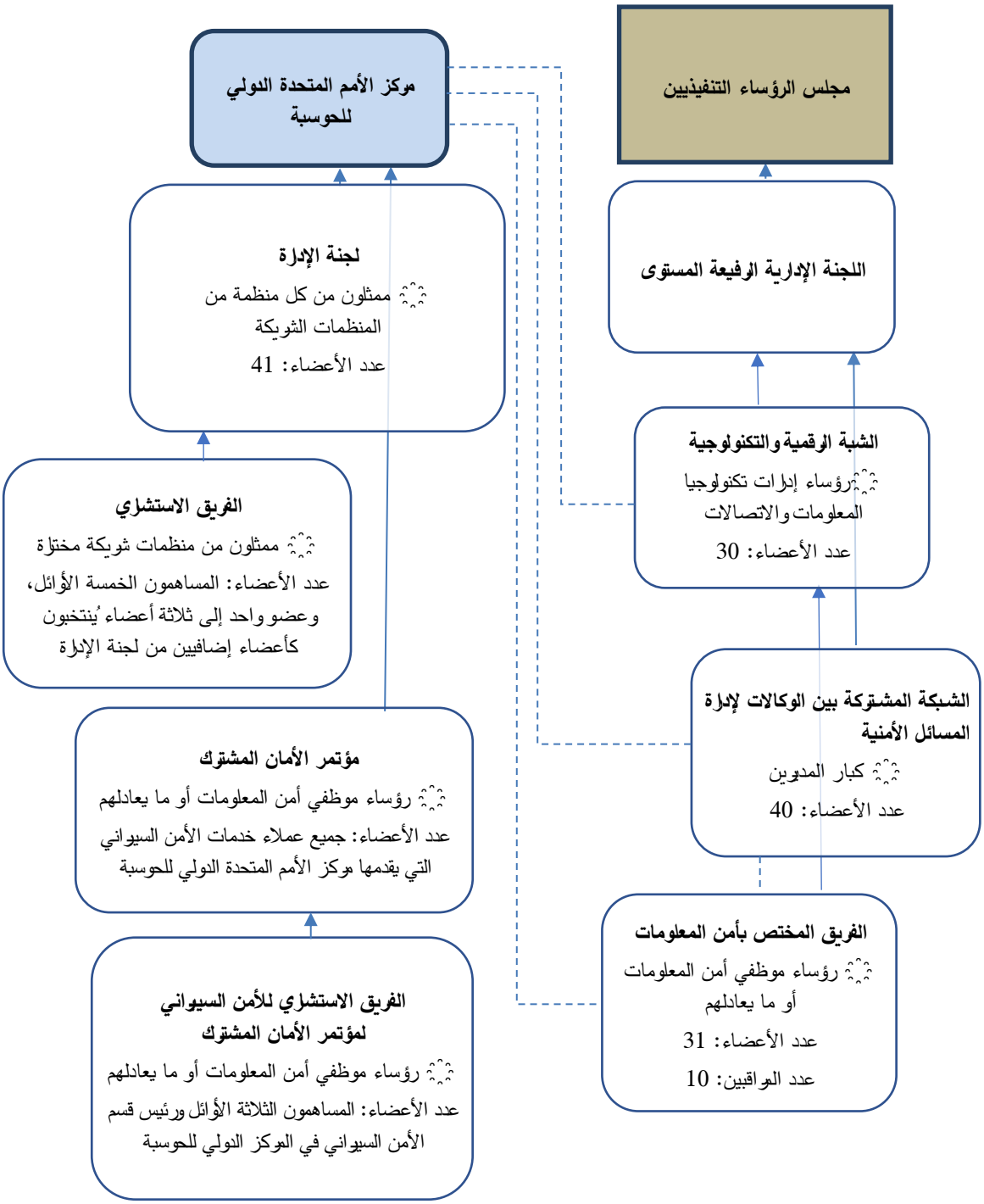
ترتيبات الأمن السيبراني والتسلسل الإداري للمسؤوليات في المنظمات المشارِكة في وحدة التفتيش المشتركة، حتى كانون الثاني/يناير 2021

المنظمات المشارِكة	*تُدار شؤون الأمن السيبراني من خلال قدرات داخلية مكرسة أو متخصصة*	*تغطي إدارة تكنولوجيا المعلومات والاتصالات في المنظمة الأمن السيبراني (إلى جانب الوظائف الأخرى المتعلقة بتكنولوجيا المعلومات والاتصالات)*	*يُستخدم "رئيس موظفي أمن المعلومات كخدمة" أو تُستخدم خدمة حوكمة الأمن التي يقدمها مركز الأمم المتحدة الدولي للحوسبة*	*مسؤولية أمام رئيس تكنولوجيا المعلومات والاتصالات (أو ما يعادله)*
الأمانة العامة للأمم المتحدة	√		X	√
برنامج الأمم المتحدة المشترك المعني بفيروس نقص المناعة البشرية/الإيدز		√	X	√
مؤتمر الأمم المتحدة للتجارة والتنمية		√	√ (عميل حالي)	√
برنامج الأمم المتحدة الإنمائي	√		X	√
برنامج الأمم المتحدة للبيئة		√	X	√
صندوق الأمم المتحدة للسكان	√ (يجري العمل على تعيين رئيس موظفي أمن المعلومات)	√ (إلى أن يتم التعيين)	√ (عميل حالي)	√
مفوضية الأمم المتحدة لشؤون اللاجئين	√		X	√
منظمة الأمم المتحدة للطفولة	√		√ (عميل حالي)	√
مكتب الأمم المتحدة المعني بالمخدرات والجريمة/مكتب الأمم المتحدة في فيينا		√	X	√
مكتب الأمم المتحدة لخدمات المشاريع	√		X	رئيس موظفي أمن المعلومات مسؤول أمام رئيس القسم المالي ومدير الإدارة
وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين في الشرق الأدنى	√		X	√
هيئة الأمم المتحدة للمرأة		√	√ (عميل سابق)	√
برنامج الأغذية العالمي	√		√ (عميل سابق)	√
منظمة الأغذية والزراعة للأمم المتحدة	√		√ (عميل حالي)	√
الوكالة الدولية للطاقة الذرية	√		X	√

المنظمات المشارِكة	*تُدار شؤون الأمن السيبراني من خلال قدرات داخلية مكرسة أو متخصصة*	*تغطي إدارة تكنولوجيا المعلومات والاتصالات في المنظمة الأمن السيبراني (إلى جانب الوظائف الأخرى المتعلقة بتكنولوجيا المعلومات والاتصالات)*	*تُستخدم "رئيس موظفي أمن المعلومات كخدمة" أو تُستخدم خدمة حوكمة الأمن التي يقدمها مركز الأمم المتحدة الدولي للحوسبة*	*مسؤولية أمام رئيس تكنولوجيا المعلومات والاتصالات (أو ما يعادله)*
منظمة الطيران المدني الدولي	√		√ (عميل سابق)	رئيس موظفي أمن المعلومات مسؤول أمام رئيس الإدارة
منظمة العمل الدولية	√		X	√
المنظمة البحرية الدولية		√	X	√
الاتحاد الدولي للاتصالات	√		X	√
منظمة الأمم المتحدة للتربية والعلم والثقافة	√		√ (عميل حالي)	√
منظمة الأمم المتحدة للتنمية الصناعية		√	X	√
منظمة السياحة العالمية		√	X	√
الاتحاد البريدي العالمي		√	X	√
منظمة الصحة العالمية	√		√ (عميل سابق)	√
المنظمة العالمية للملكية الفكرية	√		X	لدى رئيس شعبة الأمن وضمان المعلومات دور مزدوج إذ أنه يمارس وظيفة رئيس موظفي الأمن ويعتبر مسؤولاً عن الأمن المادي وأمن المعلومات، وهو مسؤول أمام مساعد المدير العام لشؤون الإدارة والمالية والتنظيم
المنظمة العالمية للأرصاد الجوية		√	√ (عميل حالي)	√

المرفق السادس

الترتيبات المؤسسية والتشغيلية المشتركة بين الوكالات بشأن الأمن السيبراني



المصدر: من إعداد وحدة التفتيش المشتركة.

المرفق السابع

نظرة عامة على خدمات الأمن السيبراني لمركز الأمم المتحدة الدولي للحوسبة التي اشتركت فيها المنظمات المشارِكة في وحدة التفتيش المشتركة حتى كانون الثاني/يناير 2021

خدمة الأمن السيبراني	*وصف مقتضب*	*عدد المنظمات الحالية المشاركة في وحدة التفتيش المشتركة والتي اشتركت في خدمات المركز*	*عدد المنظمات السابقة المشاركة في وحدة التفتيش المشتركة والتي اشتركت في خدمات المركز أو أنجزت مشاريعها معه*
الأمان المشترك – المعلومات الاستخباراتية للتهديدات	القيام بصورة مستمرة حسنة التوقيت بجمع المعلومات من أعضاء الوكالات؛ وشركات الأمن التجارية؛ ومقدمي الخدمات؛ والوكالات الحكومية على المستوى الاتحادي ومستوى الولايات والمستوى المحلي؛ وموارد إنفاذ القانون والموارد الموثوقة الأخرى، مما يمكّن الكيانات المشتركة من تقاسم أية معلومات ذات صلة بتهديدات الأمن المادي والأمن السيبراني ويمكن اتخاذ إجراءات على أساسها وكذلك أي معلومات تتعلق بالحوادث.	17	
خدمة التوقيع الإلكتروني المشتركة	تتيح القدرة على توفير التواقيع الرقمية.	14	
التوعية بأمن المعلومات	تقدم خدمات استشارية استراتيجية لمساعدة المنظمة على وضع إستراتيجية متقدمة فعالة للتوعية بأمن المعلومات، ومختبر للتعلم أو لدعم الاتصالات قائم سحابياً ورائد في هذه الصناعة، ويشمل ذلك نواتج متوخاة من خلال الرسائل والنشرات والملصقات ودعم البوابات.	7	3
إدارة الضعف	مزيج من العمليات والتكنولوجيات التي توفر تحديد أوجه الضعف وعيوب التكوين وتصحيحها بصورة مستمرة. ويتم تحقيق ذلك من خلال أمور منها مسوحات أوجه الضعف لدى المضيف وفي التطبيقات، وفحص التكوين الأمني ورصد بصمة الإنترنت.	6	1
خدمات دعم الحوكمة ورئيس موظفي أمن المعلومات	خدمة نظام إدارة أمن المعلومات بهدف حماية أصول المنظمة والتخفيف من خطر التعرض لأثر سلبي على السمعة، ومن فقدان المعلومات ذات الصلة، والأفعال الخبيثة، وكذلك المخاطر على الملكية الفكرية والبيانات الحساسة والسمعة.	6	5
خدمات محاكاة التصيد الاحتيالي	اختبارات لفعالية برامج التوعية بأمن المعلومات في المنظمات. وتتضمن الأداة كلاً من تصميم وتنفيذ حملات محاكاة التصيد الاحتيالي وتقارير المتابعة.	6	
خدمة العمليات الأمنية المشتركة	توفر خبرة متخصصة لمراقبة أحداث الأمن السيبراني وتحليلها والاستجابة لها، مما يمكّن الكيانات المشتركة من الاستجابة للحوادث الأمنية في الوقت المناسب باستخدام مجموعة من العمليات والحلول القائمة على التكنولوجيا.	4	1

خدمة الأمن السيبراني	*وصف مقتضب*	*عدد المنظمات الحالية المشاركة في وحدة التفتيش المشتركة والتي اشتركت في خدمات المركز*	*عدد المنظمات السابقة المشاركة في وحدة التفتيش المشتركة والتي اشتركت في خدمات المركز أو أنجزت مشاريعها معه*
الاستجابة للحوادث	توفر الإجراءات للتعامل مع الحوادث استناداً إلى معايير الصناعة لتحليل البيانات المتعلقة بالحادث ولتحديد الاستجابات المناسبة لأي حادث أمني في المنظمة في الوقت الفعلي.	4	7
تقييم الأمن السحابي	التقييم والترحيل والتنفيذ والدعم التشغيلي المُدار بالكامل بالإضافة إلى إدارة التكلفة لعدد من الحلول السحابية.	4	1
اختبار الاختراق	تمكّن من تحديد نقاط الضعف في ضوابط أمن المعلومات ويحدد مدى قدرة الخصوم على اختراق الشبكة أو الأنظمة التي يتم اختبارها.	3	4
البنية التحتية للمفاتيح العامة المشتركة	توفير وإدارة تشفير المفاتيح والتوقيعات الرقمية العامة والخاصة، مما يخلق بيئة آمنة للمعاملات الإلكترونية ونقل البيانات.	3	
إدارة الهوية والوصول	جمع المعلومات المتعلقة بتطبيقات إدارة الهوية والوصول وتحليلها وعرضها.	2	1
الأمان المشترك – إدارة المعلومات والأحداث	توفر تحليلًا في الوقت الفعلي للتحذيرات الأمنية التي تولدها التطبيقات والمعدات الشبكية.	1	

المصدر: قائمة خدمات مركز الأمم المتحدة الدولي للحوسبة (تموز/يوليه 2021) وردود المنظمات المشارِكة على استبياني وحدة التفتيش المشتركة.

المرفق الثامن

مقارنة لعضوية الكيانات النشطة في مجال الأمن السيبراني، حتى كانون الثاني/يناير 2021

المنظمات المشاركة	*الشبكة الرقمية والتكنولوجية (الدورة الثالثة والثلاثون، 2019)*	*الفريق المختص بأمن المعلومات (الندوة الثامنة، 2019)*	*لجنة إدارة مركز الأمم المتحدة الدولي للحوسبة (2020)*	*عملاء خدمة الأمن السيبراني التابعة لمركز الأمم المتحدة الدولي للحوسبة (السابقون والحاليون)*
الأمانة العامة للأمم المتحدة	√	√	√	X
برنامج الأمم المتحدة المشترك المعني بفيروس نقص المناعة البشرية/الإيدز	√	X	√	X
مؤتمر الأمم المتحدة للتجارة والتنمية	√	X	√	√
برنامج الأمم المتحدة الإنمائي	√	√	√	√
برنامج الأمم المتحدة للبيئة	√	X	√	X
صندوق الأمم المتحدة للسكان	√	√	√	√
موئل الأمم المتحدة	√	X	X[1]	X
مفوضية الأمم المتحدة لشؤون اللاجئين	√	√	√	√
منظمة الأمم المتحدة للطفولة	√	√	√	√
مكتب الأمم المتحدة المعني بالمخدرات والجريمة/مكتب الأمم المتحدة في فيينا	X	X	X[2]	√
مكتب الأمم المتحدة لخدمات المشاريع	√	X	√	√
وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين في الشرق الأدنى	√	X	√	√
هيئة الأمم المتحدة للمرأة	√	√	√	√
برنامج الأغذية العالمي	√	√	√	√
منظمة الأغذية والزراعة للأمم المتحدة	√	X	√	√
الوكالة الدولية للطاقة الذرية	√	√	√	√
منظمة الطيران المدني الدولي	√	X	√	√
منظمة العمل الدولية	√	√	√	√
المنظمة البحرية الدولية	√	X	√	√
الاتحاد الدولي للاتصالات	√	√	√	√
منظمة الأمم المتحدة للتربية والعلم والثقافة	√	X	√	√

(1) أفاد مركز الأمم المتحدة الدولي للحوسبة أن موئل الأمم المتحدة كان ممثلاً في لجنة الإدارة من خلال الأمانة العامة للأمم المتحدة.

(2) أفاد مركز الأمم المتحدة الدولي للحوسبة أن مكتب الأمم المتحدة المعني بالمخدرات والجريمة/مكتب الأمم المتحدة في فيينا كان ممثلاً في لجنة الإدارة من خلال الأمانة العامة للأمم المتحدة.

المنظمات المشاركة	*الشبكة الرقمية والتكنولوجية (الدورة الثالثة والثلاثون، 2019)*	*الفريق المختص بأمن المعلومات (الندوة الثامنة، 2019)*	*لجنة إدارة مركز الأمم المتحدة الدولي للحوسبة (2020)*	*عملاء خدمة الأمن السيبراني التابعة لمركز الأمم المتحدة الدولي للحوسبة (السابقون والحاليون)*
منظمة الأمم المتحدة للتنمية الصناعية	√	√	√	√
منظمة السياحة العالمية	X	√	X	√
الاتحاد البريدي العالمي	X	√	√	X
منظمة الصحة العالمية	X	√	√	√
المنظمة العالمية للملكية الفكرية	√	√	√	√
المنظمة العالمية للأرصاد الجوية	√	√	√	√

المرفق التاسع

مسرد المصطلحات المتعلقة بالأمن السيبراني

مســـح روبوتي (Bot herding)، شبكة روبوتية (botnet)	الشبكة الروبوتية تتألف من عدد كبير من أجهزة الحاسوب المخترقة التي تُستخدم في إنشاء رسائل بريد طفيلي أو فيروسات وإرسالها، أو في إغراق شبكة ما برسائل هجوم لقطع الخدمة. *المصدر*: ESCAL Institute of Advanced Technologies, glossary of security terms /www.sans.org/security-resources/glossary-of-terms
الخرق (Compromise)	الإفصـــاح المتعمد أو غير المتعمد عن المعلومات، مما يؤثر ســلباً على ســريتها أو سلامتها أو توفرها. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
هجوم قطع الخدمة الموزع (Distributed Denial of Service attack)	هجوم تستخدم فيه أنظمة متعددة مخترقة لمهاجمة هدف واحد. ويجبر تدفق الرسائل الواردة إلى النظام المستهدَف ذلك النظام على الإغلاق وقطع الخدمة عن المستخدِمين الشرعيين. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
تشفير (Encryption)	وظيفة رياضية تحمي المعلومات بجعلها غير قابلة للقراءة من قبل أي شخص باستثناء أولئك الذين لديهم المفتاح لفكّها *المصـــدر*: National Cyber Security Centre (the United Kingdom) www.ncsc.gov.uk/information/ncsc-glossary
جهاز استخدام نهائي (End point device)	أي جهاز متصـل بالشـبكة، مثل أجهزة الحاسـوب المكتبية أو المحمولة أو الهواتف الذكية أو الأجهزة اللوحية أو الطابعة أو غيرها من الأجهزة المتخصـصـــة، مثل أجهزة نقطة البيع أو أكشاك البيع بالتجزئة، والتي تعمل كجهاز للاستخدام النهائي في شبكة موزعة. *المصدر*: Barracuda Networks Inc., Glossary www.barracuda.com/glossary/endpoint-device
جدار الحماية الناري (Firewall)	حاجز أمني يُنصـب بين شـبكتين ويتحكم في مقدار حركة المرور التي يمكن أن تمر بين الشـبكتين وأنواعها. ويحمي هذا الجدار موارد الأنظمة المحلية من الوصـول إليها من الخارج. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
إنترنت الأشياء (Internet of things)	شـبكة من الأجهزة اليومية الممكَّنة بالإنترنت والقادرة على الاتصـال وتبادل المعلومات فيما بينها. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
البرمجيات الخبيثة (Malware)	برمجيات ضـارة مصـممة لاختراق نظام حاسوب أو إعطابه دون موافقة مالكه. وتشمل الأشـكال الشـائعة للبرمجيات الخبيثة فيروسـات الحاسـوب والفيروسـات الدودية المتنقلة وأحصنة طروادة التجسس وبرامجيات الإعلانات. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary

التصيد الاحتيالي (Phishing)	محاولة من قبل طرف ثالث للحصول على معلومات سرية من فرد أو مجموعة أو منظمة عن طريق تقليد أو انتحال علامة تجارية معينة، مشهورة عادةً، لتحقيق مكاسب مالية. ويحاول المتصيدون الاحتياليون خداع المستخدِمين للإفصاح عن البيانات الشخصية، مثل أرقام بطاقات الائتمان وبيانات دخول حساباتهم المصرفية عبر الإنترنت وغيرها من المعلومات الحساسة، والتي يمكن أن يستخدمونها بعد ذلك لارتكاب أفعال احتيالية. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
برمجيات الفدية (Ransomware)	نوع من البرمجيات الخبيثة التي تمنع وصول المستخدم إلى نظام ما أو بيانات معينة حتى يتم دفع مبلغ من المال. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
تكنولوجيا معلومات الظل (Shadow IT)	استخدام من جانب إدارة أو فرد لأجهزة أو برمجيات من دون معرفة فريق تكنولوجيا المعلومات أو فريق الأمن في المنظمة. *المصدر*: Cisco www.cisco.com/c/en/us/products/security/what-is-shadow-it.html
الهندسة الاجتماعية	التلاعب بالأشخاص بهدف دفعهم إلى تنفيذ إجراءات محددة أو إفشاء معلومات مفيدة للمهاجم. *المصدر*: National Cyber Security Centre (the United Kingdom) www.ncsc.gov.uk/information/ncsc-glossary
التصيد الاحتيالي الانتحالي (Spear phishing)	استخدام رسائل البريد الإلكتروني المنتحلة لإقناع الأشخاص ضمن منظمة ما بكشف أسمائهم أو كلمات مرورهم كمستخدِمين. وعلى خلاف التصيد الاحتيالي الذي ينطوي على إرسال البريد بأعداد كبرى، يعتبر التصيد الاحتيالي الانتحالي محدود النطاق وموجه جيداً. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
الانتحال (Spoofing)	انتحال عنوان مرسل رسالة ما بقصد الدخول غير القانوني إلى نظام مأمون. *المصدر*: Committee on National Security Systems (the United States) https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
شبكة خاصة افتراضية (Virtual private network)	شبكة اتصالات خاصة تستخدم عادة ضمن شركة، أو من جانب عدة شركات أو منظمات مختلفة، للتواصل عبر شبكة أوسع. وتكون اتصالات الشبكة الخاصة الافتراضية مشفرة عادةً لحماية حركة المرور من المستخدِمين الآخرين الموجودين في الشبكة العامة التي تعمل الشبكة الخاصة الافتراضية ضمنها. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
ضعف (Vulnerability)	عيب أو ضعف في تصميم أو تنفيذ نظام للمعلومات، أو في بيئة ذلك النظام، يمكن استغلاله للتأثير سلباً على أصول المنظمة أو عملياتها. *المصدر*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary

المرفق العاشر

نظرة عامة على الإجراءات التي يتعين على المنظمات المشارِكة اتخاذها بناء على توصيات وحدة التفتيش المشتركة

تقرير		الأثر المنشود	مركز الأمم المتحدة الدولي للحوسبة	الأمم المتحدة	برنامج الأمم المتحدة المشترك المعني بفيروس نقص المناعة البشرية ومتلازمة نقص المناعة المكتسب/الإيدز	مؤتمر الأمم المتحدة للتجارة والتنمية	مركز التجارة الدولية	برنامج الأمم المتحدة الإنمائي	برنامج الأمم المتحدة للبيئة	صندوق الأمم المتحدة للسكان	برنامج الأمم المتحدة المستوطنات البشرية	مفوضية الأمم المتحدة لشؤون اللاجئين	منظمة الأمم المتحدة للطفولة (اليونيسيف)	مكتب الأمم المتحدة المعني بالمخدرات والجريمة	مكتب الأمم المتحدة لخدمات المشاريع	وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين في الشرق الأدنى (الأونروا)	هيئة الأمم المتحدة للمساواة بين الجنسين وتمكين المرأة	برنامج الأغذية العالمي	منظمة الأغذية والزراعة للأمم المتحدة	الوكالة الدولية للطاقة الذرية	منظمة الطيران المدني الدولي	منظمة العمل الدولية	المنظمة البحرية الدولية	الاتحاد الدولي للاتصالات	منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)	منظمة الأمم المتحدة للتنمية الصناعية	منظمة السياحة العالمية	الاتحاد البريدي العالمي	منظمة الصحة العالمية	المنظمة العالمية للملكية الفكرية	المنظمة العالمية للأرصاد الجوية
	لاتخاذ إجراءات للعلم		☒ ☐	☐ ☒	☒ ☐	☐ ☒	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐	☒ ☐
التوصية 1		و		ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر	ر
التوصية 2		و		ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش	ش
التوصية 3		ج	ر																										
التوصية 4		ج		ش																									
التوصية 5		و		ر																									

مفتاح الجدول:

ش: توصية يتخذ الجهاز التشريعي قراراً بشأنها

ر: توصية يتخذ الرئيس التنفيذي إجراءً بشأنها

☐: توصية لا تتطلب أن تتخذ هذه المنظمة إجراءً بشأنها

الأثر المنشود: أ: تعزيز الشفافية والمساءلة؛ **ب:** نشر الممارسات الجيدة/الفضلى؛ **ج:** تعزيز التنسيق والتعاون؛ **د:** تعزيز التماسك والمواءمة؛ **هـ:** تعزيز المراقبة والامتثال؛ **و:** تعزيز الفعالية؛ **ز:** وفورات مالية كبيرة؛ **ح:** تعزيز الكفاءة؛ **ط:** غير ذلك.